Radia Client Automation Enterprise

For the Windows® and Linux operating systems

Software Version: 9.00

User 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

Trademark Notices

Adobe® is a trademark of Adobe Systems Incorporated.

Android™ is a trademark of Google Inc.

Apple, iPhone, and iPad are trademarks of Apple Computer, Inc., registered in the U.S. and other countries.

Intel® is a trademark of Intel Corporation in the U.S. and other countries.

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

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

Oracle and Java are registered trademarks of Oracle Corporation and/or its affiliates.

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.

Disclaimer for PDF Version of Online Help

This document is a PDF version of the online help. This PDF file is provided so you can easily print multiple topics from the help information or read the online help in PDF format.

Note: Some topics do not convert properly to PDF, causing format problems. Some elements of online help are completely removed from the PDF version. Those problem topics can be successfully printed from within the online help.

Contents

Chapter 1

Introduction

Radia Client Automation Enterprise is a PC software configuration management solution that provides software and HP hardware management features, including OS image deployment, patch management, remote control, HP hardware driver and BIOS updates, and software distribution and usage metering all from an integrated web-based console.

About This Publication

This publication provides detailed information and instructions for using the Radia Client Automation Console, Publisher, Application Self-service Manager, and the Image Preparation Wizard.

For requirements and directions on installing and initially configuring RCA Core and Satellites Servers, see the *Radia Client Automation Enterprise Installation and Upgrade Guide*.

RCA Documentation

The Radia Client Automation documentation that is available on the media is also installed during the Core installation. These documents are available as PDFs and can be accessed on the Core server using the Windows Start menu, the shortcut link on the desktop, or by using a browser from any device with access to the Core server machine at: `http://`*HPCA_Host:*`3466/docs`, where *HPCA_Host* is the name of the server where RCA is installed.

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
InstallDir	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`

Variable	Description	Default Values
SystemDrive	Drive label for the drive where the RCA server is installed	C:

Chapter 2

Getting Started

After you have installed RCA, you are ready to start using the web-based RCA Console (the Console) to begin managing your environment.

The sections in this chapter introduce:

- The RCA Console that you will use to perform various administrative and configuration tasks. See "Accessing the Web-based RCA Console" below.
- The tasks that you must complete to begin managing your RCA environment. This includes configuration steps and where to get more information. See "Implement RCA" on page 33.

Accessing the Web-based RCA Console

The RCA server uses a Console through which various administrative and configuration tasks can be performed. For more information on these tasks, see "Operations" on page 221 and "Configuration" on page 253.

There are four methods by which you can launch the RCA Console. You can:

- Double-click the **Radia Client Automation Console** desktop icon.
- Navigate the Windows **Start** menu path of the machine on which the RCA server was installed.
- Open a Microsoft® Internet Explorer® (minimum version 7.0) or Mozilla Firefox (minimum version 2.0) web browser on any device in your environment and go to:

  `http://`*`HPCA_host`*`:3466/`

  Where *HPCA_host* is the name of the server on which RCA is installed.

  Each method will launch the RCA Console, which will prompt you for login credentials. When prompted, specify your user name and password, and click **Sign In**.

  > **Note:** The default user name is `admin` and the default password is `secret`. For more information on changing the default user name and password, and adding users to the Console-access authority list, see "Configuration" on page 253.

- Insert a smart card.

  > **Note:** Smart Card authentication is available on Enterprise Core Servers only.

  Follow these steps to launch the RCA Console using smart card:

  a. Open a Microsoft® Internet Explorer® (minimum version 7.0) or Mozilla Firefox (minimum version 2.0) web browser on any device in your environment and go to:

     `https://`*`HPCA_host/`*

Where *HPCA_host* is the name of the server on which RCA is installed.

b. Click **Sign on using Smart Card.**

> **Note:** To see **Sign on using Smart Card**, SSL must be enabled and you must access the login page through SSL. To log in, see "Smart Card Authentication" on page 275.

c. When prompted, select the certificate that matches a trusted certificate in the Core Server trust store. This is configured through the SSL section in the RCA Console.

d. When prompted, specify your Smart Card pin number.

Important Notes

- The RCA console may open additional browser instances when you are running wizards or displaying alerts. To access these wizards and alerts, be sure to include RCA as an Allowed Site in your browser's pop-up blocker settings.
- For security, RCA automatically logs out the Console user if the user remains idle for 20 minutes. The Console user must log on again to continue using the Console. To increase the inactivity time before the current user is logged out, see "Increasing the Inactivity Time" below.
- To view the graphical reports in the **Reporting** section of the Console, you require either Java Runtime or Java Virtual Machine. You can install Java from http://java.com/en/index.jsp.
- **Windows 2003 Server**: To allow local access to RCA on a device with the Windows 2003 Server operating system, you must enable **Bypass proxy server for local address** in the **Local Area Network** (**LAN**) settings.
- The display language for RCA Console user interface is same as the display language set for the OS. You can change the OS display language to view the RCA Console in the updated language. After changing the OS display language, if the RCA Console user interface is not updated in the new display language, reboot your computer, and then log on to the RCA Console.

Increasing the Inactivity Time

Complete the following steps to increase the RCA Console inactivity time:

1. Navigate to the `<InstallDir>\tomcat\webapps\sessionmanager\WEB-INF` directory.
2. Using a text editor open the `sessionmanager.properties` file.
3. Set the value for the parameter `http.session.timeout.minutes` to the amount of time (in minutes) for which the Console user can remain in idle state, after which the user is automatically logged-out. By default, this value is set as 20 minutes.
4. Save and close the `sessionmanager.properties` file.
5. Restart the HPCA Tomcat service.

Implement RCA

The following sections describe the initial tasks that you will complete to begin using RCA to manage your environment. All of these tasks are completed using the RCA Core Console. Some of the tasks are required (*mandatory*) to establish a viable RCA environment; others, although *optional*, are also included because they enable additional basic administrative functionality.

The following tabs of the RCA Core Console enables you to access the various administrative tasks:

- Dashboard
- Management
- Reporting
- Operations
- Configuration

Note: It will not be necessary to access all of these tabs to complete the configuration tasks.

Mandatory Tasks

The tasks that are listed in this section must be completed to establish a viable and functioning RCA-managed environment.

1. **Import Devices**: Import your client devices into the RCA environment so that they are “known” to the RCA server. For more information, see "Import Devices" on next page.
2. **Deploy RCA Agent**: Deploy the RCA agent to the client devices that you have imported. This will bring them under the control of RCA.

   There are several methods by which to deploy an RCA agent; these are described in "Deploy the RCA Agent" on next page.
3. **Configure Policy**: Use RCA to establish the “state” of the RCA agents on your client devices. For more information, see "Configure Policy" on next page.

Optional Tasks

The tasks that are listed in this section can be completed to establish additional administrative control over, and functionality within, your RCA environment. More information about each of these tasks is presented in the respective sections.

- "Manage Vulnerabilities" on page 36
- "Configure Client Operations Profiles" on page 36
- "Configure Patch Management" on page 40
- "Deploy Operating System Images" on page 42
- "Enable Out of Band Management" on page 43

Import Devices

You must import (into RCA) the devices in your environment that you want to have managed by RCA. Doing so will make RCA aware of them, and will enable you to collect inventory information and deploy software and patches.

- On the Device Management General tab, click **Import** to launch the Import Device Wizard (see "Importing Devices" on page 145).
- Follow the steps in the wizard to import devices.

When devices have been imported, you can deploy the RCA agent to manage software, patches, and inventory.

Deploy the RCA Agent

The RCA agent gets deployed to and installed on a device to facilitate an RCA administrator managing the device. The agent can be deployed to a device, or deployed to several devices that belong to a group.

The RCA agent is deployed to devices by using the Agent Deployment Wizard (see "Deploying the RCA Agent" on page 147). When the wizard completes, an Agent Deployment job is created.

For additional information about the RCA agent, see the *Radia Client Automation Enterprise Application Manager and Application Self-Service Manager Reference Guide*.

Configure Policy

RCA resolves a managed agent's desired state according to the policy entitlements that an RCA administrator has defined for a machine or user. The policy entitlements can be defined:

- **Internally**: In the PRIMARY.POLICY Domain of the Configuration Server Database (CSDB).
- **Externally**: In an LDAP directory, such as Active Directory.

  The Core CSDB is pre configured with default instances that make it easy to implement existing external policy. The Core and Satellite servers can be set to enable and configure an external policy connection.

Configuring Internal Policy

Policy for RCA agents can be configured in the PRIMARY.POLICY.USER Class of the Core CSDB. When an RCA agent connects to the CSDB, if its user identity has been defined as an instance in the USER Class, resolution will occur according to the policy that is defined in that instance. If you are using this method for your policy store, you should:

- Disable the policy services on the Core and Satellite servers.
- Add USER Instances to the USER Class and connect them to the services to which the users are entitled.

For more information on establishing this method of internal policy, see the chapter, Creating Users and Groups in Configuration Server Database in *Radia Client Automation Enterprise Administrator User Guide*.

Configuring External Policy

Policy settings can be applied to an existing LDAP (or other external) directory and then enabled for use with an RCA environment.

When using an external policy store, the default behavior in the Core CSDB is:

- For RCA agent connects, if the user is not defined by a USER Instance, resolution defaults to using the machine domain name and looks for policy defined in an external LDAP directory that has been configured for access using the policy settings on the Core and Satellite Consoles.
- The resolution by machine name from an external directory is defined in the _NULL_ INSTANCE_ of PRIMARY.POLICY.USER. This instance includes an _ALWAYS_ (Utility Method) connection with its attribute set to SYSTEM.ZMETHOD.LDAP_RESOLVE.

Implementing an External Policy Store

The policy configuration default values for an external policy store are set to connect to an LDAP directory, and manage policies using the fully qualified domain name of the RCA agent-managed machines. To manage policies using different parameters, adjust the ZMTHPRMS attribute in the LDAP_RESOLVE method, as discussed in To implement an external LDAP policy store.

By default, configuring the Core for an external directory service results in the Portal also being configured to use (for policy) the same external directory service. The external directory service connection is derived from the Base DN.

To implement an external LDAP policy store:

1. Configure the Core so that the Policy service can connect to the external directory service that is used for policy.
2. Enable and configure full-service Satellites to connect to the external directory service.
3. Use the LDIF file that was generated at the Policy page of the Core Console (and which contains the schema changes) to modify your directory schema so that the RCA policy settings are used.

   The command to backup an existing LDAP is:

   `LDIFDE -f` *OutputFileName*

   The command to update the external directory service is:

   ```
   LDIFDE -i -f HPCAExtensions.ldif -v
   ```

   Note: The `LDIFDE` command is applicable to Windows server platforms only. For additional information, see the Microsoft Knowledge Base article, Using LDIFDE to import and export directory objects to Active Directory.

   For more information, see the *Radia Client Automation Enterprise Policy Server Reference Guide*.

4. If necessary, modify the LDAP_RESOLVE method in the PRIMARY.SYSTEM.ZMETHOD Class of the Core Configuration Server Database.

   By default, the CSDB is pre configured to use the LDAP_RESOLVE method and manage policies by the fully qualified domain name of the machine. The ZMTHPRMS attribute defines this:

   ```
   ZMTHPRMS = ldap:\\\<ADINFO.COMPDN>>
   ```

   This requires that the machine be a member of the domain that corresponds to the directory in which policy has been defined. If the machine is not a member of the domain, ADINFO.COMPDN will be blank.

   a. Adjust the ZMTHPRMS value to manage policy using a different value. To do this, see *Configuring the LDAP Method* in the *Radia Client Automation Enterprise Policy Server Reference Guide*.

   b. IMPORTANT: If you adjust the ZMTHPRMS value in the Core CSDB, always perform a synchronization with the Satellite to bring down the new value to each Satellite that is enabled for Configuration and Policy.

Following Policy Server configuration, use the Management tab to add, administer, and query the policy entitlements in your LDAP policy store.

Verifying Policy Resolution

To verify that policy is being resolved through a Satellite, do the following.

1. Use the Management tab to browse the policy directory and entitle an RCA agent to a service through its directory service object. For more information, see the "Directory Objects" on page 131.
2. Have the RCA agent installed on the device, with a SAP entry directing it to the Satellite as **PRI 10**, Core as **PRI 20**.
3. Perform an RCA agent connect and verify that the entitled service is available for installation (using Application Self-Service Manager) or is installed (for Application Manager).

Manage Vulnerabilities

To support HPCA Vulnerability Management, you must:

- Create Notify settings
- Review the Console settings
- Configure the **HP Live Network** settings on the Configuration tab of the Console

For additional information, see the *Security and Compliance Management* chapter.

Configure Client Operations Profiles

In an RCA server environment, use **Client Operations Profiles** (**COPs**) to direct your RCA agents to the Satellite access points in your enterprise for their configuration and data resources.

Create Server Access Profile Instances

The SAP Class of the Core Configuration Server Database contains samples for each type of **Server Access Profile** (**SAP**).

You need to create new instances for each Satellite in your environment. Full-service Satellites generally have two instances each, and streamlined Satellites a single instance, as discussed in this section.

Note: The Configuration Server Database changes that are detailed in this must be done on a Core CSDB.

A Satellite server CSDB is a replication of its upstream server CSDB (either a Core or another Satellite) and should never be modified.

- *hostname*_**RCS Instance**: Use the CORE_RCS instance to create a *hostname*_RCS instance for full-service Satellites.

  The URI value of the *hostname*_RCS instance must be modified to point to the hostname of the machine that is hosting the Satellite.

- *hostname*_**RPS** Instance: Use the CORE_RPS instance to create a SAT_RPS instance for each full-service and each streamlined Satellite. For a friendly name, you could use *hostname* –Data to represent its role of providing data resources to RCA agents.

  The URI value of the *hostname*_RPS instance must be modified to point to the hostname of the machine that is hosting the Satellite.

Example

Assume an environment that includes two Satellites (PARISSAT3 and EUROSAT1) and requires the three SAP instances that are listed in the following table:

Sample SAP Instances for Two Satellites

Hostname	Satellite Mode	SAP Instance Name (Friendly Name)	SAP Type	SAP Priority
PARISSAT3	Streamlined	PARISSAT3_RPS (PARISSAT3 - DATA)	Data	10
EUROSAT1	Full-service	EUROSAT1_RPS (EUROSAT1 - DATA)	Data	20
EUROSAT1	Full-service	EUROSAT1_RCS (EUROSAT1 - RCS)	RCS	30

To create a Server Access Profile instance for a Satellite:

1. On the Core server, open the Radia Client Automation Administrator CSDB Editor and navigate to the **Primary** File, **Client** Domain, **Server Access Profile (SAP)** Class of the CSDB.

For information on how to access the RCA Administrator, see the *Radia Client Automation Enterprise Administrator User Guide*.

2. From the PRIMARY.CLIENT.SAP Class, copy the `CORE_RCS Instance` (friendly name: `Core - RCS`) to an instance named *hostname*`_RCS` with a friendly name of *hostname* `- RCS`. (In the example, the EUROSAT1_RCS instance has a friendly name of EUROSAT1 - RCS.)
3. Select and modify the *hostname*`_RCS` Instance; change the URI attribute to point to the hostname of the machine that is hosting the Satellite, as in:

   `URI = tcp://`*satellite_hostname*`:3464`
   `TYPE = RCS`
   `ROLE = OSMR`
4. Copy the `CORE_RPS` Instance (friendly name: `Core - RPS`) to a `CLIENT.SAP.`*hostname*`_RPS` instance with a friendly name of *hostname* `- Data`.

   `Data` indicates that this SAP entry addresses the server's role of providing data resources to the RCA agents. (In the example, the EUROSAT1_RPS instance has a friendly name of EUROSAT1 - Data.)
5. Select and modify the new *hostname*`_RPS` Instance; change the URI attribute to point to the full-service Satellite's hostname, as in:

   `URI = http://`*satellite_hostname*`:3466`
   becomes `http://EUROSAT1:3466`
   `TYPE = DATA`
   `ROLE = DZ`
6. Copy the newly created *hostname*`_RPS` Instance to create another instance for the streamlined Satellite. (In the example, the PARISSAT3_RPS instance has a friendly name of PARISSAT3 - Data.)
7. Modify the newly created SAP instance and set the URI attribute to point to the streamlined Satellite's hostname.
8. Save the changes.

Modify Server Access Profiles for Patch Distribution using the Gateway

If you are patching Microsoft devices, you can use a lightweight patching model by configuring the following patch distribution settings.

- Enable Download of Patch Metadata only
- Enable Gateway

When using these patch distribution settings, make sure that the SAP instances for the Core and Satellites that are defined with a TYPE of `DATA`, also include a ROLE of `P`. These instances are typically named Core_RPS and *satellite_hostname*_RPS.

If these SAP entries do not include the Role of `P`, modify them using the following procedure:

To modify your SAP instances to deliver patch binaries from the gateway:

For basic information on creating or editing SAP instances, see "Create Server Access Profile Instances" on page 37.

1. From the Core server, use the CSDB Editor to open the SAP instance for the `CORE_RPS` (the one with TYPE = DATA) and make the following changes:

   Add a ROLE value of **P**.

   The values should include the addition in bold:

   ```
   TYPE = DATA
   URI = http://hostname:3466
   ROLE = DZP
   ```

2. Save your changes to the `CORE_RPS` instance.
3. Apply the same ROLE change from Step 1 to your Satellite SAP instances defined with TYPE = DATA. These instances are generally named *satellite_hostname*_RCS.
4. Save all changes to the * _RPS instances for the Satellites.

Connect SAP Instances to a Location Class Instance

On the Core server, use PRIMARY.CLIENT.LOCATION Class instances to define the SAP priorities based on location criteria. The priority for a SAP is defined directly above the connection to that SAP instance in the SAPPRI attribute.

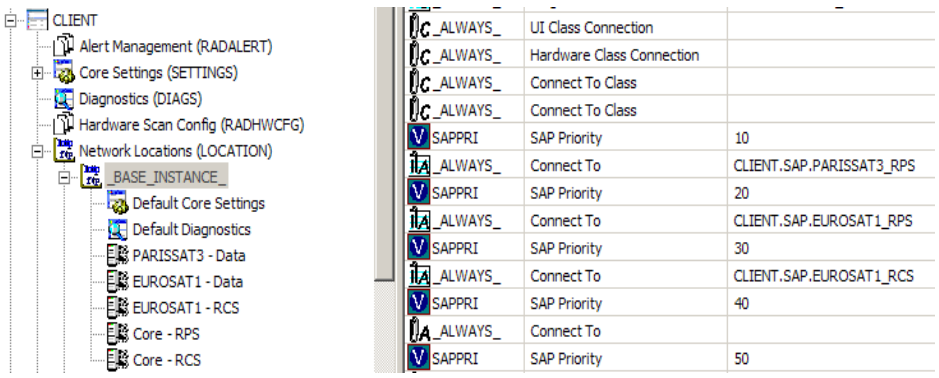
By default, the `Core_RPS` and `Core_RCS` instances are connected to the CLIENT.LOCATION._BASE_INSTANCE_ with priorities of 60 and 70, respectively.

Note: The priority values run low to high; the lower the number, the higher the priority. So, by assigning a lower number priority to Satellites, RCA agents will attempt to connect to them as their preferred access points. They will use the Core (with a higher priority number) as the failover access point.

To connect the Core and Satellite SAP instances to a LOCATION Class Instance:

1. On the Core server, use the Radia Client Automation Administrator CSDB Editor to set a priority for each SAP instance for each LOCATION Class Instance.

   For example, the following image shows SAP Instances connected to the `CLIENT.LOCATION._BASE_INSTANCE_` so that all RCA agents will use the Satellites as the preferred access points.



2. Connect the `CLIENT.SAP.PARISSAT3_RPS` Instance to the first available connection in the `CLIENT.LOCATION._BASE_INSTANCE_` and give it a priority of 10.
3. Connect the `CLIENT.SAP.EUROSAT1_RPS` Instance to the second available "Connect To" connection and give it a priority of 20.
4. Connect the `CLIENT.SAP.EUROSAT1_RCS` Instance to the third available "Connect To" connection and give it a priority of 30.

By giving the Satellite SAP instances higher priorities than the Core SAP instances, RCA agents will first attempt to connect to the Satellites. If the Satellites are unavailable, they will attempt to connect to the Core.

Enable Client Operations Profiles in RCA Agents

There are several ways to enable COPs in your RCA agents, depending on whether the RCA agents are already installed.

If an RCA agent is already installed on a device, you can modify the `args.xml` file to include the `<COP>Y</COP>` entry. Place the entry above the `</ARGUMENTS>` entry and save the changes.

Note: The `args.xml` file is located in `\lib` of the directory in which the RCA agent was installed. The default location is `C:\Program Files\Hewlett-Packard\HPCA\Agent`.

Alternatively, use `COP=Y` in the actions when running `radskman` (or any command to run an RCA agent connect) from a command line. For more information, see the *Radia Client Automation Enterprise Application Manager and Application Self-Service Manager Reference Guide*.

Synchronize the Satellites

To ensure that these changes to the Core CSDB take effect on the Satellites, run a synchronization from each Satellite Console.

Configure Patch Management

Before setting up an RCA environment to include patch management, your RCA databases should be appropriately configured. For details, see the *Radia Client Automation Enterprise Installation and Upgrade Guide*.

Patch management implementation involves setting up the Core and Satellite servers, and then using the Core Console to configure the vendor and acquisition-related settings, and begin patch acquisitions.

Use RCA to deploy and manage Microsoft, RedHat, and SuSE patches, Adobe patches, Java patches, and HP Softpaqs. Configure the server architecture using the following procedure:

1. Create a SQL database for patch and inventory report data.
2. Define an ODBC DSN.
3. Install a Core server and configure the following:

- Infrastructure Management
- Patch Management
- Policy (if using an external policy directory)

Note: When the Patch ODBC settings are saved in the Core Console, the Core server automatically runs an initial synchronization between the Patch Management database and the Core Configuration Server Database.

4. Install a Satellite server (recommended).

Completing the above tasks creates the RCA server environment for Patch Management.

Patch Management Administration Tasks

1. Enable Patch during the Core installation.
2. Complete all Patch Management configuration settings from the **Configuration** tab of the Console.
   - Create acquisition jobs for getting Microsoft, RedHat, Adobe, Java, and SuSE patches, as applicable.

     Note: You must download Java patches manually and save them at a specific location. Provide this location when you configure **Vendor Settings** in the **Patch Management** option under the **Configuration** tab. For more information, see "Java Feed Settings" on page 322.

     Note: Patch Management using Metadata is enabled by default. This feature reduces the time it takes to acquire patches and the overall load on the Core Configuration Server. For details, see "Patch Management Using Metadata" on page 355.

   - HP Softpaqs use a single, pre configured acquisition job. To take advantage of this, run an inventory against HP managed devices so that their HP Softpaq SysIDs can be automatically added to the acquisition settings for HP Softpaqs.
3. Perform patch acquisitions from the Core Console **Operations** tab.
4. After acquiring patches and publishing them to the Core CSDB, synchronize the content of the Core and Satellite servers using either a scheduled job or a Satellite Console Operations task.
   - Use the Core Console Management tab to create and run jobs to synchronize the content of the Core and Satellite servers.
   - Use the Satellite Console **Operations** tab to synchronize the Core and Satellite servers. The Satellite Console can be accessed at `http://satellite_hostname:3466`.
5. The next time the agents connect, a patch scan is run to discover which bulletins are applicable to which devices. Use the Dashboards and Reports tabs to view the results of the patch scans.

6. Apply policy to entitle bulletins to your managed devices. The applicable patches will be deployed without user intervention. Use the Dashboards and Reports to see the Patch compliance status of the managed devices.

Once applied, Adobe or Java patches cannot be removed as in case of Microsoft patches. You need to remove the entire Adobe or Java application.

Limitation on Modifying Configuration Files

HP discourages the customizing of configuration files for any of the components that are installed with the Core and Satellite servers.

Deploy Operating System Images

RCA can be used to deploy and manage operating system images. To deploy and manage operating system images, it recommends that you:

1. Enable the OS Manager service on the Core server.

   On the Core Console, Configuration tab, OS Management option, Settings area, select **Enable**.

   The "Operations" on page 221, "Configuration" on page 253, and "Managing the Enterprise" on page 131 chapters of this guide further discuss OS Manager settings in the Core Console.

2. Leave the default Core server name (zone) of **HP**.
3. Enable the OS Manager service on at least one Satellite server.

   On the Satellite Console, Configuration tab, Operating Systems area, select **Enable**.

   The "Configuration" on page 253 chapter of this guide further discusses OS Manager settings in the Satellite Console.

Your RCA server environment is now ready to use the OS Manager with its default configuration.

Core and Satellite Server Functions

The RCA servers perform the following OS Manager-related functions.

- The Core server hosts the tools and services that are used for:
  - Publishing the operating system images to the authoritative CSDB.
  - Performing OS Manager administrative tasks on the Console.
  - Creating policy entitlements.
- The Satellite server assumes the role of the OS Manager Server and Proxy Server; it handles requests for operating system images from the Configuration Server and provides the resources for these images to the managed devices.

  After you have published operating system images to the Core CSDB, use the Satellite Console **Operations** tab to synchronize and preload the operating system image resources onto the Satellite Server.

RCA OS Manager Notes

- By default, when the OS Manager is installed with a Core or Satellite server, it is configured to use the Linux Service OS—it is not set up to run WinPE as the Service OS.

  To convert the environment to use WinPE as the default Service OS, see the Converting the Service OS to WinPE Appendix in the *Radia Client Automation Enterprise OS Management Reference Guide*.

- The RCA Thin Client server can be installed using the RCA Console; it can also be enabled and disabled there.

Enable Out of Band Management

Out of Band Management (OOBM) refers to operations that are performed on a computer when it is in one of the following states.

- Plugged in but not actively running (off, in standby, hibernating)
- An operating system has not been loaded (software or boot failure)
- The software-based management agent is not available

The RCA Console supports OOBM of **Intel vPro** and **DASH**-enabled devices.

This section provides an overview of RCA OOBM. For more information on the features and functionality of RCA OOBM, see the *Radia Client Automation Enterprise Out of Band Management User Guide*.

Features

RCA provides the following OOBM features:

- Takes advantage of hardware-based management capabilities in PCs with vPro technology, as well as those with an implementation of the DASH standard.
- Improves hardware and software inventories, and reduces the need for desk-side visits.
- Provides *System Defense* capabilities for vPro devices that allow for selective network isolation.
- Provides *Agent Presence* capabilities that allow for the monitoring of local agents running on vPro systems.
- Provides an operating system-independent and tamper-resistant worm-containment system for vPro devices.
- Provides a secure communications channel through **Hypertext Transfer Protocol** (**HTTP**) authentication and **Transport Layer Security** (**TLS**).

Configuration Tasks

This section briefly describes some of the Administrator-based tasks that are performed on the **Configuration** tab of the RCA Console. An RCA administrator should perform these configuration

tasks as preparation for managing OOB devices. For more information on these tasks, see the *Radia Client Automation Enterprise Out of Band Management User Guide*.

- **Enable Out of Band Management**: The first thing an RCA administrator must do to perform OOBM tasks.

  Under Out of Band Management, click **Enablement**.

- **Select the Device Type**: The RCA Console offers three choices for device type: DASH Devices, vPro Devices, and Both.

  Under Out of Band Management, click **Device Type Selection**.

- **Manage vPro System Defense**: This option appears only if vPro Devices was selected as the device type to be managed.

  Under Out of Band Management, click **vPro System Defense Settings**.

  Note: System Defense settings do not apply to DASH devices.

Operations Tasks

This section briefly describes some of the tasks that can be performed in the Administrator and Operator roles of RCA. These OOB device-management tasks are performed on the **Operations** tab of the RCA Console by an RCA *administrator* or *operator*. For more information on these tasks, see the *Radia Client Automation Enterprise Out of Band Management User Guide*.

- **Provision Devices**: vPro devices must be provisioned before RCA can discover and manage them.

  Under Out of Band Management, click **vPro Provisioning**.

  Note: This option does not appear on the **Operations** tab if you have opted to manage only DASH devices because it is not relevant for these devices.

- **Manage Devices**: RCA administrators and operators can manage multiple and individual OOB devices.

  Under Out of Band Management, click **Device Management**.

- **Manage Groups**: RCA administrators and operators can manage groups of vPro devices.

  Under Out of Band Management, click **Group Management**.

- **View Alerts**: RCA administrators and operators can view the alerts generated by provisioned vPro devices if you have an alert subscription to the device.

  Under Out of Band Management, click **Alert Notifications**.

Chapter 3

Security and Compliance Management

The Security and Compliance Management features in RCA enable you to monitor and manage security vulnerabilities, configuration compliance, and security tool performance across your environment. This chapter includes the following topics:

Introduction

The RCA security and compliance management solution includes the following areas:

An overview of each area is provided in this chapter.

Vulnerability Management

Vulnerability management is the process of identifying, locating, and rectifying software security and vulnerability issues in the enterprise. There are three main steps in this process:

1. Obtain updated vulnerability definitions and scanner.
2. Scan the managed devices in the enterprise for the presence of vulnerabilities.
3. Report the vulnerability assessment of the devices scanned, including summary information for the enterprise as a whole.

The following terms are used throughout the RCA vulnerability management solution:

Vulnerability Management Terms

Term	Definition
vulnerability	A weakness in a system, its configuration, or its software that allows an individual to compromise the system's integrity to gain unauthorized access to its resources.

Term	Definition
exposure	Exposure can refer to a measurement of the various vulnerabilities in an environment. It also can be used to refer to a piece of software that provides information or capabilities that a hacker might use to attack or exploit a system.
CVE	Common Vulnerabilities and Exposures The CVE is a dictionary of common names (CVE Identifiers) for publicly known information security vulnerabilities and exposures. The CVE was started in 1999. It is currently sponsored by the United States Department of Homeland Security and managed by the MITRE Corporation. For more information, see http://cve.mitre.org
NVD	National Vulnerability Database The NVD is the U.S. government repository of standards based vulnerability management data. This data enables automation of vulnerability management, security measurement, and compliance. For more information, see http://nvd.nist.gov
CVSS	Common Vulnerability Scoring System The CVSS is a standard severity scoring system for information security vulnerabilities. CVSS includes three groups of metrics: Base, Temporal, and Environmental. For more information, see http://www.first.org/cvss
OVAL	Open Vulnerability and Assessment Language OVAL is the standard used to encode and transmit security information and system details. It is based on three XML schemas that represent the three security vulnerability assessment process steps: representing system configuration, expressing a specific machine state, and reporting the results of the assessment. The purpose of the CVE is to catalog all known vulnerabilities. The purpose of OVAL is to describe how to identify specific vulnerabilities. Most OVAL definitions are based on a CVE, but some are not. HP Live Network transmits information in OVAL and CVE format to RCA. For more information, see http://oval.mitre.org/

Compliance Management

Compliance management is the process of identifying, locating, and rectifying software configuration problems on managed client devices in the enterprise. There are three main steps in this process:

- Obtain updated compliance benchmarks and scanner.
- Scan the managed client devices in the enterprise to determine whether their configuration is in or out of compliance with the pertinent policy or regulatory standard defined by the compliance benchmarks.
- Report the results of the compliance scans, including summary information for the enterprise as a whole.

At this point, the administrator can take steps to resolve any configuration issues identified.

The following terms are used throughout the RCA compliance management solution:

Compliance Management Terms

Term	Definition
CCE	Common Configuration Enumeration The CCE is a dictionary of names for software security configuration issues (for example, access control settings and password policy settings). By providing unique identifiers for system configuration issues, the CCE facilitates fast and accurate correlation of configuration data across multiple information sources and tools. The CCE is currently managed by the MITRE Corporation. For more information, see http://cce.mitre.org
FDCC	Federal Desktop Core Configuration The FDCC is a security configuration mandated by the Office of Management and Budget (OMB) for all U.S. government agencies. The FDCC currently exists for Microsoft Windows Vista® and XP operating system software. The Windows Vista FDCC is based on the *Microsoft Security Guide for Vista*, which was developed through a collaborative effort of the Defense Information Security Agency (DISA), the National Security Agency (NSA), and NIST. The guide reflects the consensus recommended settings from DISA, NSA, and NIST for the Windows Vista platform. The Windows XP FDCC is based on a U.S. Air Force customization of the Specialized Security-Limited Functionality (SSLF) recommendations in NIST SP 800-68 and Department of Defense (DoD) customization of the recommendations in *Microsoft's Security Guide for Internet Explorer 7.0*. There are also FDCC benchmarks for Windows XP Firewall, Windows Vista Firewall, and Internet Explorer 7. For more information, see http://nvd.nist.gov/fdcc/index.cfm
USGCB	The United States Government Configuration Baseline The purpose of the USGCB initiative is to create security configuration baselines for Information Technology products widely deployed across the federal agencies. The USGCB baseline has evolved from the FDCC mandate. The USGCB is a Federal government-wide initiative that provides guidance to agencies on what should be done to improve and maintain an effective configuration settings focusing primarily on security. The USGCB currently exists for Microsoft Windows XP, Windows Vista, and Windows 7 operating system software. These recommendations were developed at the National Institute of Standards and Technology (NIST), which collaborated with DoD and Microsoft to produce the Windows 7, Windows 7 Firewall, Internet Explorer 8 USGCB. There are also USGCB benchmarks for Windows 7 Firewall, and Internet Explorer 8. For more information, see http://usgcb.nist.gov/index.html.
SCAP	Security Content Automation Protocol (pronounced ess-kap)

Term	Definition
	SCAP is a framework of interoperable and automatable security standards established by the National Institute of Standards and Technology (NIST). SCAP enables organizations to automate security monitoring, vulnerability management, and security policy compliance evaluation. SCAP incorporates the following specifications: • CVE (see "Vulnerability Management" on page 45) • CCE (see "CCE " on previous page) • Common Platform Enumeration (CPE), a naming convention for hardware, operating system (OS), and application products • Extensible Configuration Checklist Description Format (XCCDF), an XML specification for structured collections of security configuration rules used by OS and application platforms • OVAL (see "Vulnerability Management" on page 45) • CVSS (see "Vulnerability Management" on page 45) Because SCAP uses XML-based standards, SCAP content is both human and machine readable. NIST provides SCAP content, such as vulnerability and product enumeration identifiers, through a repository supplied by the National Vulnerability Database (NVD). For more information, see http://nvd.nist.gov/scap.cfm
CIS	Center for Internet Security The CIS developed a set of compliance standards before the time that NIST created SCAP. As of the publication of this documentation, the CIS had not released any additional benchmarks for newer operating systems. The HP Live Network team provides CIS benchmarks in SCAP format to Live Network content subscribers. For more information, see http://cisecurity.org.

A group of related compliance requirements is known as a **benchmark** (for example, FDCC-Windows-Vista). Benchmarks can be revised. A benchmark is given a new version name whenever it is revised (for example, FDCC-Windows-Vista v1.1.0.0).

Benchmarks contain **rules**. Each rule includes one or more automated tests that are used to determine whether or not a client device meets the requirements specified by that rule.

A benchmark consists of one or more **profiles**, which are used to define different levels of compliance within that benchmark. A profile specifies the following:

- A set of rules in the benchmark (possibly all of them)
- For each rule, the value that determines compliance against that rule

Compliance with a rule is determined by the profile. When RCA runs a compliance scan on a managed client device, it evaluates the requirements for the applicable benchmark profile.

The FDCC benchmarks each contain a single profile. The CIS benchmarks contain separate profiles for different types of systems. The Windows XP (v2.01) CIS benchmark, for example, contains profiles for Legacy, Enterprise Standalone, Enterprise Mobile, and Specialized Security systems.

Each rule is assigned a **weight** based on the potential effect and exposure to the enterprise if client devices do not comply with that rule. When a compliance scan is performed on a managed client device, a **score** is determined that reflects how many compliance rules passed and failed. This score represents a device's compliance with respect to a particular benchmark profile (SCAP checklist).

Note: In certain compliance reports and dashboards, compliance results for a particular benchmark are aggregated across all profiles that pertain to each managed client device. See "Compliance Management Reports" on page 212 and the "Compliance Management Dashboard" on page 104 for more information.

The benchmark, profiles, and rules are all delivered as a bundle of files known as an SCAP **datastream**. These files are read by SCAP-capable tools, such as the RCA compliance scanner.

Security Tools Management

RCA scans the managed client devices in your enterprise to determine what security tools are present and to collect pertinent information about the products detected. The following types of security tools are supported:

- Anti-virus tools
- Anti-spyware tools
- Software firewalls

HPCA Security Tools Management (STM) scanner contains embedded knowledge about various security products that it can detect. The HPCA STM scanner enables RCA to determine which specific security products are installed, which are enabled, when the most recent anti-virus and anti-spyware scan was performed on each client device, and when virus and spyware definitions were most recently updated on the client devices. The collected information is then displayed in the Security Tools Management dashboard and related reports.

To view the list of products currently supported by HPCA STM scanner, see the following URL: https://hpln.hp.com/page/security-tools-management

Note: The STM scanner detects and provides detailed information for the products listed on the above URL. For other products, STM scanner detects and provides the following basic information: protection status, product name, product version, and vendor name.

HP Live Network

RCA is integrated with HP Live Network, which provides security and compliance management content (data) and executable scanners. Your RCA installation comes with a small subset of the HP Live Network content for demonstration purposes. To obtain updated definitions and

scanners—and use the security and compliance management features in the RCA Console— see "Accessing HP Live Network Content" on page 127.

How Security and Compliance Management Works in RCA

Radia Client Automation offers a security and compliance management solution that enables you to detect security vulnerabilities and configuration policy compliance issues on managed client devices in your enterprise. This solution enables you to quickly assess the severity and scope of the related risk. You can then take steps to remediate problems identified.

RCA is integrated with the HP Live Network, a subscription service that tracks, triages, and analyzes the latest security vulnerability and regulatory compliance information available. See the figure "Security and Compliance Management in RCA" on page 52.

You can use the RCA Console to configure RCA to automatically download new security and compliance content from the HP Live Network on a periodic basis, rather than depending on a manual process. This content includes the following:

- Security and compliance scanners for client devices
- Detailed information about individual vulnerabilities, including descriptions, disclosure dates, severity levels, and available vendor patches or bulletins
- The current FDCC SCAP data stream available from NIST

The HP Live Network content is then pushed to the Configuration Server Database (CSDB) as deployable services, and managed client devices can be subsequently scanned for security and compliance issues according to the schedule and policy that you specify. This content is also pushed to the Reporting database.

The RCA Console provides dashboards that show the security and compliance status of your enterprise at a glance. It also provides a Patch Management Dashboard to help you quickly assess patch policy compliance across the enterprise. For more information, see "Using the Dashboards" on page 83.

Security and compliance scanning is supported for managed client devices with the following operating systems:

Platforms Supported

Scan Type	Supported Operating Systems
Vulnerability	Windows 2003, Windows 2008, Windows XP, Windows Vista, and Windows 7
Compliance	Windows XP, Windows Vista, and Windows 7
Security Tools	Windows XP, Windows Vista, Windows 7, Windows 8, Windows 2003, Windows 2008, and Windows 2008 R2

How HP Live Network Content is Updated

HP Live Network provides two types of security and compliance management content:

- Data – vulnerability definitions and SCAP data
- Scanners – a vulnerability scanner, a compliance scanner, and a security tools management scanner

In order to access the HP Live Network content, see "Accessing HP Live Network Content" on page 127.

When you update your RCA security and compliance management content – either from HP Live Network or from the file system – the following three things happen:

1. Both the updated scanners and data are copied into a temporary directory.
2. The data is pushed from the temporary directory to the Core database. This drives the detailed definition reports and primes the database for processing the collected scan results.
3. Both the data and scanners are loaded into the CSDB.

When a client device with a configured security policy subsequently makes a connection to the SECURITY Domain in the CSDB, the data and scanners are deployed to that client device. At this point, the client device will be scanned. The results of the scans are then sent to the Core database.

Security and Compliance Management in RCA

1. Updated security and compliance content is downloaded and analyzed by the HP Live Network team. The HP Live Network scanners are updated, if necessary (this is rare).
2. Updated security and compliance content, including the HP Live Network scanners, is downloaded by RCA from HP Live Network and published to the CSDB and the Core database.
3. Client devices are scanned for security and compliance problems by RCA.

The security and compliance content that is loaded into the CSDB includes both “service” definitions and “master” definitions. The service definitions are related to the scanning services and are deployed to the platform-specific agents for performing the scans. The master definitions are used when you move content from a test environment to a production environment (see "Move HP Live Network Content from a Test Environment to a Production Environment" on page 441).

For vulnerability scanning, the master definitions include the National Vulnerability Database (NVD) CVE definitions and the platform-specific Open Vulnerability Assessment Language (OVAL) definitions required by RCA. It is the combination of these two sets of definitions for each platform that enable RCA to create the Vulnerability Management reports.

For compliance scanning, the master definitions include the compliance benchmarks in SCAP format.

For security tools management scanning, there are no definitions. The scanner simply looks for the presence of all supported security tools and determines whether each tool is enabled. For anti-virus and anti-spyware tools, the scanner also determines when each tool last updated its definitions and when it last performed a full system scan.

Scanning Services in Detail

The Configuration Server Database (CSDB) contains a SECURITY Domain, which includes the services responsible for security and compliance scanning. When you install RCA, the following services are available in the SECURITY domain:

- <Discover FDCC 1.0 OS Compliance>
- <Sample Discover Vulnerabilities (Limited Edition)>
- <Vulnerability Management (Limited Edition)>

As you perform HP Live Network content updates, additional services become available. You can use these services to run security and compliance scans on an agent system and send the results back to the Reporting database.

Note: The security tools management scanning service is not available until you perform your first HP Live Network content update.

<Discover Security Tools>

Note: When you perform your first HP Live Network content update, the vulnerability scanner service is renamed:

<Discover Vulnerabilities>

The version of the scanner shipped with RCA is labeled “Limited Edition,” because it contains only a subset of the vulnerability definitions. This version works only on 32-bit platforms. When you perform your first update, the complete set of definitions known to RCA becomes available for scanning.

Although the name of the service changes, any entitlements that you have established do not change.

Viewing the Scanning Services

To view the scanning services:

1. Sign in to the RCA Console.
2. Click the **Management** tab.
3. In the left pane, click **Services**. The list of available CSDB domains opens.
4. In the left pane, click **Security**.

5. In the Catalog pane, click one of the Security services. For example:
   - SECURITY.ZSERVICE.DISCOVER_VULNERABILITY
   - SECURITY.ZSERVICE.DISCOVER_FDCC_1-0_OS
   - SECURITY.ZSERVICE.HP_SECTOOLS_MGMT_ALL_V001

   The Service Details window opens. For more information about services, see "Service Information" on page 145.

The CSDB initially contains an instance of PRIMARY.SECURITY.ZSERVICE called <Discover Vulnerabilities (Limited Edition)> for vulnerability scanning and another instance called <Discover FDCC 1.0 Compliance> for compliance scanning. As other benchmarks are added to the HP Live Network content, new instances will become available. After you perform your first HP Live Network update, the <Discover Security Tools> service is added.

The CSDB also contains an instance of PRIMARY.SECURITY.TIMER called Daily Vulnerability Scan, which determines when the vulnerability scanner is executed on target systems. Although they are separate instances, the <Discover Vulnerabilities> service has a connection to the Daily Vulnerability Scan timer.

Note: There is no built-in timer for compliance or security tools scanning. You must set up a DTM job to schedule regular compliance and security tools scans on your target devices. For more information, see "Create an RCA Job to Schedule or Trigger a Scan" on page 56. Alternatively, you can set up your own compliance scanning timer in the CSDB.

The following example is a snapshot of the Admin CSDB Editor showing a subset of the parameters for the Daily Vulnerability Scan service:

ZSCHDEF	Timer Parameter	DAILY(&ZSYSDATE,08:30:00,16:30:00)
ZSCHTYPE	Type [IMMEDIATE/DEFERRED]	DEFERRED
ZSCHFREQ	Frequency [PERIODIC/ONCE/RANDOM]	RANDOM

The timer does not directly invoke the scanner. When the timer expires, `radskman` performs a connect operation to the SECURITY Domain. This causes one of the following methods to be executed: ZCREATE, ZVERIFY, ZUPDATE, or ZREPAIR. When any of these methods is executed, the scanner is launched on the target system.

By default, the timer is configured to run daily at a randomly selected time between 08:30 and 16:30 local (system) time.

Note: You must explicitly entitle your target devices to the scanning services before you can use them. For more information, see "Schedule or Trigger a Scan" on next page.

Configuring Security and Compliance Management

See "Live Network" on page 305.

Common Security and Compliance Management Tasks

This section contains information about the following tasks:

Update HP Live Network Content

To update the HP Live Network content, see "Accessing HP Live Network Content" on page 127.

Schedule or Trigger a Scan

You can use the RCA Console to schedule a periodic vulnerability scan, compliance scan, or security tools scan – or any combination of the three – on a target device (or group of devices). You can also trigger an immediate scan. There are two steps required:

1. Entitle a device (or group of devices) to one or more of the Security services. When you install RCA, the following two services are available in the SECURITY domain:
   - <Discover FDCC 1.0 OS Compliance>
   - <Sample Discover Vulnerabilities (Limited Edition)>
   - <Vulnerability Management (Limited Edition)>

   As you perform HP Live Network content updates, additional services become available as new benchmarks are added. After you perform your first update, the vulnerability service is renamed, and the (Limited Edition) qualifier is deleted. The <Discover Security Tools> service also becomes available after your first content update.

   For more information, see "Entitle A Device for Scanning" on next page.
2. Schedule or trigger a scan from the RCA Console by creating a job using the Security Connect job action template. For more information, see "Create an RCA Job to Schedule or Trigger a Scan" on next page.

   You can also trigger an immediate scan on a single device by performing an agent connect operation from that target device to the SECURITY Domain in the CSDB. Scans are triggered whenever an agent connect operation from a properly entitled target device to the SECURITY Domain in the CSDB occurs. For more information, see "Start a Scan from a Target Device" on page 57.

For information about how RCA performs a scan, see "Scanning Services in Detail" on page 53.

Entitle A Device for Scanning

Before you can initiate a vulnerability, compliance, or security tools scan on a managed client device (or group of devices), you must properly entitle the pertinent devices to the required scanning services.

To entitle a device (or group of devices) for scanning:

1. On the Management tab, expand the zone containing the devices that you want to entitle.
2. In the left navigation tree, click **Devices** if you want to entitle a single device. If you want to entitle a group of devices, click **Group**.
3. From the shortcut menu for the device or group that you want to entitle, select **View/Edit Properties**. A new window Directory Object opens.
4. In the left navigation tree, click **Policies**.
5. Click the Launch Policy Management () button to open the Policy Management Wizard.
6. From the Service Domain list, select **Security**.
7. Select the box to the left of one or more of the Security services. The following services are available “out of the box” when you install RCA:
   - On the Management tab, expand the zone containing the devices that you want to entitle.
   - On the Management tab, expand the zone containing the devices that you want to entitle.
   - On the Management tab, expand the zone containing the devices that you want to entitle.

     The SECURITY.ZSERVICE.HP_SECTOOLS_MGMT_ALL_V001 service, for example, is available after your first update.
8. Click **Add to Selection**.
9. Click **Next**.
10. Under Policy Configuration, select **Allow**.
11. Under Priority, select the priority that you want the scans to have on the managed client device (or devices) when it runs.
12. Click **Next**.
13. Review the settings for the service(s). If you want to change a setting, click **Previous**. When you are ready to proceed, click **Commit**.
14. Click **Close** to close the Execution Status dialog box.

Create an RCA Job to Schedule or Trigger a Scan

To schedule or trigger a security or compliance scan on one or more target devices from the RCA Console, you must create a job for those devices. When a job created with the Security Connect job action template runs, all services in the SECURITY domain to which these devices are entitled are executed.

To create a job to schedule or trigger a scan:

1. On the Management tab, expand the zone containing the devices that you want to scan.
2. In the left navigation tree, click **Devices** if you want to scan a single device. If you want to scan a group of devices, click **Group**.
3. From the drop-down menu for the device or group that you want to scan, select **Create a Job** to open the job creation wizard.

   In the wizard, required fields are marked with an asterisk (*).
4. From the **Job Type** list, select either **DTM** or **Notify**.

   In a DTM job, the agents on the target devices connect to the RCA Core server to get a list of jobs and then execute those jobs when the job timers expire. A DTM job is most appropriate when you want to set up a regular scanning schedule for these devices.

   In a Notify job, the RCA Core server asks agent to perform the scan. A Notify job is most appropriate when you want certain target devices to perform a single scan at a specific time – or immediately.
5. Specify a **Name** for the job.
6. Specify a **Job Description**.
7. From the **Job Action Template** list, select **Security Connect**.
8. Click **Next**.
9. Specify the schedule for the job. See "Schedules" on page 150 for more information.

   DTM jobs can be executed either once or on a regular schedule. Notify jobs can only be executed once, so many of the schedule settings are disabled on this page of the wizard.
10. Click **Next**.
11. Review the settings for your job. To view the devices that will be scanned, click *n* **Target Device(s)**, where *n* is the number of devices to be scanned. If you want to change any settings, click **Previous**. When you are ready to proceed, click **Submit**.
12. Click **Close** to close the Execution Status dialog box.

For more information about RCA jobs, see "Managing Jobs" on page 148.

Start a Scan from a Target Device

To install the latest security and compliance management content and trigger an immediate scan on a client device, you can simply perform a client connect from that device to the SECURITY Domain in the CSDB.

To perform an agent connect to the SECURITY Domain:

On a managed client device, open a command line window, and execute the following command:

```
radskman dname=security,context=m,uid=$machine,cop=y
```

This command triggers an update to all the services in the SECURITY domain, including the security and compliance management services, to which the client device is entitled.

To trigger *only* a vulnerability scan, add the following parameter to the radskman command:

```
sname=DISCOVER_VULNERABILITY
```

To trigger *only* a compliance scan, add an `sname` parameter for the compliance service that you want to trigger to the `radskman` command. For example:

```
sname=DISCOVER_FDCC_1-0_OS
```

To trigger *only* a security tools scan, add the following parameter to the radskman command:

```
sname=HP_SECTOOLS_MGMT_ALL_V001
```

Remember to separate the `radskman` options with commas but *not* spaces.

Note: Uninstalling the management agent on a client device does not remove the scanners. To remove the security service, first remove the policy and then, perform a client connect to remove the service before you uninstall the management agent.

View the Results of a Scan or Update

You can use the reports available in the RCA Console to view the results of a vulnerability, compliance, or security tools scan. You can also view the status of HP Live Network content updates. You can filter the reports to see only the information that interests you. See "Using Reports" on page 205 for more information.

You can also use the dashboards to find summary information in either chart or grid format. See "Using the Dashboards" on page 83 for more information.

Find Vulnerability Remediation Information

By using the Vulnerability Management reports or dashboard, in many cases you can find a link to a vendor bulletin containing remediation information for a particular vulnerability. Sometimes this information is strictly advisory, and sometimes it includes a software patch for the affected application or operating system.

There are many ways to find the vendor bulletin for a specific vulnerability. The following procedures describe two simple ways to do this.

To find guided remediation information for a particular vulnerability:

1. On the Reporting tab, expand the list of Vulnerability Management reports.
2. Open a report that lists vulnerabilities, such as the Top Vulnerabilities report under Executive Summaries or Application Vulnerabilities report under Vulnerability Reports.
3. Click the **CVE ID** or **OVAL Definition** for a particular vulnerability. A new report, which includes patch and advisory information, opens for this vulnerability.

   Caution: If the status of a particular vulnerability is Unknown, and the CVSS score is null, be sure to investigate this vulnerability thoroughly by using the NVD, the CVE repository, and any other resources at your disposal. In this situation, RCA may be unable to provide the information that you need to make an informed decision about the issue.

4. Click the link in the **Bulletin** column if you want to go to the vendor's site.

Finding Guided Remediation Information for a Particular Device

To find guided remediation information for a particular device:

1. On the Reporting tab, expand the list of Vulnerability Management reports.
2. Under Device Reports, click **Scanned Devices**.
3. Click the Details ( ) icon for a particular device. The following reports open for this device:
   - Device Details
   - Device Vulnerability Details

     You can filter the Device Vulnerability Details report by Severity or OVAL Definition ID. See "Filtering Reports" on page 216 for more information.
4. Click the Details ( ) icon for a particular vulnerability. The following reports open:
   - Vulnerability Details
   - Vulnerability Remediation Details

     You can filter the Vulnerability Remediation Details report by Severity, Vendor, or CVE ID.
5. Click the link in the **Bulletin** column if you want to go to the vendor's site.

If the bulletin includes a patch, you can use the Patch Management features in the RCA Console to entitle the pertinent devices to that patch.

In addition to the methods described here, you can also drill down to a specific vulnerability report through certain "Vulnerability Management Dashboard" on page 91 panes.

Find Information about Compliance Failures

You can use the Compliance Management reports to drill down to detailed information about specific rules that failed on a particular device during the most recent compliance scan.

To view details for one of the most noncompliant devices:

1. On the Reporting tab, expand the list of Compliance Management reports.
2. Under Executive Summaries, click **Top SCAP Noncompliant Devices**.
3. Click the Switch to Detailed View ( ) icon to display the data in table format. Each row in the table corresponds to the most recent scan results for a particular compliance benchmark, version, and profile on a particular device.
4. Click a value in the **Rules Failed** column. A list of any compliance rules associated with this benchmark, version, and profile that failed for this device is displayed.

Viewing Details about the Compliance Test Results for Any Device

To view details about the compliance test results for any device:

1. On the Reporting tab, expand the list of Compliance Management reports.
2. Under Device Reports, click **Scanned Devices**.

   Each row in the table corresponds to the most recent scan results for a particular compliance benchmark, version, and profile on a particular device.

3. Click the Details ( ) icon in any row. The following reports open for the pertinent device:
   - Device Details – information about the device itself, including hardware, IP address, and operating system
   - Benchmarks by Device – most recent scan results for each benchmark, version, and profile tested on this device
4. In the Benchmarks by Device report, click a value in one of the following three columns:
   - **Rules Passed**

     A list of any compliance rules associated with this benchmark, version, and profile that passed for this device is displayed.
   - **Rules Failed**

     A list of any compliance rules associated with this benchmark, version, and profile that failed for this device is displayed.
   - **All Other Rule States**

     A list of compliance rules that neither failed nor passed for this device. This counter is incremented when a test returns one of the following codes:
     - ERROR
     - UNKNOWN
     - NOT_APPLICABLE
     - NOT_CHECKED
     - NOT_SELECTED
     - INFORMATIONAL
     - FIXED

In addition to the methods described here, you can also drill down to detailed information by using certain "Compliance Management Dashboard" on page 104 panes.

Find Information About Security Tools

RCA provides options to manage the security tools. The tools can be enabled or disabled, definitions can be updated, and scans initiated. The tools can be enabled selectively based on the Product Name, Product Version, or the Vendor.

RCA also gives you the ability to discover anti-virus, anti-spyware, and firewall tools running on your devices. The Security Tools Management dashboards and reports provide the following information:

Security Tools Management Dashboards and Reports Information

Security Tool	Information Available
Anti-virus	Name and version of the product installed Whether the tool is currently enabled Last time the tool performed a full system scan Last time the virus definitions were updated Specific version of the current definitions
Anti-spyware	Name and version of the product installed Whether the tool is currently enabled Last time the tool performed a full system scan Last time the spyware definitions were updated Specific version of the current definitions
Firewall	Name and version of the software firewall installed Whether the firewall is enabled Rules used by that firewall (applies to Windows XP SP2 or later service packs and Windows Vista firewalls only)

See the following topics for more detailed information:

- "Security Tools Management Dashboard" on page 113
- "Security Tools Management Reports" on page 212

Unlike compliance or vulnerability management, security tools management does not require you to download extra “definition” files. All of the knowledge about gathering information about security tools installed on a device is embedded in the scanner. As necessary, HP Live Network updates the scanner to support newly released security tools (anti-virus, anti-spyware, and firewalls).

Adding new Products for Security Tools Management

STM scanner uses the STMLibrary, an XML file that contains an entry for each security product supported by STM scanner. Each entry defines the product detection and data collection logic for the corresponding product. For the STM scanner to support new product, you need to add an entry for the corresponding security product into the STMLibrary.xml under the appropriate section.

The STM Library is updated periodically or on demand whenever a new security product support is required and uploaded to the HP Live Network. The STM Library is updated automatically in your RCA environment when you connect to HP Live Network. You can use the information given in this section and customize the STMLibrary.xml file if you have an urgent need to add new security products.

Customize the STMLibrary.xml File

Perform the following steps to customize the STMLibrary.xml file:

1. Open the RCA Administrator CSDB Editor window. The default user name and password to open the CSDB Editor window are admin and secret respectively.
2. Expand **Primary** -> **Security** -> **Application Packages**.
3. Expand **Security Tools Scanner for Windows** -> **Security Tools Scanner for Windows: <all>**.
4. Right-click the **Security Tools Scanner for Windows\security\sectools\scanner\STMLibrary.xml** option and select the **Edit this Component** option from the popup menu.
5. Select the notepad.exe and browse to any text editor to open the STMLibrary.xml file in a text editor. Click **OK**.
6. Edit the STMLibrary.xml file as per your requirement and save it to a temp location. Refer to the "STM Library Schema" below and "Sample STMLibrary.xml" on page 72 sections to know more about STM Library components.

Replace the STMLibrary.xml File

After you make the required changes in the STMLibrary.xml file, you must replace the existing STMLibrary.xml file in the CSDB:

Perform the following steps to replace the STMLibrary.xml file:

1. Open the RCA Administrator CSDB Editor window. The default user name and password to open the CSDB Editor window are admin and secret respectively.
2. Expand **Primary** -> **Security** -> **Application Packages**.
3. Expand **Security Tools Scanner for Windows** -> **Security Tools Scanner for Windows: <all>**.
4. Right-click the **Security Tools Scanner for Windows\security\sectools\scanner\STMLibrary.xml** option and select the **Replace Component Data** option from the popup menu.
5. Browse to your customized STMLibrary.xml file saved at temp location.
6. Click **Yes** to confirm the file replacement.

STM Library Schema

STM Library is an XML file, STMLibrary.xml, that contains an entry for each security product supported by STM scanner. Each entry defines the product detection and data collection logic for the corresponding product. For the STM scanner to support new products, you need to add an entry for the corresponding security product into the STMLibrary under the appropriate section.

The top level tag in the STMLibrary is <SecurityApplication>. The <SecurityAppliaction> tag contains three security types tags as follows each one for the supported security tools:

- <AntiViruses>
- <AntiSpywares>
- <Firewalls>

The security type tags listed above contain a respective product tag as listed below.

- <AntiVirus>
- <AntiSpyware>
- <Firewall>

The security type tags can contain multiple product tags. Each product tag represents a security product. The table below list various attributes of the product tags.

Attribute	Description
Name	Specifies the name of the product
Verison	Specifies the version of the product
WMIName	Specifies the name displayed in the WMI explorer for the product

Product Tags Definitions

The product tags contain the following definitions:

- <IsInstalled>: Detects whether a product is installed or not on a machine.
- <Detection>: Contains sub tags for the every piece of information that is gathered from machine if the product is installed on the machine.
- <Remediation>: Contains sub tags to remediate the product if found vulnerable.

The sub tags list for anti-virus and anti-spyware products are same. However, the sub tags for firewall products are different.

Detection sub tags for anti-virus and anti-spyware

The table below lists thesub tags used in the <Detection> definition for the <AntiVirus> and <AntiSpyware> product tags.

Sub tag	Description
<ProductName>	Name of the product
<ProductVersion>	Version of the product
<VendorName>	Vendor name
<DataFileDirectory>	Location where the definition files are stored
<DefinitionDate>	The latest definition date
<DefinitionVersion>	The latest definition version
<DefinitionVersion>	Version of the engine
<InstallDirectory>	Location where the product is installed on the machine

<IsFileSystemProtectionStatusEnforced>	Is the security product currently turned on
<IsFullSystemScanInProgress >	Is the scan currently running
<IsUpdateInProgress>	Is the update currently running
<LastFullSystemScan>	The last time of the full system scan

Remediation sub tags for anti-virus and anti-spyware

The table below lists the sub tags used in the <Remediation> definition for the <AntiVirus> and <AntiSpyware> product tags.

Sub tag	Description
<SystemProtectionTurnOn >	Turn on the product , if turned off
<SystemProtectionTurnOff>	Turn off the product, if turned on
<RunFullSystemScan>	Run the full system scan
<RunDefinitionUpdate>	Run the security product update

Detection sub tags for firewall

The table below lists the sub tags used in the <Detection> definition for the <Firewall> product tag.

Child tag	Description
<ProductName>	Name of the product
<ProductVersion>	Version of the product
<VendorName>	Vendor name
<Policies>	Rules defined for the firewall
<InstallDirectory>	Location where the product is installed on the machine
<IsEnabled>	Is firewall turned on
<IsProductAuthentic/>	Is the product authentic

Remediation sub tags for firewall

The table below lists the sub tags used in the <Remediation> definition for the <Firewall> product tags.

Child tag	Description
<FirewallProtectionTurnOn>	Turn on the firewall
<FirewallProtectionTurnOff>	Turn off the firewall

Operation Tags

The product tag definitions make use of the operation tags and logical tags to perform data collection or remediation activities. For example, the Registry operation tag retrieves and captures the name for a security product from registry.

Note: Whenever the Name attribute appears in an operation tag, the value defined for the Name attribute is considered as substitution variable. This substitution variable is scoped inside the product tag, which means a substitution variable for a particular product cannot be used for another product. To reference the substitution variable, the value defined for the corresponding Name attribute should be placed within the %% symbols. In addition to the substitution variable, the %% can be used to reference the value of system environment variables and Detection sub tags.

The STMLibrary.xml makes use of the following operation tags.

<Registry>

The Registry tag is used to perform read and write operations on Windows registry. The table below lists the attributes of the Registry tag and the possible values.

Attribute	Possible Value	Description
Name	Customer defined value	A variable to store the value data retrieved from registry. The Name attribute is used in conjunction with the Evaluate attribute. If the Evaluate attribute is used, the value retrieved from the registry is stored in the variable you defined in the Name attribute. Else, the value is not stored in the variable you defined in the Name attribute.
Verb	Exists	Used to check the presence of the particular registry key under the hive. If attribute is not specified, returns the value of the registry key. This is an optional attribute.
Key	Any key defined by the vendor	Represents a value name from registry
Reg	Complete path of registry hive	Complete path of registry hive
Arch	32 64 32|64 64|32	Read 32-bit registry Read 64-bit registry Read 32 bit registry and if value not found , read 64 bit Read 64 bit registry and if value not found , read 32 bit
FormatType	getDirName	Return the absolute path till the parent directory, if the value from registry is an absolute path.

Evaluate	False	Used along with the Name attribute. When used, the value retrieved from the registry is stored in the variable you specified in the Name attribute.
Type	REG_DWORD REG_SZ REG_BINARY	Read or write the DWORD value from/to registry Read or write the string value from/to registry Read or write the binary value from/to registry
value	Any REG_ DWORD/REG_ SZ/REG_ BINARY value	If used, signifies the write operation.

Example:

```
<Registry Name="EngineVersionMajor" Reg="HKEY_LOCAL_
MACHINE\SOFTWARE\McAfee\AVEngine" Key="EngineVersionMajor" Type="REG_
DWORD" Evaluate="false" />
```

<Process>

The Process tag is used to perform process related activities, such as creation of process and check whether the process is running. The table below lists the attributes of the Process tag and the possible values.

Attribute	Possible Values	Description
Path	Path of the executable	Specifies the path where the executable of the process resides.
Verb	Check	Checks whether the process is running
	Create	Creates the process
ProcessName	Process Name	Name of the process
CommandLine	Process Command Line	Command line of the process
WindowTitle	Window title	Window Title of the process, if it has a window

Example:

```
<Process Verb="Check" ProcessName="ccSvcHst.exe"
WindowTitle="LiveUpdate Status"/>
```

<RunCommand>

The RunCommand tag is used to execute commands that are executed by the vendor. The table below lists the attributes of the RunCommand tag and the possible values.

Attribute	Possible Values	Description
Name	Customer defined value	A variable to store the value returned upon command execution. The Name attribute is used in conjunction with the Evaluate attribute. If the Evaluate attribute is used, the output of the command execution is stored in the variable you defined in the Name attribute. Else, the output is not stored in the variable you defined in the Name attribute.
Path	Absolute path to the command executable	Specifies the absolute path to the command location
Command	Command name	Specifies the command to be executed
Args	Command arguments	Arguments to be passed along with the command, if any
Evaluate	False	Used along with the Name attribute. When used, the output of the command execution is stored in the variable you specified in the Name attribute.

Example:

```
<RunCommand Command="netsh" Args = "advfirewall set allprofiles state
on" Path = "%InstallDirectory%\" />
```

<FileProperties>

The FileProperties tag is use to read the file property values. The table below lists the attributes of the FileProperties tag and the possible values.

Attribute	Possible Values	Description
Path	Path of the file	Absolute path of file to which property value is to be retrieved

Value	Comments	Returns the comments specified in the file property
	InternalName	Returns the Internal name of the file specified in the file property
	ProductName	Returns the Product name specified in the file property
	CompanyName	Returns the Company name specified in the file property
	LegalCopyright	Returns the copy right information specified in the file property
	ProductVersion	Returns the version of product specified in the file property
	FileDescription	Returns the file description specified in the file property
	LegalTrademarks	Returns the Legal Trademarks specified in the file property
	PrivateBuild	Returns the Information about a private version of the file
	FileVersion	Returns the Version number of the file specified in the file property
	OriginalFilename	Returns the Original name of the file, not including a path
	CreationDate	Returns the Creation time of the file
	ModifiedDate	Returns the last modification time of the file
	AccessTime	Returns the last access time of the file.

Example:

```
<FileProperties Path="%DataFileDirectory%\NAVENG32.DLL"
Value="FileVersion" />
```

<FileRead>

The FileRead tag is used to read the file contents according to the attribute values. The table below lists the attributes of the FileRead tag and the possible values.

Attribute	Possible Values	Description
Path	Path of the file	The absolute path where the file resides
Line	Line number	Line number , If the line number is given as 3 , the 3rd line from the file is returned
PivotString	Any string value	Searches for first occurrence of pivot string, if found will return the string following it till an end of line is encountered
Evaluate	false	If Evaluate is set to false, the content read is not returned instead the content are stored for further reference.

Name	Customer defined value	A variable to store the content read. The Name attribute is used in conjunction with the Evaluate attribute. If the Evaluate attribute is used, the content read is stored in the variable you defined in the Name attribute. Else, the content is not stored in the variable you defined in the Name attribute.

Example:

```
<FileRead Name="Temp" Path="C:\temp\<anyfile.txt>" Line="3"
PivotString="xyz" Evaluate="false" />
```

<DirRead>

The DirRead tag is used to read directory and file names within a directory. The table below lists the attributes of the DirRead tag and the possible values.

Attribute	Possible Values	Description
Name	Customer defined value	A variable to store the output. The Name attribute is used in conjunction with the Evaluate attribute. If the Evaluate attribute is used, the output is stored in the variable you defined in the Name attribute. Else, the output is not stored in the variable you defined in the Name attribute.
Path	Absolute path of the directory	Absolute path of the directory to read
Verb	File	Returns the file names within the path specified, delimited by "|"
	Dir	Return the directories names within the path specified, delimited by "|"
Evaluate	False	If Evaluate is set to false, the output is stored in the variable you defined in the Name attribute for further reference.

Example:

```
<DirRead  Name="DIR" Evaluate="false" Path="%DataPAth%" Verb="dir" />
```

<XMLRead>

The XMLRead tag is used to read the value or attribute value of XML Node. The table below lists the attributes of the XMLRead tag and the possible values.

Attribute	Possible Values	Description
Name	Customer	A variable to store the output.

	defined variable	The Name attribute is used in conjunction with the Evaluate attribute. If the Evaluate attribute is used, the output is stored in the variable you defined in the Name attribute. Else, the output is not stored in the variable you defined in the Name attribute.
Evaluate	False	If Evaluate is set to false, the output is stored in the variable you defined in the Name attribute for further reference.
Node	Tag name	Specifies the XML tag where data is to be read
Attribute	Attribute name	This is an optional attribute. Retrieves value from the attribute name of the tag specified in the Node attribute.
Path	XML file location	Absolute path of the XML file

Example:

```
<XMLRead Name="Protect" Evaluate ="false"
Path="%InstallDirectory%settings\xyz.xml" Node="root/xyz/profile"
Attribute = "profile" />
```

<String>

The String tag is used to perform string operations. The table below lists the attributes of the String tag and the possible values.

Attribute	Possible Values	Description
Verb	Return	Returns the value in the Value attribute.
	Compare	Compares the value in the Value attribute with the Expected Value attribute and returns true if both values match, else returns false.
	NCompare	Compares the value in the Value attribute with the Expected Value attribute and returns false if both values match, else returns true.
value	Any string value	Stores the string value for operation specified in the Verb attribute, usage of substitution variable is allowed. It is also allowed to have value as a composition of substitution variables and normal strings. For example, %Major%.%Minor%
Evaluate	True	Used when the Value attribute has any substitution variable and needs substitution.
ExpectedValue	Any string value	Contains any string value. Used when the Verb is Compare or Ncompare.

Example:

```
<String Verb="Compare" value="%xyz%" ExpectedValue="abc"
Evaluate="true"/>
```

<Integer>

The Integer tag is used to perform integer operations. The table below lists the attributes of the String tag and the possible values.

Attribute	Possible Values	Description
Verb	Return	Returns the value in the Value attribute
	Compare	Compares the value in the Value attribute with the Expected Value attribute and returns true if both values match, else returns false.
value	Any integer value	Contains returned value or the value used for comparisons
ExpectedValue	Any integer value	Used when the verb is Compare or Ncompare

Example:

```
<Integer Verb="Compare" value="%DisableRealtimeMonitoring%"
ExpectedValue="0"/>
```

Logical Connector Tags

The logical connector tags are used to combine operation tags to accomplish a task. When logical connector tags are used, the value returned by the last tag in the logical connector tags is the return value. Nesting of logical connector tags is allowed. The logical connector tags work the same way logical operators work.

The logical connector tags available are

<And>

<Or>

<Not>

The <And> tag processes all the nodes placed within it, while the <Or> tag processes the nodes sequentially till it encounters a successful operation, after which it terminates.

Example snippet:

```
- <SystemProtectionTurnOff>
- <And>
```

```
<Registry Reg="HKEY_LOCAL_MACHINE\SOFTWARE\McAfee\SystemCore\VSCore\On
Access Scanner\BehaviourBlocking" Key="APEnabled" Type="REG_DWORD"
value="0" />

<Registry Reg="HKEY_LOCAL_MACHINE\SOFTWARE\McAfee\SystemCore\VSCore\On
Access Scanner\BehaviourBlocking" Key="BOPEnabled" Type="REG_DWORD"
value="0" />

</And>

</SystemProtectionTurnOff>

- <RunFullSystemScan>

- <Or>

<Process Verb="Create" Arch="64" ProcessName="scan64.exe"
Path="%InstallDirectory%x64\scan64.exe" />

<Process Verb="Create" Arch="32" ProcessName="scan32.exe"
Path="%InstallDirectory%scan32.exe" />

</Or>

</RunFullSystemScan>
```

Sample STMLibrary.xml

This section explain the STMLibrary.xml schema of one product for each security type—anti-virus, anti-sypware, and software firewall.

Anti-virus McAfee VirusScan Enterprise 8.8

McAfee VirusScan Enterprise 8.8 Schema

```
<?xml version="1.0" encoding="UTF-8"?>

<SecurityApplication>

<AntiVirus Name="McAfee VirusScan Enterprise 8.8" Version="8.8"
WMIName="McAfee VirusScan Enterprise">

- <IsInstalled>

<Registry Verb="Exists" Reg="HKEY_LOCAL_
MACHINE\SOFTWARE\McAfee\ePolicy Orchestrator\Application
Plugins\VIRUSCAN8800" Key="Install Path" Type="REG_SZ" />

</IsInstalled>

- <Detection>

- <ProductName>

<Registry Reg="HKEY_LOCAL_MACHINE\SOFTWARE\McAfee\ePolicy
Orchestrator\Application Plugins\VIRUSCAN8800" Key="Product Name"
Type="REG_SZ" />

</ProductName>
```

```
- <ProductVersion>

<Registry Reg="HKEY_LOCAL_MACHINE\SOFTWARE\McAfee\ePolicy
Orchestrator\Application Plugins\VIRUSCAN8800" Key="Version"
Type="REG_SZ" />

</ProductVersion>

- <VendorName>

<String Verb="Return" value="McAfee, Inc." />

</VendorName>

- <DataFileDirectory>

<Registry Reg="HKEY_LOCAL_MACHINE\SOFTWARE\McAfee\AVEngine" Key="DAT"
Type="REG_SZ" />

</DataFileDirectory>

- <DefinitionDate>

<Registry Reg="HKEY_LOCAL_MACHINE\SOFTWARE\McAfee\AVEngine"
Key="AVDatDate" Type="REG_SZ" />

</DefinitionDate>

- <DefinitionVersion>

<Registry Name="AVDatVersion" Reg="HKEY_LOCAL_
MACHINE\SOFTWARE\McAfee\AVEngine" Key="AVDatVersion" Type="REG_DWORD"
Evaluate="false" />

<Registry Name="AVDatVersionMinor" Reg="HKEY_LOCAL_
MACHINE\SOFTWARE\McAfee\AVEngine" Key="AVDatVersionMinor" Type="REG_
DWORD" Evaluate="false" />

<String Verb="Concat" value="%AVDatVersion%.%AVDatVersionMinor%"
Evaluate="true" />

</DefinitionVersion>

- <EngineVersion>

<Registry Name="EngineVersionMajor" Reg="HKEY_LOCAL_
MACHINE\SOFTWARE\McAfee\AVEngine" Key="EngineVersionMajor" Type="REG_
DWORD" Evaluate="false" />

<Registry Name="EngineVersionMinor" Reg="HKEY_LOCAL_
MACHINE\SOFTWARE\McAfee\AVEngine" Key="EngineVersionMinor" Type="REG_
DWORD" Evaluate="false" />

<String Verb="Concat"
value="%EngineVersionMajor%.%EngineVersionMinor%" Evaluate="true" />

</EngineVersion>

- <InstallDirectory>
```

```
<Registry Reg="HKEY_LOCAL_MACHINE\SOFTWARE\McAfee\ePolicy
Orchestrator\Application Plugins\VIRUSCAN8800" Key="Install Path"
Type="REG_SZ" />

</InstallDirectory>

- <IsFileSystemProtectionStatusEnforced>

- <Or>

<Registry Reg="HKEY_LOCAL_MACHINE\SOFTWARE\McAfee\SystemCore\VSCore\On
Access Scanner\BehaviourBlocking" Key="APEnabled" Type="REG_DWORD" />

<Registry Reg="HKEY_LOCAL_MACHINE\SOFTWARE\McAfee\SystemCore\VSCore\On
Access Scanner\BehaviourBlocking" Key="BOPPEnabled" Type="REG_DWORD"
/>

</Or>

</IsFileSystemProtectionStatusEnforced>

- <IsFullSystemScanInProgress>

- <Or>

<Process Verb="Check" ProcessName="scan32.exe"
Path="%InstallDirectory%scan32.exe" />

<Process Verb="Check" ProcessName="scan64.exe"
Path="%InstallDirectory%x64\scan64.exe" />

</Or>

</IsFullSystemScanInProgress>

- <IsUpdateInProgress>

<Process Verb="Check" ProcessName="MCUPDATE.EXE"
Path="%InstallDirectory%MCUPDATE.EXE" />

</IsUpdateInProgress>

<LastFullSystemScan />

</Detection>

- <Remediation>

- <SystemProtectionTurnOn>

- <And>

<Registry Reg="HKEY_LOCAL_MACHINE\SOFTWARE\McAfee\SystemCore\VSCore\On
Access Scanner\BehaviourBlocking" Key="APEnabled" Type="REG_DWORD"
value="1" />

<Registry Reg="HKEY_LOCAL_MACHINE\SOFTWARE\McAfee\SystemCore\VSCore\On
Access Scanner\BehaviourBlocking" Key="BOPEnabled" Type="REG_DWORD"
value="1" />

</And>

</SystemProtectionTurnOn>
```

```
- <SystemProtectionTurnOff>

- <And>

<Registry Reg="HKEY_LOCAL_MACHINE\SOFTWARE\McAfee\SystemCore\VSCore\On
Access Scanner\BehaviourBlocking" Key="APEnabled" Type="REG_DWORD"
value="0" />

<Registry Reg="HKEY_LOCAL_MACHINE\SOFTWARE\McAfee\SystemCore\VSCore\On
Access Scanner\BehaviourBlocking" Key="BOPEnabled" Type="REG_DWORD"
value="0" />

</And>

</SystemProtectionTurnOff>

- <RunFullSystemScan>

- <Or>

<Process Verb="Create" Arch="64" ProcessName="scan64.exe"
Path="%InstallDirectory%x64\scan64.exe" />

<Process Verb="Create" Arch="32" ProcessName="scan32.exe"
Path="%InstallDirectory%scan32.exe" />

</Or>

</RunFullSystemScan>

- <RunDefinitionUpdate>

<Process Verb="Create" ProcessName="MCUPDATE.EXE"
Path="%InstallDirectory%MCUPDATE.EXE" WaitToComplete="true" />

</RunDefinitionUpdate>

</Remediation>

</AntiVirus>

</SecurityApplication>
```

Anti-spyware McAfee VirusScan Enterprise 8.8

McAfee VirusScan Enterprise 8.8 Schema

```
<?xml version="1.0" encoding="UTF-8"?>

<SecurityApplication>

<AntiSpywares>

<AntiSpyware Name="McAfee VirusScan Enterprise 8.8" Version="8.8">

<IsInstalled>

<Registry Verb="Exists" Reg="HKEY_LOCAL_
MACHINE\SOFTWARE\McAfee\ePolicy Orchestrator\Application
Plugins\VIRUSCAN8800" Key="Install Path" Type="REG_SZ" />
```

```
</IsInstalled>

<Detection>

<ProductName>

<Registry Reg="HKEY_LOCAL_MACHINE\SOFTWARE\McAfee\ePolicy
Orchestrator\Application Plugins\VIRUSCAN8800" Key="Product Name"
Type="REG_SZ" />

</ProductName>

<ProductVersion>

<Registry Reg="HKEY_LOCAL_MACHINE\SOFTWARE\McAfee\ePolicy
Orchestrator\Application Plugins\VIRUSCAN8800" Key="Version"
Type="REG_SZ" />

</ProductVersion>

<VendorName>

<String Verb="Return" value="McAfee, Inc." />

</VendorName>

<DataFileDirectory>

<Registry Reg="HKEY_LOCAL_MACHINE\SOFTWARE\McAfee\AVEngine" Key="DAT"
Type="REG_SZ" />

</DataFileDirectory>

<DefinitionDate>

<Registry Reg="HKEY_LOCAL_MACHINE\SOFTWARE\McAfee\AVEngine"
Key="AVDatDate" Type="REG_SZ" />

</DefinitionDate>

<DefinitionVersion>

<Registry Name="AVDatVersion" Reg="HKEY_LOCAL_
MACHINE\SOFTWARE\McAfee\AVEngine" Key="AVDatVersion" Type="REG_DWORD"
Evaluate="false" />

<Registry Name="AVDatVersionMinor" Reg="HKEY_LOCAL_
MACHINE\SOFTWARE\McAfee\AVEngine" Key="AVDatVersionMinor" Type="REG_
DWORD" Evaluate="false" />

<String Verb="Concat" value="%AVDatVersion%.%AVDatVersionMinor%"
Evaluate="true"/>

</DefinitionVersion>

<EngineVersion>

<Registry Name="EngineVersionMajor" Reg="HKEY_LOCAL_
MACHINE\SOFTWARE\McAfee\AVEngine" Key="EngineVersionMajor" Type="REG_
DWORD" Evaluate="false" />
```

```
<Registry Name="EngineVersionMinor" Reg="HKEY_LOCAL_
MACHINE\SOFTWARE\McAfee\AVEngine" Key="EngineVersionMinor" Type="REG_
DWORD" Evaluate="false"/>

<String Verb="Concat"
value="%EngineVersionMajor%.%EngineVersionMinor%" Evaluate="true"/>

</EngineVersion>

<InstallDirectory>

<Registry Reg="HKEY_LOCAL_MACHINE\SOFTWARE\McAfee\ePolicy
Orchestrator\Application Plugins\VIRUSCAN8800" Key="Install Path"
Type="REG_SZ" />

</InstallDirectory>

<IsFileSystemProtectionStatusEnforced>

<Or>

<Registry Reg="HKEY_LOCAL_MACHINE\SOFTWARE\McAfee\SystemCore\VSCore\On
Access Scanner\BehaviourBlocking" Key="APEnabled" Type="REG_DWORD" />

<Registry Reg="HKEY_LOCAL_MACHINE\SOFTWARE\McAfee\SystemCore\VSCore\On
Access Scanner\BehaviourBlocking" Key="BOPPEnabled" Type="REG_DWORD"
/>

</Or>

</IsFileSystemProtectionStatusEnforced>

<IsFullSystemScanInProgress>

<Or>

<Process Verb="Check" ProcessName="scan32.exe"
Path="%InstallDirectory%scan32.exe" />

<Process Verb="Check" ProcessName="scan64.exe"
Path="%InstallDirectory%x64\scan64.exe" />

</Or>

</IsFullSystemScanInProgress>

<IsUpdateInProgress>

<Process Verb="Check" ProcessName="MCUPDATE.EXE"
Path="%InstallDirectory%MCUPDATE.EXE" />

</IsUpdateInProgress>

<LastFullSystemScan />

</Detection>


<Remediation>

<SystemProtectionTurnOn>
```

```
<And>

<Registry Reg="HKEY_LOCAL_MACHINE\SOFTWARE\McAfee\SystemCore\VSCore\On
Access Scanner\BehaviourBlocking" Key="APEnabled" Type="REG_DWORD"
value="1" />

<Registry Reg="HKEY_LOCAL_MACHINE\SOFTWARE\McAfee\SystemCore\VSCore\On
Access Scanner\BehaviourBlocking" Key="BOPEnabled" Type="REG_DWORD"
value="1" />

</And>

</SystemProtectionTurnOn>

<SystemProtectionTurnOff>

<And>

<Registry Reg="HKEY_LOCAL_MACHINE\SOFTWARE\McAfee\SystemCore\VSCore\On
Access Scanner\BehaviourBlocking" Key="APEnabled" Type="REG_DWORD"
value="0" />

<Registry Reg="HKEY_LOCAL_MACHINE\SOFTWARE\McAfee\SystemCore\VSCore\On
Access Scanner\BehaviourBlocking" Key="BOPEnabled" Type="REG_DWORD"
value="0" />

</And>

</SystemProtectionTurnOff>

<RunFullSystemScan>

<Or>

<Process Verb="Create" Arch="64" ProcessName="scan64.exe"
Path="%InstallDirectory%x64\scan64.exe"  />

<Process Verb="Create" Arch="32" ProcessName="scan32.exe"
Path="%InstallDirectory%scan32.exe"  />

</Or>

</RunFullSystemScan>

<RunDefinitionUpdate>

<Process Verb="Create" ProcessName="MCUPDATE.EXE"
Path="%InstallDirectory%MCUPDATE.EXE" WaitToComplete="true" />

</RunDefinitionUpdate>

</Remediation>

</AntiSpyware>

</AntiSpywares>

</SecurityApplication>
```

Microsoft Windows Firewall 7

Microsoft Windows Firewall 7 Schema

```
<?xml version="1.0" encoding="UTF-8"?>

<SecurityApplication>

<Firewalls>

<Firewall Name="Microsoft Windows Firewall" Version="7">

<IsInstalled>

<Registry Verb="Exists" Reg="HKEY_LOCAL_
MACHINE\SYSTEM\CurrentControlSet\services\SharedAccess"
Key="ImagePath" Type="REG_SZ" />

</IsInstalled>

<Detection>

<ProductName>

<String Verb="Return" value="Microsoft Windows Firewall" />

</ProductName>

<ProductVersion>

<Registry Name="ServiceDll" Reg="HKEY_LOCAL_
MACHINE\SYSTEM\CurrentControlSet\services\SharedAccess\Parameters"
Key="ServiceDll" Type="REG_SZ" Evaluate="false"/>

<FileProperties Path="%ServiceDll%" Value="ProductVersion" />

</ProductVersion>

<VendorName>

<String Verb="Return" value="Microsoft Corp." />

</VendorName>

<InstallDirectory>

<Registry Reg="HKEY_LOCAL_
MACHINE\SYSTEM\CurrentControlSet\services\SharedAccess\Parameters"
Key="ServiceDll" Type="REG_SZ" FormatType="getDirName"/>

</InstallDirectory>

<Policies>

<RunCommand Name="WINFW" Command="netsh" Args="advfirewall firewall
show rule all" Path = "%InstallDirectory%\" Evaluate="False"
Parse="FirewallRule"/>

<String Verb="Return" value="%WINFW%" Evaluate="true"/>

</Policies>
```

```
<IsEnabled>

<Registry Name="StandardProfile" Reg="HKEY_LOCAL_
MACHINE\SY-
STEM\Cu-
rrentControlSet\services\SharedAccess\Parameters\FirewallPolicy\StandardProfile"
 Key="EnableFirewall" Type="REG_DWORD" Evaluate="false" />

<Registry Name="DomainProfile" Reg="HKEY_LOCAL_
MACHINE\SY-
STEM\Cu-
rrentControlSet\services\SharedAccess\Parameters\FirewallPolicy\DomainProfile"
 Key="EnableFirewall" Type="REG_DWORD" Evaluate="false" />

<Registry Name="PublicProfile" Reg="HKEY_LOCAL_
MACHINE\SY-
STEM\Cu-
rrentControlSet\services\SharedAccess\Parameters\FirewallPolicy\PublicProfile"
 Key="EnableFirewall" Type="REG_DWORD" Evaluate="false" />

<Or>

<Integer Verb="Return" value="%StandardProfile%"/>

<Integer Verb="Return" value="%DomainProfile%"/>

<Integer Verb="Return" value="%PublicProfile%"/>

</Or>

</IsEnabled>

<IsProductAuthentic>

</IsProductAuthentic>

</Detection>


<Remediation>

<FirewallProtectionTurnOn>

<RunCommand Command="netsh" Args = "advfirewall set allprofiles state
on" Path = "%InstallDirectory%\" />

</FirewallProtectionTurnOn>

<FirewallProtectionTurnOff>

<RunCommand Command="netsh" Args = "advfirewall set allprofiles state
off" Path = "%InstallDirectory%\" />

</FirewallProtectionTurnOff>

</Remediation>

</Firewall>

</Firewalls>
```

```
</SecurityApplication>
```

More Information about Security and Compliance Management

The following sections contain information about configuring and viewing security and compliance management information in the RCA Console:

- "Using the Dashboards" on page 83
- "Using Reports" on page 205
- "Live Network" on page 305

Visit the following web sites to learn more about security and compliance management:

- http://cve.mitre.org
- http://nvd.nist.gov
- http://nvd.nist.gov/scap.cfm
- http://oval.mitre.org
- http://www.us-cert.gov

Chapter 4

Using the Dashboards

The Dashboards enable you to quickly assess the status of your environment in various ways. The Dashboards offer a visual representation of certain types of information provided in the Reporting area.

This chapter includes the following topics:

Dashboard Overview

The RCA Console includes dashboards that enable you to view and assess the status of your enterprise at a glance:

- The "RCA Operations Dashboard" on page 87 shows you how much work is being done by the RCA infrastructure.
- The "Vulnerability Management Dashboard" on page 91 shows you information about any publicly known security vulnerabilities that are detected on the scanned devices in your enterprise.
- The "Compliance Management Dashboard" on page 104 shows you how well managed client devices in your environment comply with predefined policies based on established regulations and standards, such as the Federal Desktop Core Configuration (FDCC).
- The "Security Tools Management Dashboard" on page 113 shows you information about the anti-spyware, anti-virus, and software firewall products installed on the managed client devices in your enterprise.
- The "Patch Management Dashboard" on page 119 shows you information about any patch vulnerabilities that are detected on the devices in your network

Each dashboard includes two views:

Types of Dashboard Views

Type	Description
Executive View	High-level summaries designed for managers. This include historical information about the enterprise.

Type	Description
Operational View	Detailed information designed for people who use RCA in their day to day activities. This includes information about specific devices, subnets, vulnerabilities, and specific compliance or security tool issues.

Each view includes a number of information panes. You can configure RCA to show you all or a subset of these panes. See "Dashboards" on page 340 for more information.

Each dashboard also includes a home page with summary statistics and links to related reports. When you click one of these links, a separate browser window opens, and RCA displays the report.

In most dashboard panes, you can display the information in either a chart or grid format. In the grid view, the current sort parameter is indicated by the ▼ icon in the column heading. To change the sort parameter, click a different column heading. To reverse the sort order, click the column heading again. To move a column, click the background in the column heading cell, and drag the column to a new location.

In most dashboard panes, you can rest the cursor on a colored area on a bar or pie chart—or a data point on a line chart—to see additional information. Most panes also enable you to drill down into reports that provide more detailed information.

The time stamp in the lower left corner of each pane indicates when the data in the pane was most recently refreshed from its source.

Time Stamp

Note: The dashboard panes use your local time zone to display the date and time. The reports available on the Reporting tab use Greenwich Mean Time (GMT) by default. Individual report packs, however, can be configured to use either GMT or local time.

If there is no security and compliance management data in the Reporting database—for example, before the first scan has been performed—the dashboard panes do not display any data.
You can perform the following actions in the dashboard panes:

Dashboard Pane Actions

Icon	Description
	Display the information in chart format.
	Display the information in grid format.
	Display the legend for this chart.
	Refreshes the data from its source. Click the refresh icon in an individual pane to refresh the data for that pane. Click the refresh icon in the upper right corner of the dashboard to refresh all panes. The dashboard panes are not automatically refreshed if your RCA Console session times out. You must manually refresh the panes after you sign in again if you want to get the latest information from the database.

Icon	Description
	Resets the appearance of all panes within the dashboard to their factory default settings.
	For panes containing RCA data, show the corresponding report. For panes containing information from external web sites or RSS feeds, go to the source web site.
	Opens a “quick help” box or tool tip. Click this button once to see a brief description of the dashboard pane. Click it again to hide the quick help text.
	Opens a context sensitive online help topic for this pane. This control is only available when the quick help text is visible.
	Minimize a dashboard pane.
	Maximize a dashboard pane.
	After maximizing, restore the pane to its original size.

If you minimize a dashboard pane, the other panes will expand in size to fill the dashboard window. Likewise, if you maximize a dashboard pane, the other panes will be covered. To restore a pane that has been minimized, click the gray button containing its name at the bottom of the dashboard. In this example, the 24 Hour Service Events pane has been minimized:

Button that Restores a Dashboard Pane

You can drag and drop the panes to rearrange them within the dashboard window. You cannot, however, drag a pane outside of the dashboard.

When you customize the appearance of a dashboard by resizing or rearranging its panes—or switching between the chart and grid view in one or more panes—this customization is applied the next time you sign in to the RCA Console. The dashboard layout settings are stored as a local Flash shared object (like a browser cookie) on your computer. The settings are saved unless you explicitly delete them.

Note: If you press the **F5** function key while viewing one of the dashboards, you will return to that dashboard page after your browser reloads the RCA Console.

In some grid views, trend indicators show you how a particular parameter is trending since the previous scan:

Trend Indicators

Icon	Color	Direction	Description
	Red	Up	Parameter has increased; the trend is bad.
	Green	Up	Parameter has increased; the trend is good.
	Red	Down	Parameter has decreased; the trend is bad.
	Green	Down	Parameter has decreased; the trend is good.

For example, in the "Vulnerability Impact by Severity (pie chart)" on page 92, if the number of High severity vulnerabilities has increased, a red arrow pointing up is displayed. If the number High severity vulnerability has decreased, a green arrow pointing down is displayed.

To assess the trend, RCA summarizes each day's data at midnight local time. For this reason, the data for the current day is incomplete. The trending indicator is based on the previous two days.

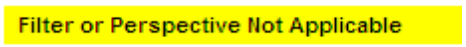
Dashboard Perspectives

Perspectives enable you to limit the information displayed in the dashboard panes to certain types of devices. The following perspectives are available by default:

- Global – All devices (no filter is applied).
- Mobile (Laptops) – Laptops and other mobile computing devices. This includes all devices with the following chassis types:
  - Portable
  - Laptop
  - Notebook
- Virtual – Virtual devices. This includes all devices whose Vendor and Model properties indicate VMware or Xen (including Citrix).
- SmartPhones/Tablets: This includes smartphones or tablets running on Android or iOS operating systems.

To apply a perspective, select it in the Perspectives box in the upper left corner of the RCA Core Console.

Because of the nature of the data that they display, certain dashboard panes are not affected by the perspectives. When you select either the Mobile or Virtual perspective, a highlighted message appears at the top of any pane that is *not* affected:



Panes that are not affected are also outlined in orange.

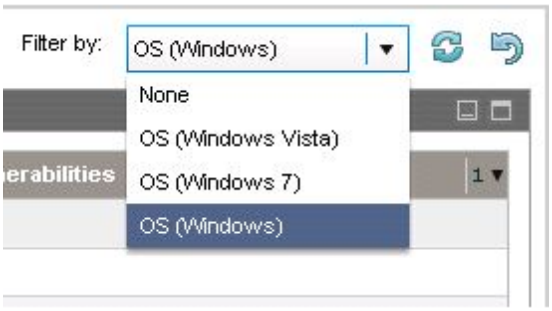
The following dashboard panes are not affected by perspectives:

- "Historical Vulnerability Assessment" on page 94
- "Historical Compliance Assessment" on page 108
- "Microsoft Security Bulletins" on page 124
- "HP Live Network Announcements" on page 98
- "HP Live Network Patch Manager Announcements" on page 122

When you select a perspective, it is applied to all the dashboard panes in the RCA Console except those that indicate, **Filter or Perspective Not Applicable**, as shown above. You cannot apply a perspective to an individual dashboard pane.

Dashboard Filters

Another way to limit the amount of data displayed in the dashboards is to use a custom Reporting filter that you have created. You can select a filter from the drop-down menu in the upper right corner of the dashboard:



RCA Operations Dashboard

This dashboard shows you the work that the RCA infrastructure is doing in your enterprise. It shows you three things:

- The number of RCA client connections
- The number of service events (installs, uninstalls, updates, repairs, and verifies) that have occurred
- The types of operations (OS, security, patch or application) that RCA has performed

The client connection and service event metrics are reported in two time frames. The Executive View shows the last 12 months. The Operational View shows the last 24 hours. Both views contain the following information panes:

- "Client Connections" below
- "Service Events" on page 89

The Executive View also includes the following pane:

- "12 Month Service Events by Domain" on page 90

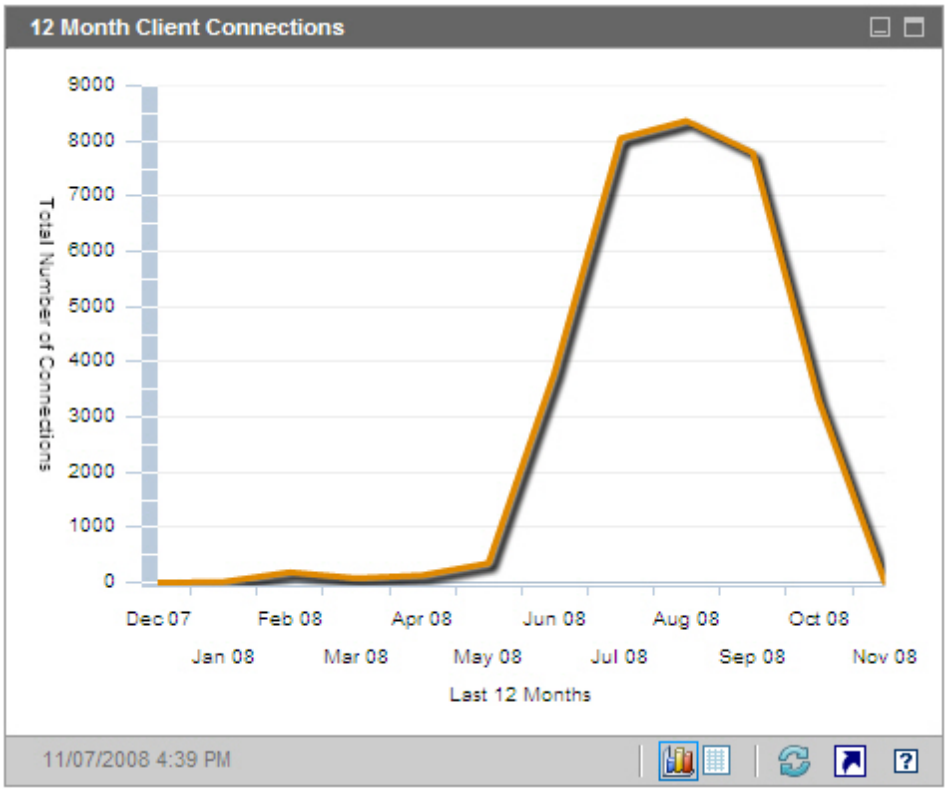
All of these panes are visible by default. You can configure the dashboard to show or hide any of these panes. For more information, see "Dashboards" on page 340.

Note: When you click RCA Operations in the left navigation pane, the RCA Operations home page is displayed. This page contains statistics and links to pertinent reports.

Client Connections

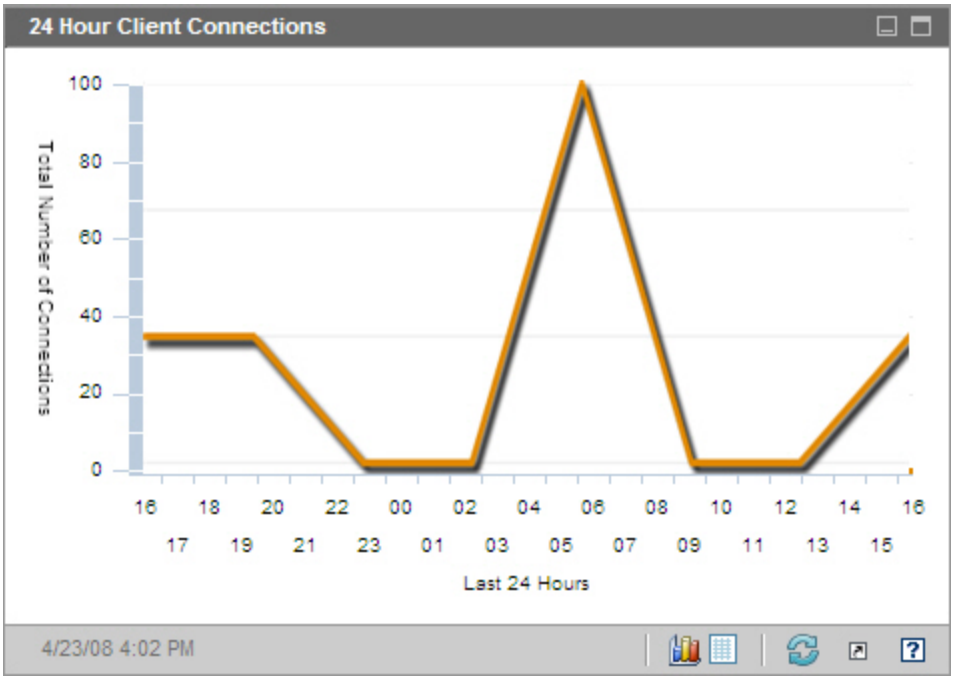
The chart view of this pane shows you the number of RCA agent client connections that have occurred over the last twelve months (Executive View) or 24 hours (Operational View). When you rest the cursor on a data point, you can see the total number of connections for that month (Executive View) or hour (Operational View).

12 Month Client Connections



The grid view for this pane lists the total number of client connections completed during each of the last twelve months.

24 Hour Client Connections



Note: The dashboard panes use your local time zone to display the date and time. The reports available on the Reporting tab use Greenwich Mean Time (GMT) by default. Individual report packs, however, can be configured to use either GMT or local time.

The grid view for this pane lists the number of client connections completed during each of the last 24 hours.

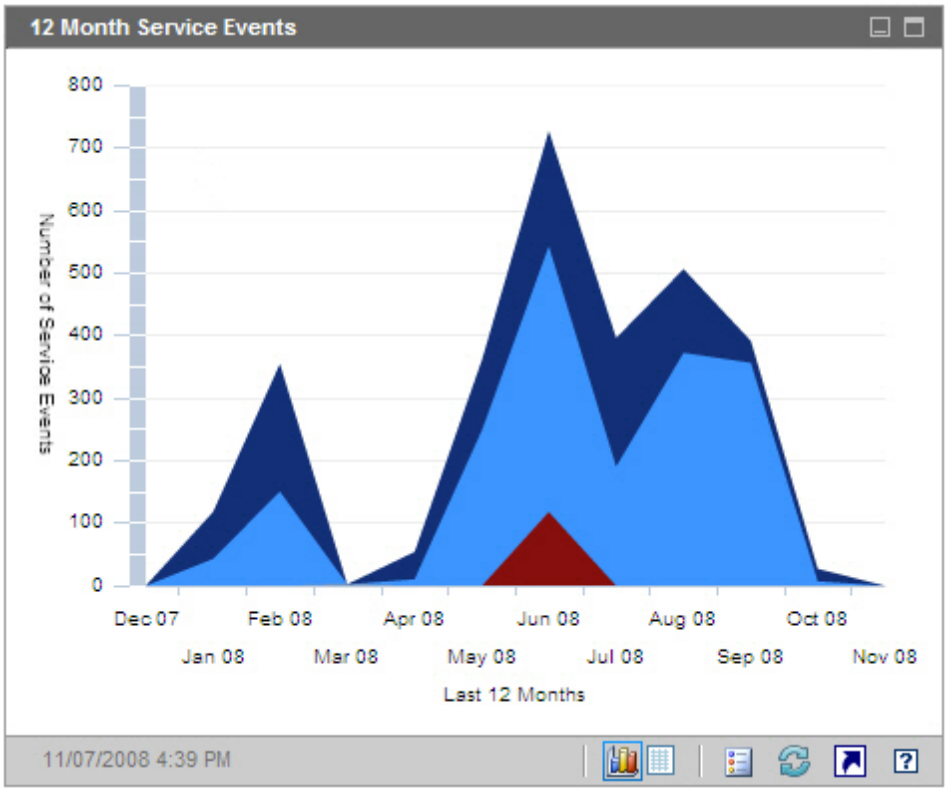
Service Events

The chart view of this pane shows the number of service events that RCA has completed over the last twelve months (Executive View) or 24 hours (Operational View) on the client devices in your enterprise. These include the number of applications that RCA has:

- Installed
- Uninstalled
- Updated
- Repaired
- Verified

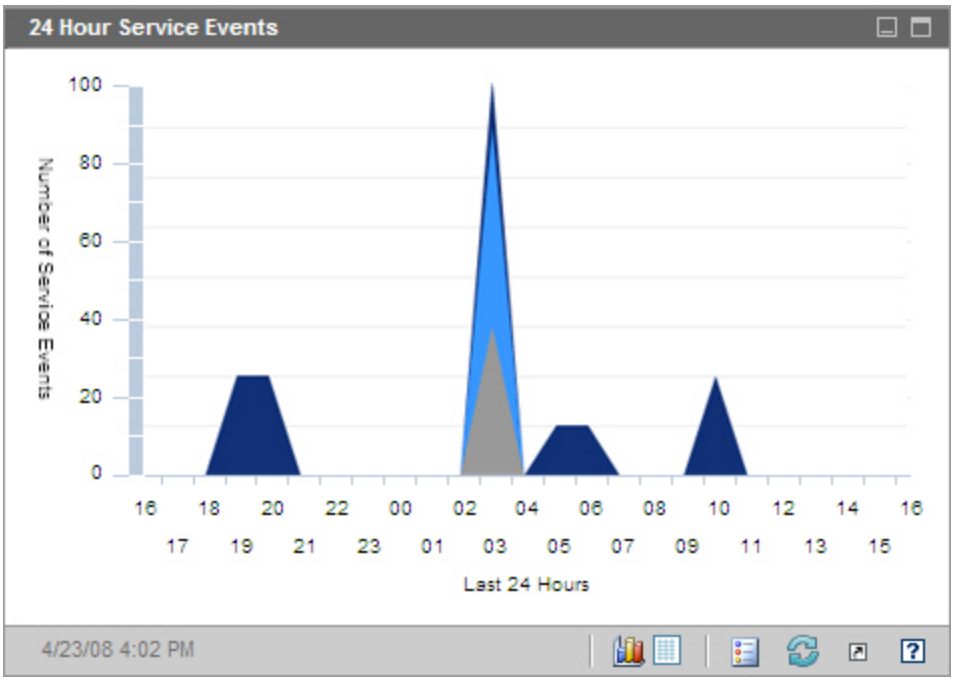
When you rest the cursor on a data point, you can see the number of service events that were completed during a particular month or hour.

12 Month Service Events



The grid view for this pane lists the number of each type of service event that was completed by RCA during each of the last twelve months.

24 Hour Service Events



Note: The dashboard panes use your local time zone to display the date and time. The reports available on the Reporting tab use Greenwich Mean Time (GMT) by default. Individual report packs, however, can be configured to use either GMT or local time.

The grid view for this pane lists the number of each type of service event that was initiated by RCA during each of the last 24 hours.

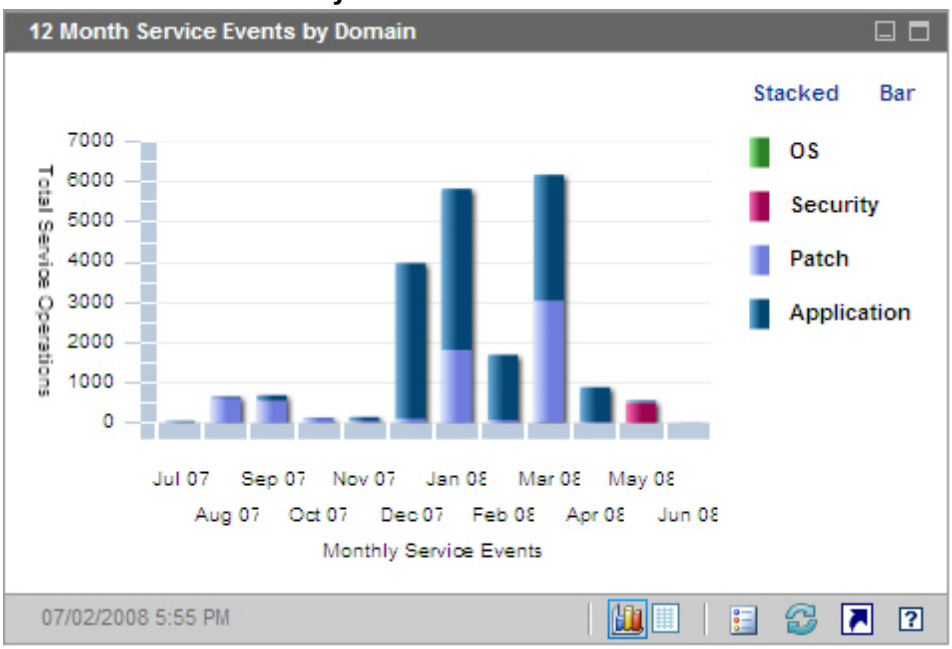
12 Month Service Events by Domain

The chart view of this pane shows you how many of each of the following services that RCA performed during each of the last 12 months:

- Operating system (OS) operations
- Security operations
- Patch operations
- Application operations

If fewer than 12 months of data are available, the chart will contain fewer bars.

12 Month Service Events by Domain



You can view the data presented in this chart in two ways.

- Stacked – the different types of service events are stacked vertically in a single bar for each month, as shown here.
- Bar – a separate bar for each type of service event is shown for each month.

The grid view lists the number of each type of service that RCA performed during each of the last twelve months.

Vulnerability Management Dashboard

RCA has the ability to collect security vulnerability information for each managed client system in your enterprise. This information is then aggregated and displayed in the Vulnerability Management dashboard.

RCA is integrated with HP Live Network, which provides updated vulnerability definitions and an executable client scanner.

Note: For a list of common vulnerability management terms used throughout the Vulnerability Management dashboard and reports, see "Security and Compliance Management" on page 45.

RCA uses the Common Vulnerability Scoring System (CVSS) Base score to place each client device in the enterprise into one of the following severity categories:

Severity Categories

Icon	Category	Highest CVSS Base Score for this Device
	High	Between 7.0 and 10

Icon	Category	Highest CVSS Base Score for this Device
	Medium	Between 4.0 and 6.9
	Low	Less than 3.9
	No Vulnerabilities	No vulnerabilities detected
	Unknown	No data available for this device

The highest severity vulnerability present on a device determines its category. If a device has at least one High severity vulnerability, its category is High. If a device has no High severity vulnerabilities but has at least one Medium severity vulnerability, its category is Medium, and so on.

Caution: If the severity of a particular vulnerability is Unknown, and the CVSS score is null, be sure to investigate this vulnerability thoroughly by using the NVD, the CVE repository, and any other resources at your disposal. In this situation, RCA may be unable to provide the information that you need to make an informed decision about the issue.

The Vulnerability Management dashboard Executive View includes the following four information panes:

- "Vulnerability Impact by Severity (pie chart)" below
- "Vulnerability Impact by Severity (bar chart)" on page 99
- "Vulnerability Impact" on page 95
- "Historical Vulnerability Assessment" on page 94

The Operational View includes the following four information panes:

- "HP Live Network Announcements" on page 98
- "Most Vulnerable Devices" on page 100
- "Most Vulnerable Subnets" on page 102
- "Top Vulnerabilities" on page 103

You can configure the dashboard to show or hide any of these panes. See "Dashboards" on page 340.

Note: When you click Vulnerability Management in the left navigation pane on the Home tab, the Vulnerability Management home page is displayed. This page contains statistics and links to pertinent reports.

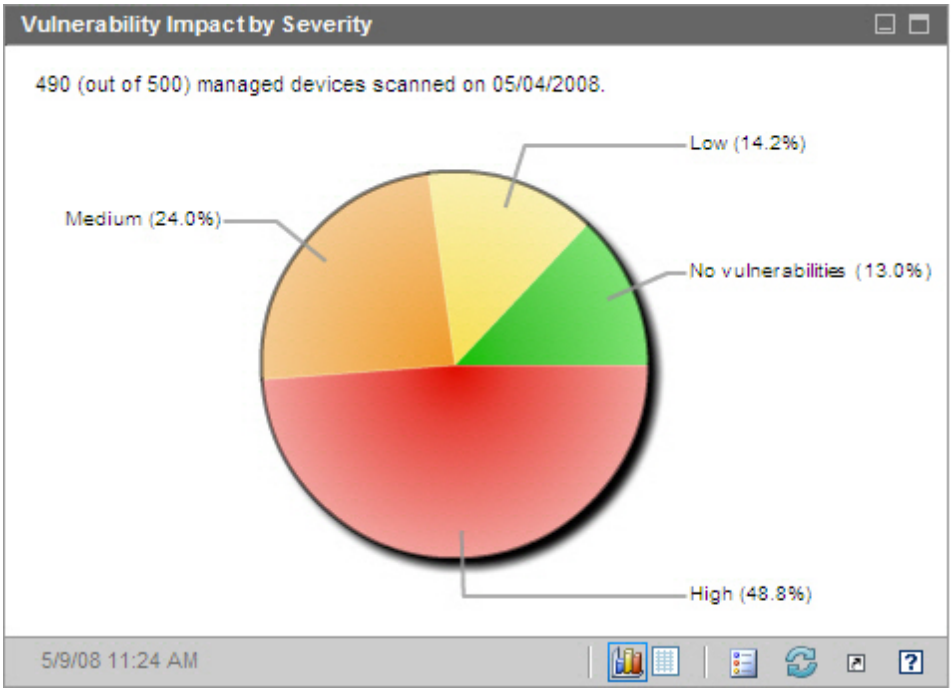
Vulnerability Impact by Severity (pie chart)

The chart view for this pane shows you the percentage of scanned devices in the enterprise that fall into each of the following five categories based on the highest severity vulnerability detected on each device:

- High (red)
- Medium (orange)
- Low (yellow)
- No Vulnerabilities (green)
- Unknown (blue)

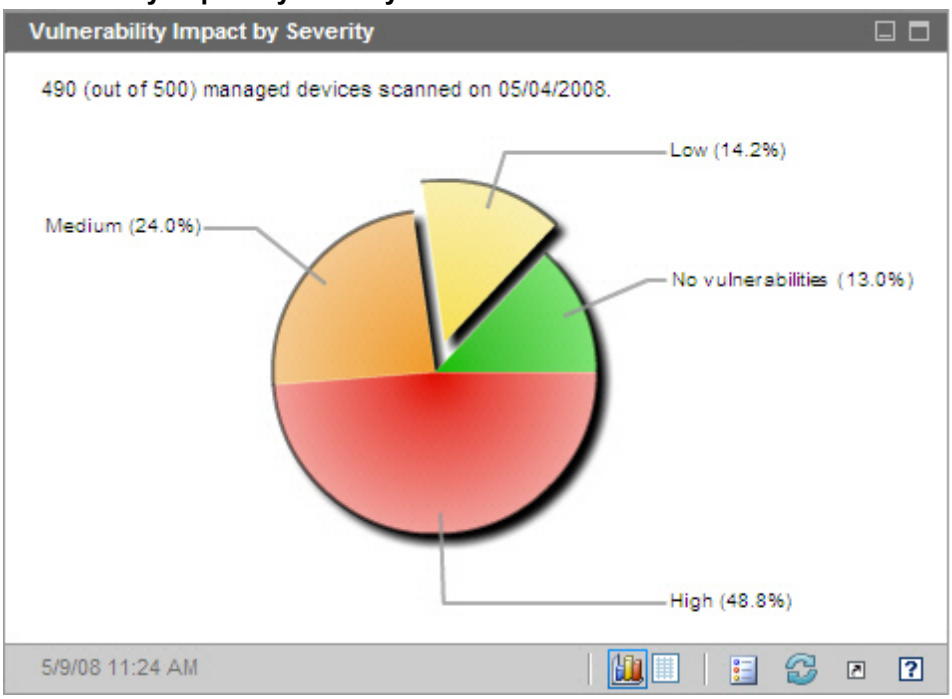
To see the number of devices in each severity category, rest the cursor on the corresponding sector of the pie chart.

Vulnerability Impact by Severity



If you click one of the wedges in the pie chart, a new browser window opens, and a detailed report is displayed. The report is filtered based on the severity category corresponding to the wedge that you clicked. After you click a wedge and open a report, that wedge separates from the rest of the pie, as shown here:

Vulnerability Impact by Severity



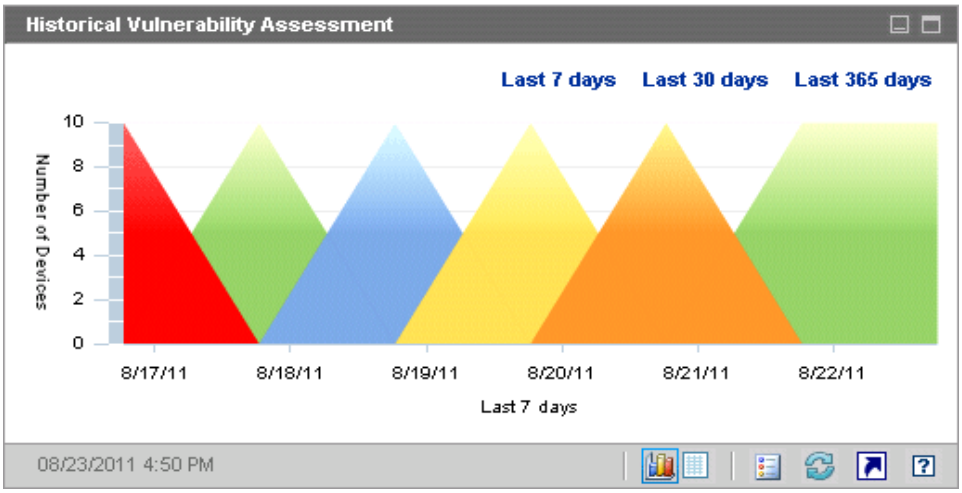
The grid view shows you how many devices fall into each severity category and whether the device count for that category has increased, decreased, or stayed the same since the previous vulnerability scan.

Historical Vulnerability Assessment

This pane shows how the information displayed in the Vulnerability Impact by Severity panes changes over time.

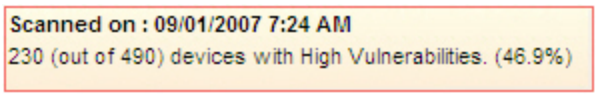
The chart view of this pane shows you the average aggregate risk in your enterprise over a period of time. The vertical axis represents the number of devices. The horizontal axis represents time. You can view data for the last seven days, 30 days, or 365 days. Each colored region represents the number of devices in each of the severity categories: High (red), Medium (orange), Low (yellow), No Vulnerabilities (green), and Unknown (blue).

Historical Vulnerability Assessment



When you rest the cursor on a data point that lies on a line between colored regions, a circle highlighting that data point appears, and a tool tip shows you the number and percentage of devices in that vulnerability category on that day.

Tool Tip



In this example, 46.9% of the 490 devices scanned had at least one high severity vulnerability. The tool tip always displays information from the last vulnerability scan performed. Typically a scan is performed daily. If a scan was not performed for several days, the graph will be flat for those days, and the information in the tool tip will not change.

The tool tips always show you when the most recent vulnerability scan was performed. As you analyze your vulnerability data, be sure to check the date of the most recent scan.

Note that the appearance of the circle that appears around the data point when a tool tip is displayed will vary depending on the color of the region underneath the circle.

The grid view for this pane lists of the number of devices in each risk category on each day during the specified time period. The grid also indicates the date on which the environment was last scanned.

Although the chart does not contain a band for devices in the Unknown severity category, the grid view includes a column for these devices.

Vulnerability Impact

The chart view of this pane shows you the relative numbers of devices that are affected by a particular vulnerability. There is one circle per vulnerability, and the size of the circles indicates the number of devices affected. The color of each circle represents the severity of the vulnerability: High (red), Medium (orange), Low (yellow), and Unknown (blue).

The vertical axis represents severity as measured by the CVSS Base score; the horizontal axis represents time since the vulnerability was first published in the National Vulnerability Database (NVD). For example:

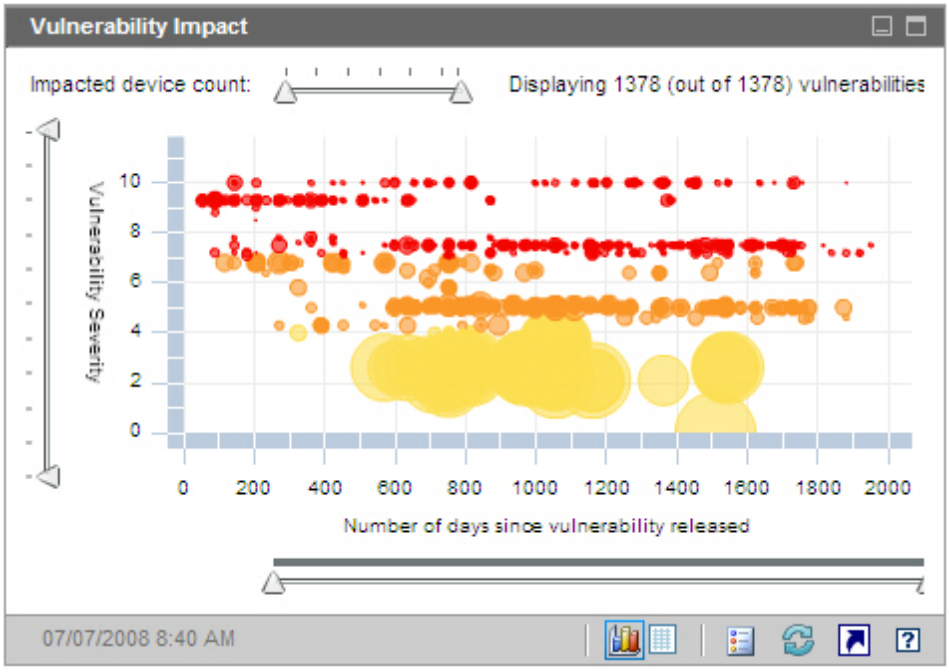
- Large red circles in the upper right portion of the chart represent severe vulnerabilities that affect a large number of devices and have been published for a relatively long time.
- Small yellow circles in the lower left portion represent issues that are of low severity, affect a smaller number of devices, and were published in the NVD relatively recently.
- An ideal chart would have no red bubbles in the upper right corner. This would imply that severe vulnerabilities are dealt with quickly.

When you rest your cursor on a particular circle, a tool tip shows you the following information about the vulnerability that the circle represents:

- Severity category (high, medium or low)
- CVE identifier and title
- Publication date
- Number of devices affected
- Total number of scanned devices

If you click one of the circles in the chart, a new browser window opens, and a detailed report is displayed. The report shows the number of devices affected by this vulnerability and information about the vulnerability itself. To obtain a list of affected devices, click the number of Devices Impacted in the report.

Vulnerability Impact



You can use the three sliders to zoom in on a particular data region. The sliders determine how many circles appear in the chart and the scale represented by each axis.

- The horizontal slider at the top of the pane enables you to specify an effect range as measured by the number of managed devices affected by a particular vulnerability.

- The vertical slider on the left enables you to zoom in on a severity range as measured by the CVSS base score.
- The horizontal slider at the bottom of the pane enables you to specify the age of the vulnerabilities displayed. The age is based on the date when a vulnerability was originally published; it does not reflect subsequent modifications to the vulnerability definition.

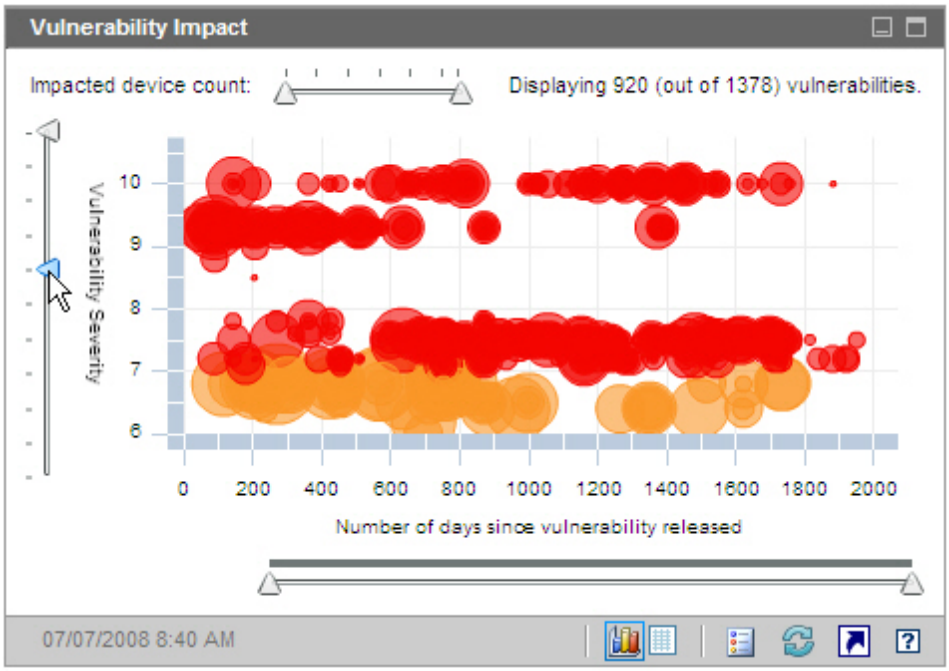
  By default, the age span displayed is 45 days. You can specify this default value when you configure the Vulnerability Management dashboard. See "Dashboards" on page 340.

When the triangles (△) are at opposite ends of a slider, the entire data range is visible. When the triangles are closer together, only a subset is visible. You can adjust both triangles on each slider.

If no data appear in the chart, move the triangles to the opposite ends of all three sliders to expose the entire data range.

In the following example, vulnerabilities with a CVSS base score of 6 or greater are shown:

CVSS of 6 or Greater



In the following example, only vulnerabilities with CVSS base scores of 6 or greater that were released during the most recent 500 days are shown:

Most Recent 500 Days

The grid view for this pane provides the following information for each vulnerability detected:

- OVAL ID – OVAL identifier for this vulnerability
- CVE ID – CVE identifier for this vulnerability
- Description – from the OVAL definition
- Severity – High, Medium, or Low severity icon and CVSS base score for this vulnerability
- Age – Number of days since this vulnerability was published in the NVD
- Device Count – number of client devices affected

The grid view displays data corresponding to the data displayed in the chart at the time the grid view is selected. If the sliders on the chart are adjusted to show a subset of the data, only this subset will appear in the grid view.

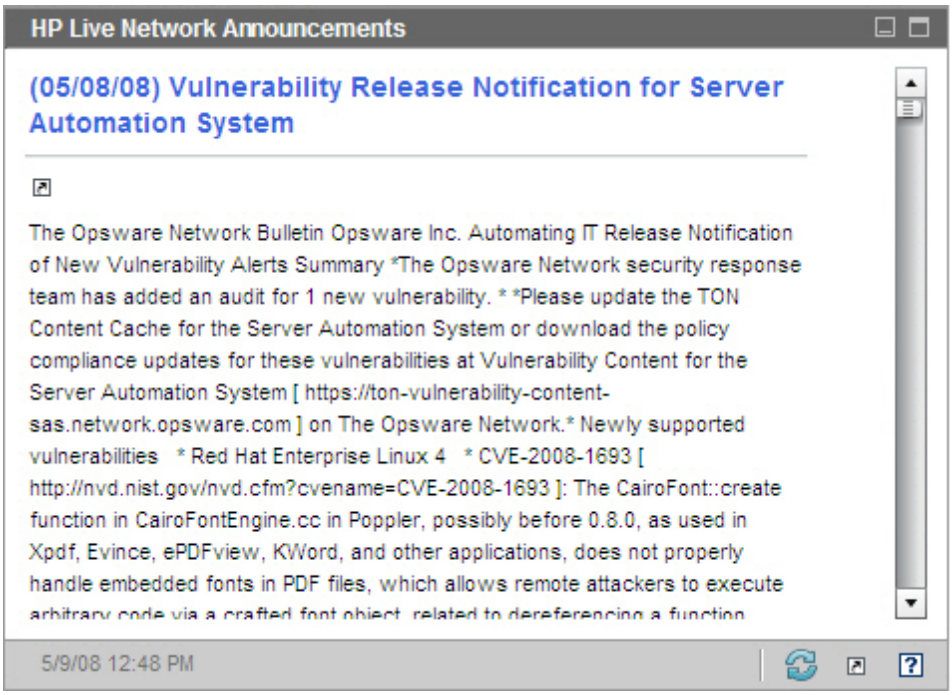
The grid is initially sorted by Device Count. To change the sort parameter, click the pertinent column heading.

To find more information about a particular vulnerability, click its OVAL or CVE identifier.

HP Live Network Announcements

This pane contains the most recently published HP Live Network vulnerability release announcements. This information is provided by an RSS feed from the HP Live Network subscription site. By default, this pane is not enabled, because it requires HP Live Network credentials to be specified before it can display information. See "Dashboards" on page 340 for information about configuring your HP Live Network credentials. Also, see "Accessing HP Live Network Content" on page 127.

HP Live Network Announcements



To find more information about a particular announcement, click the icon just below its title. A new browser window will open to the HP Live Network subscription support site. You must have an active HP Live Network subscription to access this site.

This pane does not have a chart view.

When you enable this pane on the Configuration tab, you can change the URL for the RSS feed, as well as the location of the HP Live Network authentication server (see "Dashboards" on page 340). You may also need to enable a proxy server (see "Configure the Connection to the HP Live Network Server" on page 305 and "Proxy Settings" on page 274).

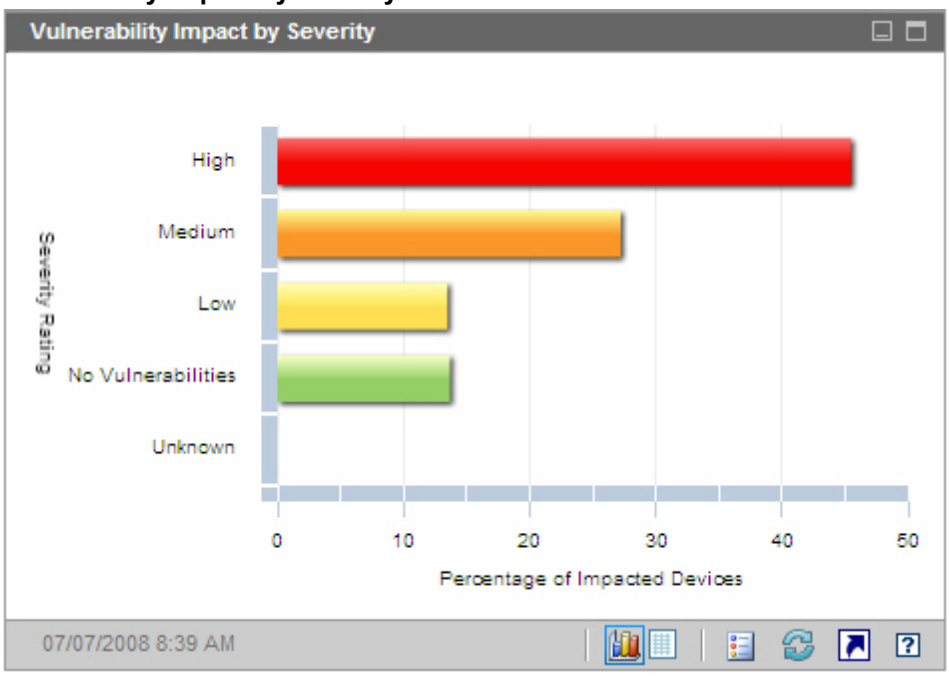
Vulnerability Impact by Severity (bar chart)

The chart view for this pane shows you the percentage of scanned devices in the enterprise that fall into each of the following five categories based on the highest severity vulnerability detected on each device:

- High (red)
- Medium (orange)
- Low (yellow)
- No Vulnerabilities (green)
- Unknown (blue)

The horizontal axis represents the percentage of devices affected in your environment. The vertical axis represents the four severity categories.

Vulnerability Impact by Severity



If you click one of the colored bars in the chart, a new browser window opens, and a detailed report is displayed. The report is filtered based on the severity category corresponding to the bar that you clicked.

The grid view for this pane shows the same information in text format. It has two columns:

- Status – severity by category
- Percentage of Impacted Devices – same as chart view

The grid also indicates whether the percentage of devices in each category has increased, decreased, or remained the same since the previous scan.

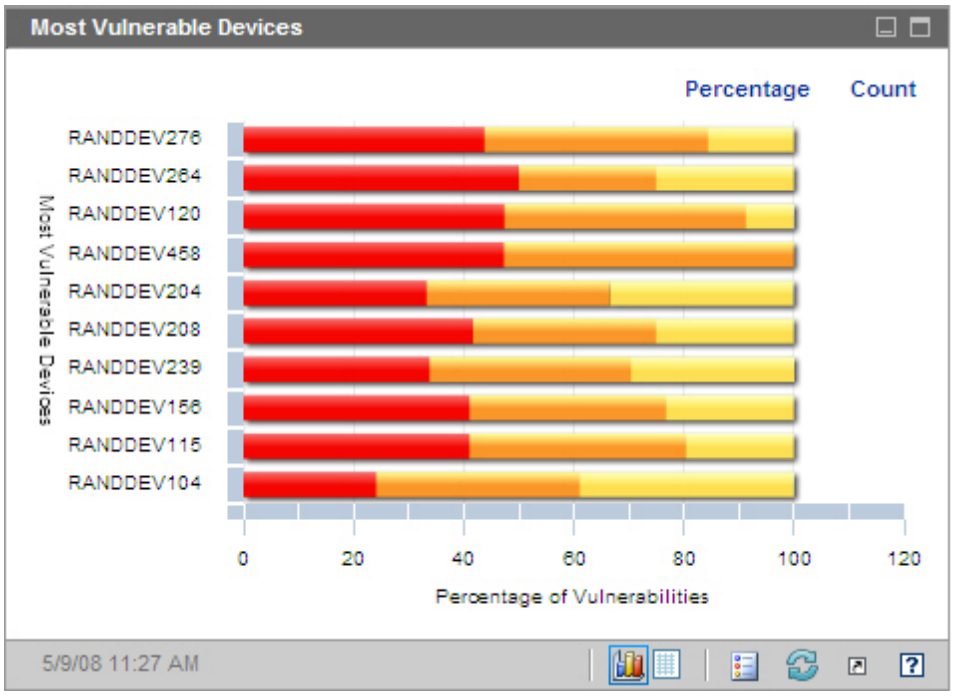
Most Vulnerable Devices

The chart view for this pane shows you the ten devices in your network that have the largest number of vulnerabilities. The colored segments in the chart represent the percentage (or number) of vulnerabilities present on a given device that fall into each of the following four categories:

- High (red)
- Medium (orange)
- Low (yellow)
- Unknown (blue)

The vertical axis lists devices by Device Identifier, and the horizontal axis shows the percentage or number of failed tests (vulnerabilities) in each risk category for this device.

Most Vulnerable Devices



To display the total number of vulnerabilities for each device listed, click **Count**. In this case, the horizontal axis uses a logarithmic scale.

Note: If a particular device has only one vulnerability, no data is shown for that device in the Count view. This is a known limitation of logarithmic scales. The data is visible in the grid view, however.

If you click one of the colored bars in the chart, a new browser window opens, and a detailed report for this device is displayed. This report is not filtered by severity – all vulnerabilities for this device are listed regardless of which colored area you clicked.

If you rest the cursor on one of the colored bars in the chart, you can see the number (and percentage) of vulnerabilities in each severity category for a particular device.

The grid view provides the following information for each device:

- Max Severity – CVSS Base score for the highest severity vulnerability detected for this device
- Device – Device identifier
- Failed Tests – number of vulnerabilities detected
- Last Scan Date – date and time of the most recent HP Live Network scan

The table is initially sorted by Failed Tests. To change the sort parameter, click the pertinent column heading.

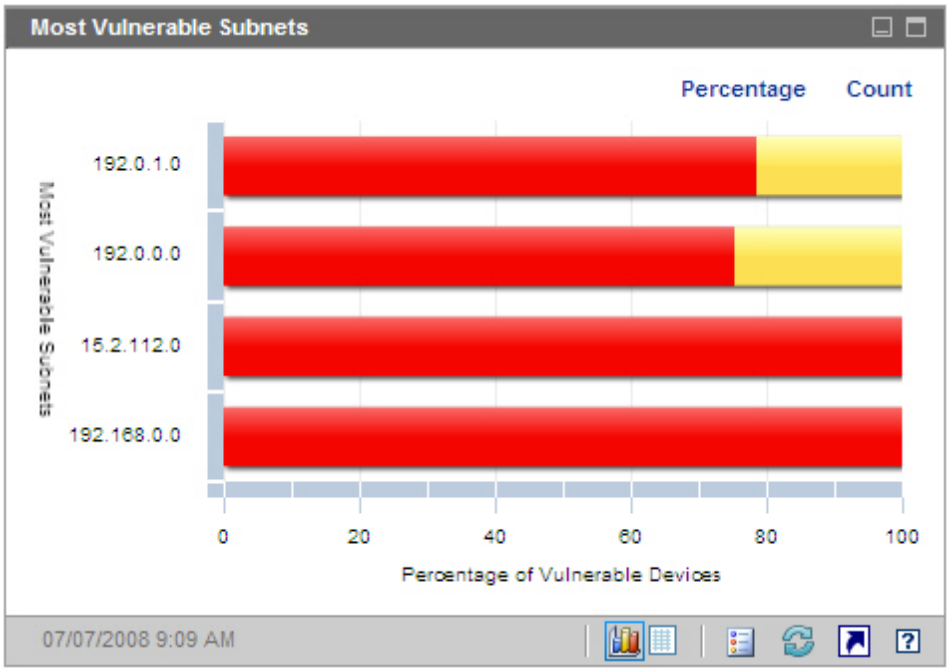
Most Vulnerable Subnets

The chart view of this pane shows you the ten most vulnerable subnets in the enterprise. It indicates the percentage of devices in each severity category: High (red), Medium (orange), Low (yellow), Unknown (blue), and No Vulnerabilities (green).

By default, this pane is disabled. To enable it, see "Dashboards" on page 340.

To view information about the devices in each subnet, rest the cursor over the horizontal bar for that subnet. A pop-up box shows you the number and percentage of devices in each severity category in this particular subnet.

Most Vulnerable Subnets



To display the number of vulnerable devices instead of the percentage, click **Count**. In this case, the horizontal axis uses a logarithmic scale.

Note: If a particular subnet has only one vulnerability, no data is shown for that subnet in the Count view. This is a known limitation of logarithmic scales. The data is visible in the grid view, however.

The grid view provides the following information for each subnet:

- Subnet address
- Total number of devices in the subnet
- Number of devices in each severity category

The table is initially sorted by High Risk devices. To change the sort parameter, click the pertinent column heading.

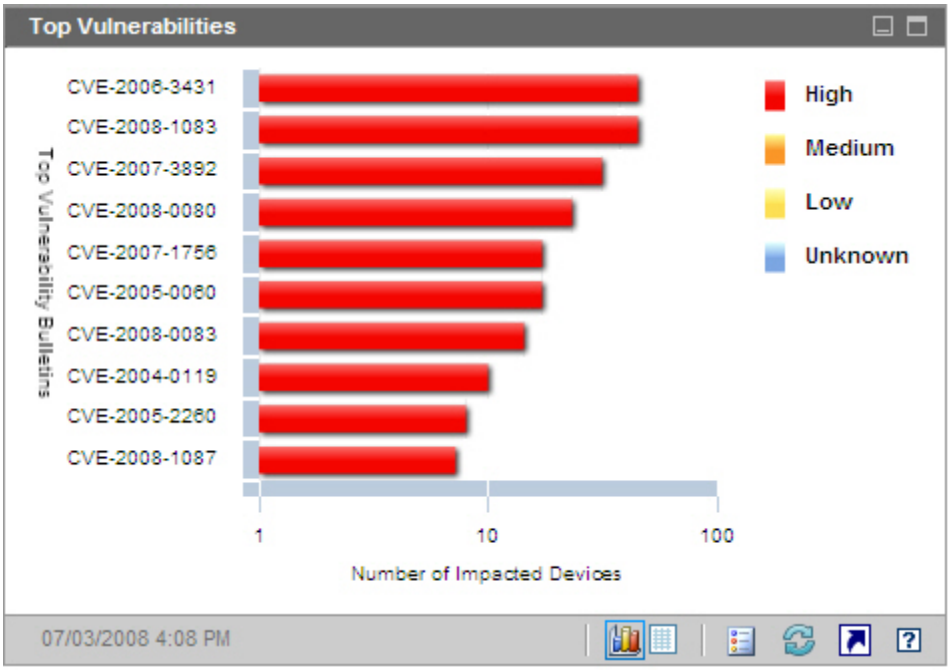
Top Vulnerabilities

The chart view of this pane shows you the ten security vulnerabilities that affect the greatest number of devices in your network. The vertical axis lists the CVE Identifiers for these ten vulnerabilities. The horizontal axis represents the number of devices affected and uses a logarithmic scale. The colors of the bars reflect the severity of each vulnerability:

- High (red)
- Medium (orange)
- Low (yellow)
- Unknown (blue)

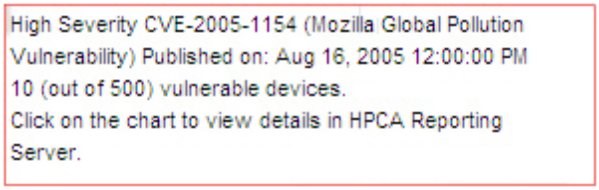
Because this chart uses a logarithmic scale, if a particular vulnerability affects only one device, no data is shown for that vulnerability in the chart view. This is a known limitation of logarithmic scales. The data is visible in the grid view, however.

Top Vulnerabilities



If you rest the cursor on the colored bar for a particular vulnerability, the CVE Identifier and description, severity, and number of devices affected is shown:

Tool Tip



If you click one of the colored bars in the chart, a new browser window opens, and a filtered report is displayed. The report lists all devices that have this vulnerability.

The grid view provides the following information for the top ten vulnerabilities detected:

- OVAL ID – OVAL ID for this vulnerability
- CVE ID – CVE ID for this vulnerability
- Description – from the CVE
- Severity – CVSS Base score for this vulnerability
- Platform Family – general type of operating system (for example, Windows)
- Device Count – number of devices affected by this vulnerability

The table is initially sorted by Device Count. To change the sort parameter, click the pertinent column heading.

To find more information about a particular vulnerability, click its CVE ID or OVAL ID.

Compliance Management Dashboard

RCA has the ability to collect regulatory compliance information for each managed client device in your enterprise. This information is then aggregated and displayed in the Compliance Management dashboard.

RCA is integrated with HP Live Network, which provides updated Compliance definitions and an executable client scanner.

Client devices are scanned using compliance rules that are based on established regulatory compliance standards, such as the Federal Desktop Core Configuration (FDCC) standard and the Center for Internet Security (CIS) standard. Compliance rules are specified using the Security Content Automation Protocol (SCAP).

Note: For more information about FDCC, CIS, and SCAP – including a list of common compliance management terms used throughout the Compliance Management dashboard and Compliance Management reports – see "Security and Compliance Management" on page 45.

The Compliance Management dashboard has a summary page and two views:

The Executive View includes the following information panes:

- "Compliance Summary by SCAP Benchmark" on page 106
- "Compliance Status" on next page
- "Historical Compliance Assessment" on page 108

The Operational View includes the following information panes:

- "Top Failed SCAP Rules " on page 111
- "Top Devices by Failed SCAP Rules " on page 112

You can configure the dashboard to show or hide any of these panes. See "Dashboards" on page 340 for additional information.

Note: When you click Compliance Management in the left navigation pane on the Home tab,

the Compliance Management home page is displayed. This page shows you the number of managed client devices that have been scanned and provides links to pertinent reports.

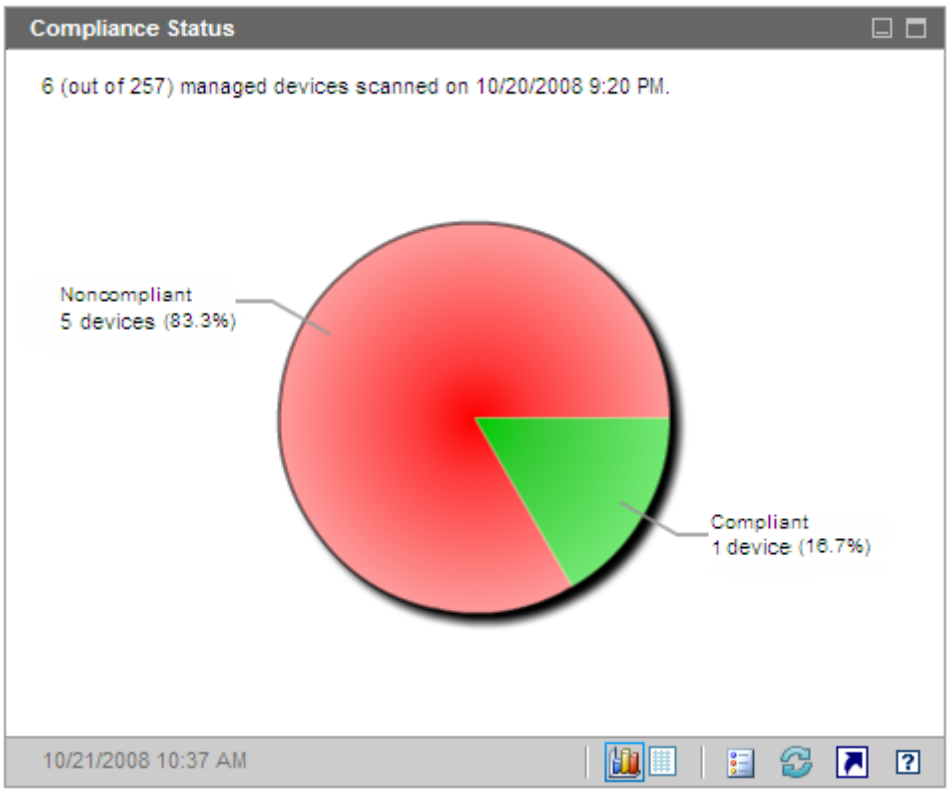
Compliance Status

This pane shows you the state of regulatory compliance across your enterprise based on the results of the most recent compliance scan completed on each managed client device. The chart view for this pane shows you the percentage of scanned devices that are in or out of compliance:

- Compliant devices (green)
- Noncompliant devices (red)

To see the number (or percentage) of devices in each state of compliance, rest the cursor on the corresponding sector of the pie chart.

Compliance Status



The number in the upper left hand corner of the pane is the total number of managed devices that were scanned. This number may not match the sum of the compliant and noncompliant devices, because some benchmarks do not apply to certain devices. For example, the fdcc-ie-7 benchmark does not apply to devices that do not have Internet Explorer 7 installed. If none of the benchmarks are applicable to a particular device, that device is considered to be neither compliant nor noncompliant.

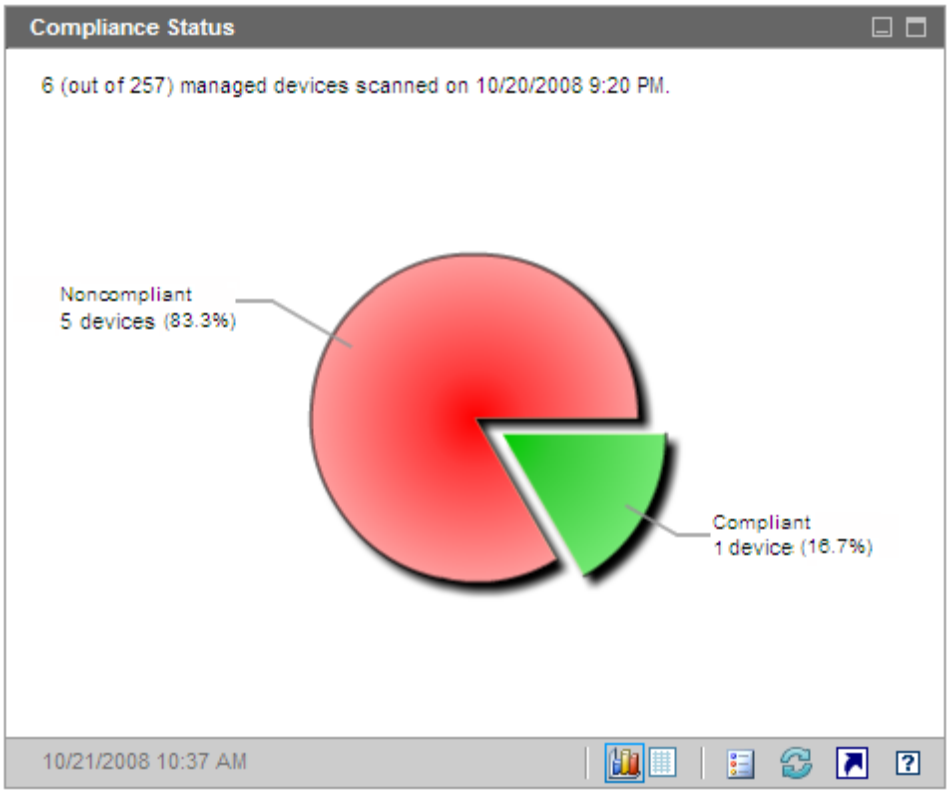
Data for each device is aggregated across all profiles in the benchmark. If a device is compliant with all applicable profiles in a benchmark, the device is considered to be compliant with that

benchmark. If a device is not compliant with even one profile in the benchmark, the device is considered noncompliant.

If you click one of the wedges in the pie chart, a new browser window opens, and the Compliance Summary by SCAP Benchmark report is displayed. This report is not filtered.

After you click a wedge and open a report, that wedge separates from the rest of the pie, as shown here:

Compliance Status After Report Opens



The grid view shows you how many devices are compliant or noncompliant. If you click either **Compliant** or **Noncompliant** in the grid view, the Compliance Summary by SCAP Benchmark report opens in a new browser window. The report is not filtered.

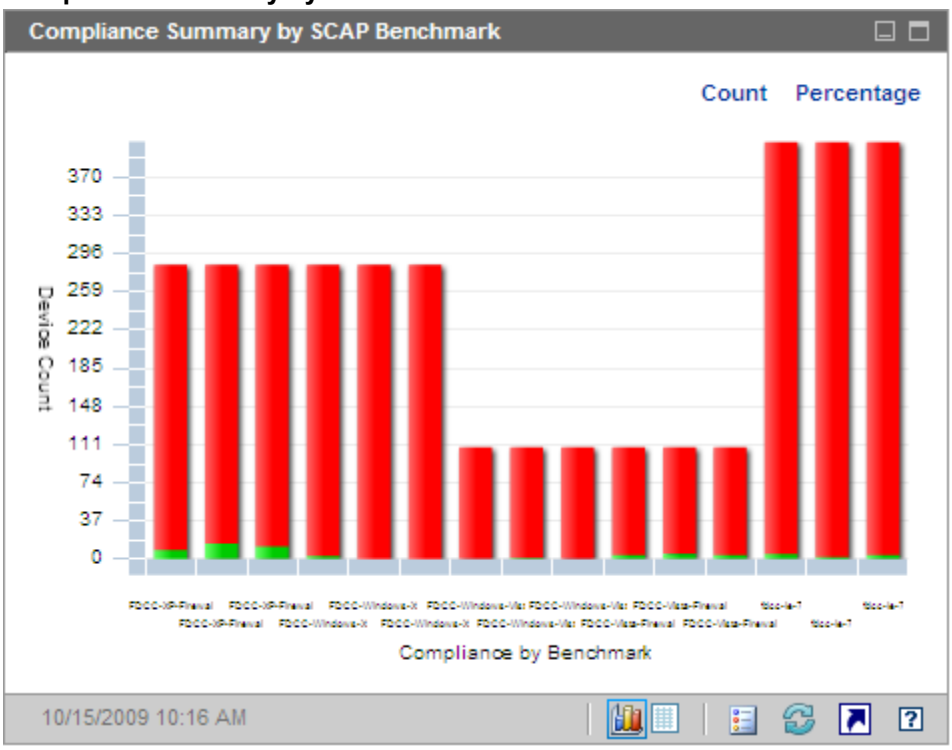
If you click the **Launch Report** button in this pane, the Benchmark Summary report opens. This report lists all profiles for which there are scan results, and it is not filtered.

Compliance Summary by SCAP Benchmark

The chart view for this pane shows you the number (or percentage) of scanned devices in the enterprise that are in or out of compliance with the associated SCAP benchmark:

- Compliant devices (green)
- Noncompliant devices (red)

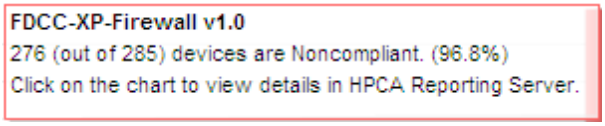
Compliance Summary by SCAP Benchmark



Only those benchmarks for which there are scan results are shown. Data for each device is aggregated across all profiles in the benchmark. If a device is compliant with all applicable profiles in a benchmark, the device is considered to be compliant with that benchmark. If a device is not compliant with even one profile in the benchmark, the device is considered noncompliant.

When you rest the cursor on one of the colored bars in the chart, a tool tip shows you information about the benchmark, including the number (or percentage) of devices in the pertinent state of compliance.

Tooltip



The tool tip always displays information from the last compliance scan performed. Typically a scan is performed daily.

If you click one of the colored segments in the bar chart, a new browser window opens, and the SCAP Scanned Devices report is displayed. The report is filtered based on the benchmark, version, and compliance status corresponding to the segment that you clicked.

The grid view for this pane shows you the number (and percentage) of devices that are compliant or noncompliant with each benchmark version. If you click a Benchmark ID in the grid view, the SCAP Compliance Rules by CCE report opens. The report is filtered based on the Benchmark ID you clicked.

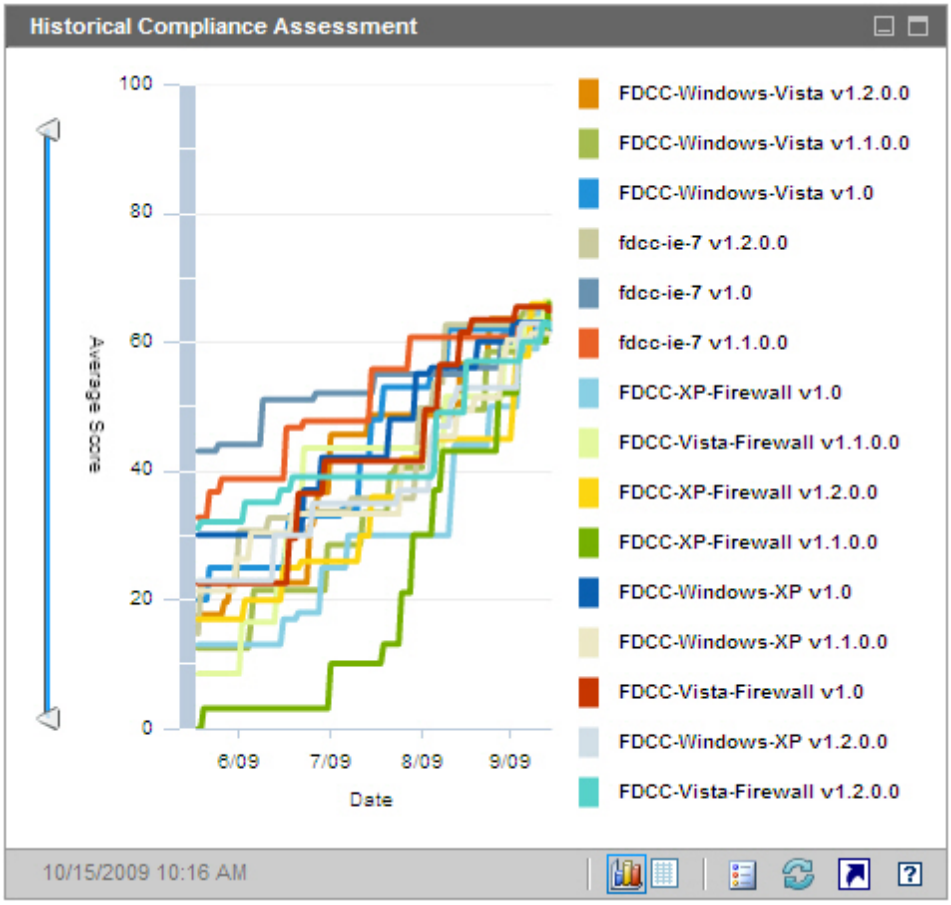
If you click the **Launch Report** button in this pane, the Benchmark Summary report opens. This report lists all profiles for which there are scan results, and it is not filtered.

If the same Benchmark ID appears more than once in the chart view for this pane, that is because different versions of the benchmark were tested. You can view the benchmark version in the chart view tooltip or in the grid view. All versions of a benchmark for which there are scan results are listed in the chart and grid view.

Historical Compliance Assessment

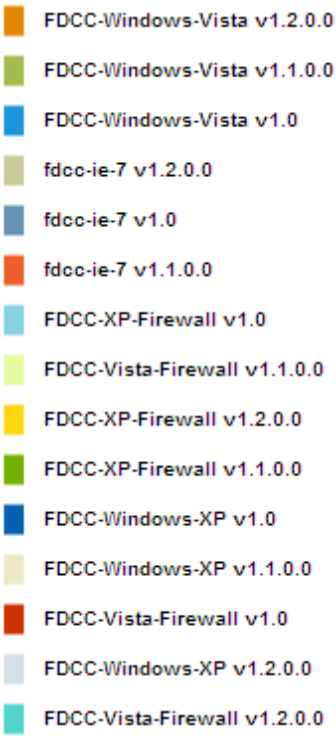
Once per day, RCA takes a snapshot of the compliance scanning results across your enterprise. Based on this snapshot, an average default score is calculated for each benchmark, version, and profile among the devices to which that profile applies. This information pane shows you the average default score for each benchmark version over time.

Historical Compliance Assessment



If a particular benchmark version contains multiple profiles, an “average of averages” calculation is performed. The average score for all profiles in that benchmark version is calculated.

The vertical axis represents the average default score. The horizontal axis represents time. Each colored line represents a different benchmark and version. The following benchmark versions are displayed in this chart:



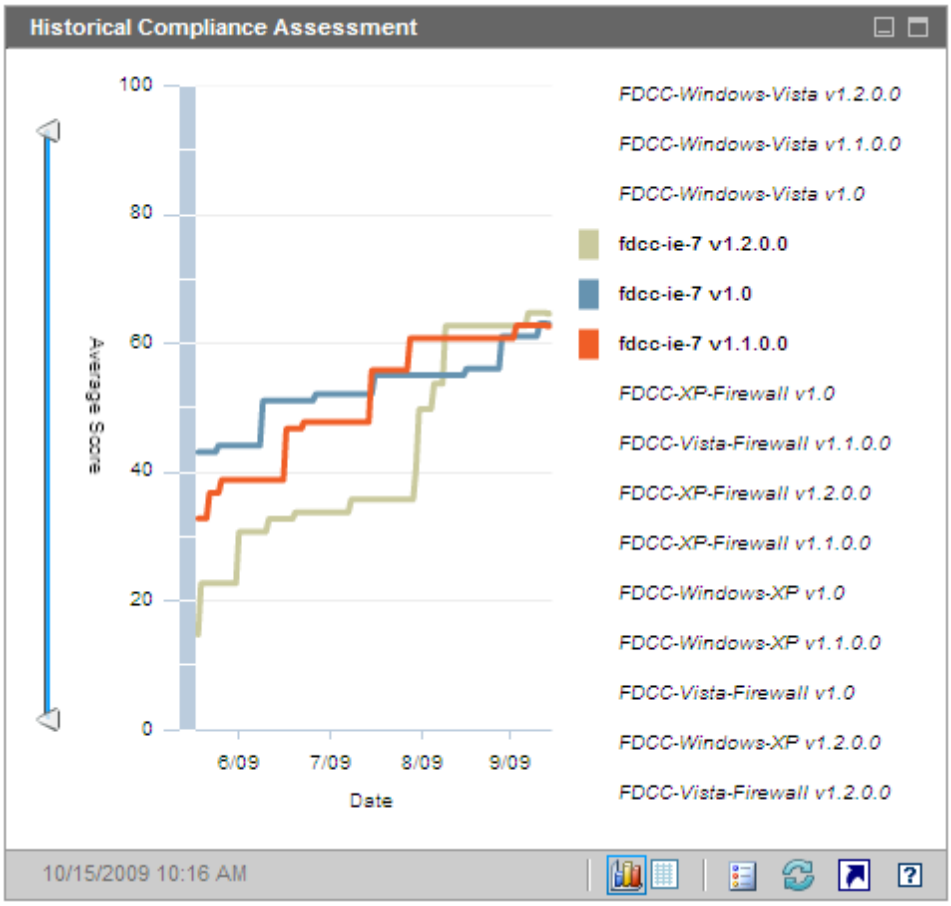
The colors are assigned dynamically and are not always the same for a specific benchmark and version. See the legend to see the current color assignments.

When you rest the cursor on one of the colored lines, a tool tip shows you the following information:

- Benchmark name and version
- Snapshot date
- Average default score for all devices that were scanned for this benchmark version. If the benchmark contains multiple profiles, this score represents the average across all profiles.

To hide a particular line in the chart view, click the corresponding item in the legend. Hidden items are shown in non-bold, italic text in the legend. To show this line again in the chart, click the legend item again.

In the following image, only benchmarks pertinent to Internet Explorer 7 are displayed in the chart:



You can use the sliders to zoom in on a particular region in the data. The sliders determine how much data appears in the chart. The range (scale) of the axis changes to represent only that range selected by the sliders. When you move or click one of the sliders, a tooltip shows you the date or score.

- The horizontal slider at the bottom of the pane enables you to specify a date range.
- The vertical slider on the left enables you to specify an average default score range

By default, the date range displayed runs from the date of the earliest compliance scanning snapshot to the date of the most recent snapshot. The average score range runs from zero to 100 by default.

When the triangles (△) are at opposite ends of a slider, the entire data range is visible. When the triangles are closer together, only a subset is visible. You can adjust both triangles on each slider.

If no data appear in the chart, move the triangles to the opposite ends of all three sliders to expose the entire data range.

Note: This pane will not contain data if a fewer than three daily compliance scanning snapshots have been taken—or if no devices have yet been scanned.

If you have just started collecting historical data, you can switch to the grid view to see that data. The grid view for this pane lists the daily average default score for each benchmark version. The table is initially sorted by date, with the most recent snapshot date listed first.

If you narrow down the data range displayed in the chart by using the sliders or by hiding some benchmark versions, the grid view will honor your customizations, and it will only contain the restricted data set.

If you refresh the chart by clicking on the circular arrow icon, the chart is restored to its initial state. The sliders return to the full-range position, all available data is displayed, and all benchmark versions are displayed.

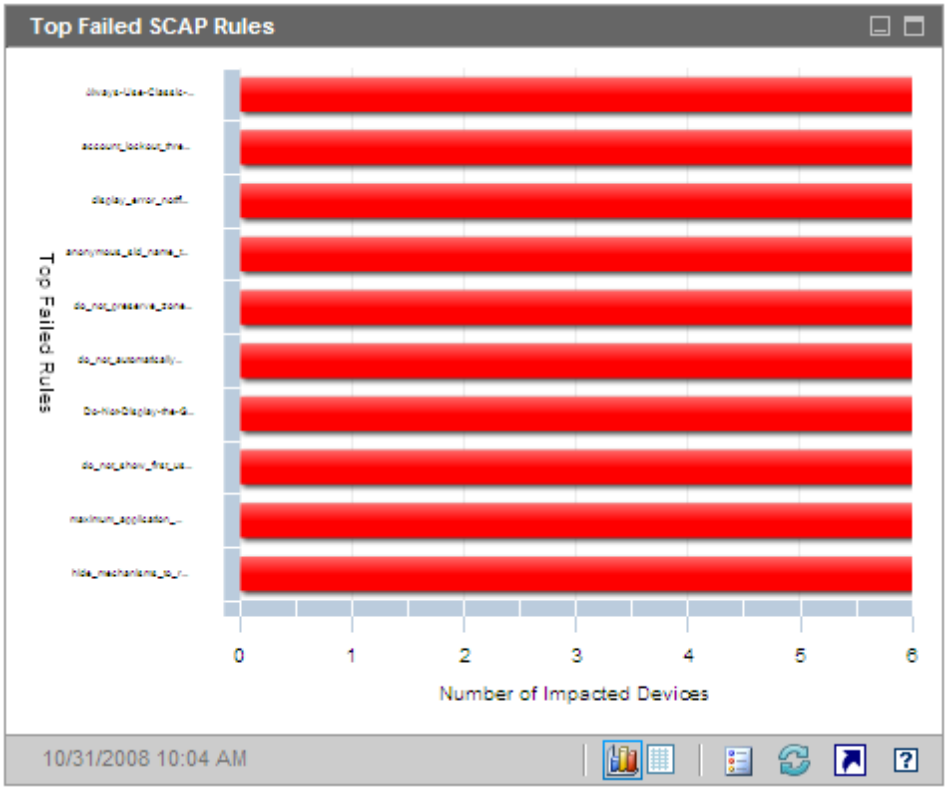
If you click the **Launch Report** button in this pane, the Historical Compliance Assessment report opens. This report lists all profiles for which there are scan results. The average score for each profile is shown.

Top Failed SCAP Rules

The chart view for this pane shows you the ten compliance checks (SCAP rules) that failed most frequently in your enterprise. The vertical axis lists the names of the pertinent compliance rules. The horizontal axis represents the number of managed client devices that are out of compliance with each rule.

To see the number of devices that failed a particular rule, rest the cursor on one of the colored bars in the chart.

Top Failed SCAP Rules



If you click one of the colored bars in the chart, a new browser window opens, and the SCAP Compliance Rules by CCE report is displayed. The report is filtered by the benchmark, version, profile, and Rule ID that corresponds to the bar that you clicked.

The grid view for this pane shows you the number of devices that failed each rule as well as the benchmark, version, and profile associated with the rule. If you click a Rule ID or Number of Devices in the grid view, the SCAP Compliance Rules by CCE report opens. The report is also filtered by the benchmark, version, profile, and Rule ID that corresponds to the row in the grid view where you clicked.

If you click the **Launch Report** button in this pane, the Top Failed SCAP Rules report opens. This report lists the ten rules that failed on the greatest number of devices. It is not filtered.

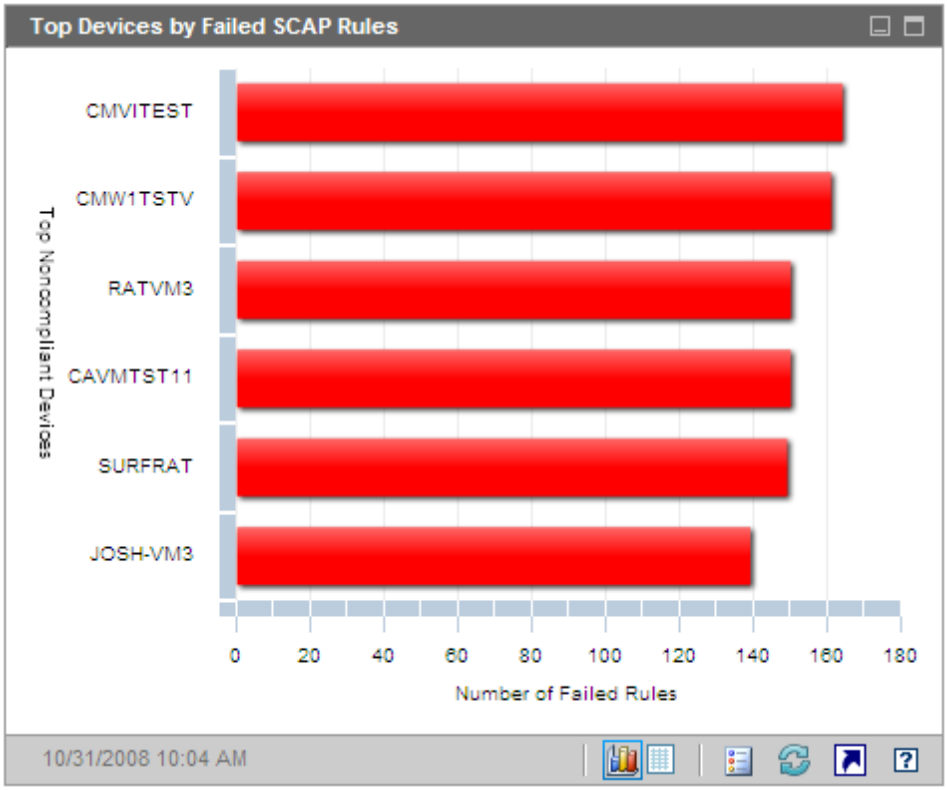
Top Devices by Failed SCAP Rules

The chart view for this pane shows you the managed client devices in your enterprise that failed the highest number of regulatory compliance checks (SCAP rules). The vertical axis lists the names of the pertinent devices. The horizontal axis represents the number of compliance rules that failed in the most recent compliance scan for each device listed.

Each bar represents the scan results for a specific benchmark, version, and profile on a specific device. To view additional details, rest the cursor on one of the colored bars in the chart.

Because each bar corresponds to a different benchmark, version, and profile, it is possible to have one device appear multiple times in this pane.

Top Devices by Failed SCAP Rules



If you click one of the colored bars in the chart, a new browser window opens, a detailed report is displayed. The report is filtered based on the device, benchmark, version, and profile corresponding to the bar that you clicked. The report has two parts:

- The Devices Scanned for Compliance portion of the report shows summary information about the most recent scan results for this benchmark, version, and profile on this device.
- The SCAP Compliance Rules by CCE portion of the report shows all of the rules associated with this benchmark, version, and profile.

The grid view for this pane shows you the number of rules that failed, the default score, and the date of the most recent scan for each device in the chart view. If you click a Device in the grid view, the Devices Scanned for Compliance report opens for that Device. The report is filtered to show the most recent scan results for this benchmark, version, and profile.

If you click the **Launch Report** button in this pane, the Top SCAP Noncompliant Devices report opens. This report is not filtered.

Security Tools Management Dashboard

RCA has the ability to scan the managed client devices in your enterprise to determine what types of security tools are present and collect pertinent information about the products detected. The following types of security products are supported:

- Anti-spyware tools
- Anti-virus tools
- Software firewalls

The collected information is then aggregated and displayed in the Security Tools Management dashboard.

RCA is integrated with HP Live Network, which provides an executable security tool scanner.

The Security Tools Management dashboard has two views: the Executive View and the Operational View.

The Executive View includes the following information panes:

- "Security Product Status" on next page
- "Security Product Summary" on page 115

The Operational View includes the following information panes:

- "Most Recent Definition Updates" on page 116
- "Most Recent Security Product Scans" on page 117

You can configure the dashboard to show or hide any of these panes. See "Dashboards" on page 340 for additional information.

Note: When you click Security Tools Management in the left navigation pane on the Home tab, the Security Tools Management home page is displayed. This page provides links to pertinent reports and shows you various statistics about Security Tool Management in your environment:

Devices Managed – Number of devices that are entitled to the HPCA Security Tools service that collects information on various security products

Devices Scanned – Number of devices that have been scanned by the HPCA Security Tools service

Last Scan Date – The last time that any of the devices in your environment were scanned by the HPCA Security Tools service

Scanner Last Downloaded On – The time when the Security Tools scanner was most recently downloaded from the HP Live Network site to RCA. See "Update HP Live Network Content" on page 55 for more information.

Security Product Status

The chart view for this pane shows you how many managed client devices have security tools – such as anti-spyware, anti-virus, or firewall software products – installed and enabled. You can display this information in either bar chart or stacked bar chart format. In both cases, the vertical axis shows the number of devices, and the horizontal axis shows the types of security tools detected.

The colors in the chart represent the following four conditions:

Security Tool Detection States

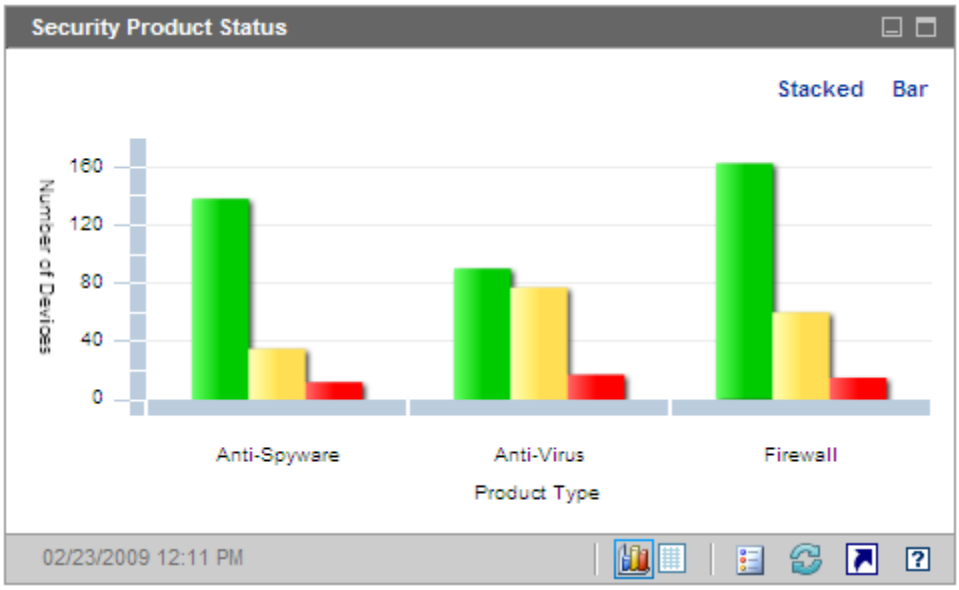
Color		Interval
	Green	Product was detected, and it was enabled.
	Yellow	Product was detected, but it was not enabled.
	Red	Product was not detected.
	Blue	Unknown

The state of a scanned device is considered Unknown under any of the following conditions:

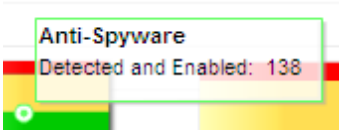
- The HP Live Network security tools scanner looked for this tool but was unable to determine its state.
- The scanner looked for this tool, but no scan records were found.
- The scanner did not look for this tool.

You can display this chart in either normal bar chart format (as shown here) or stacked bar format.

Security Product Status Pane



When you hover the mouse over a colored bar in the chart, a tool tip appears that shows you the number of devices in the corresponding state:



If you click one of the colored bars in the chart, a new browser window opens, and a filtered report is displayed. The report shows you the number of managed client devices where that type of security product (anti-virus, anti-spyware, or firewall) is in each of the following states: detected and enabled, detected and disabled, not detected, or unknown.

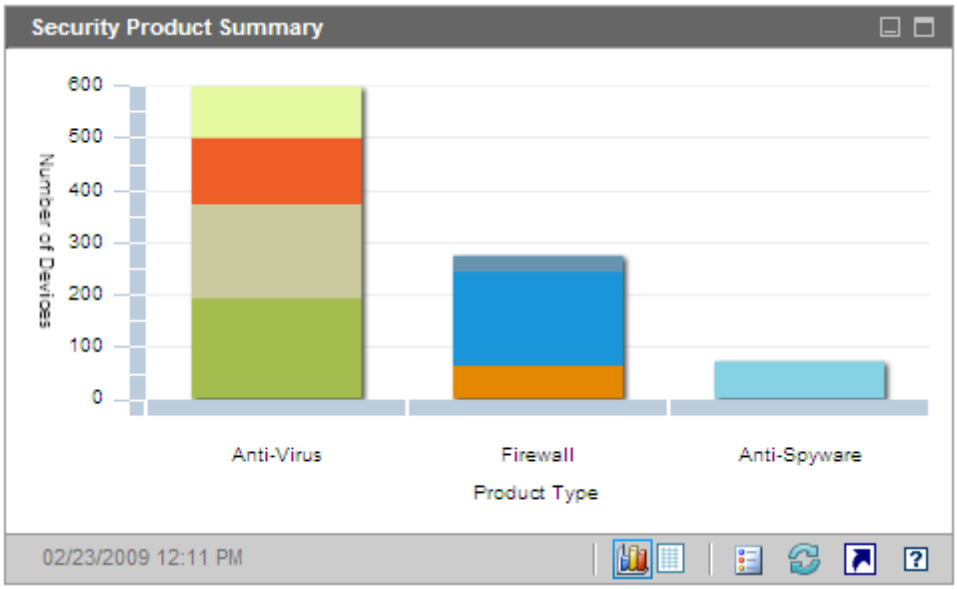
The grid view for this pane shows you total number of managed client devices whose security tools are in each state.

Security Product Summary

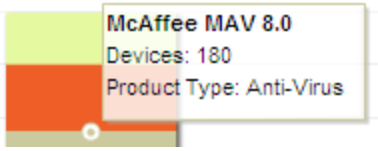
The chart view for this pane shows you which specific security products were detected on your managed client devices. The vertical axis shows the number of devices where each product was detected, and the horizontal axis shows the types of security tools detected.

The colors in the chart represent different products. Each version of a particular product is a different color.

Security Product Summary Pane



When you hover the mouse over a colored bar in the chart, a tool tip appears that shows you the number of devices where a specific security product was detected:



If you click one of the colored segments in the chart, a new browser window opens, and a filtered report is displayed. The report shows you the number of the managed client devices that have each specific security product of this type (anti-virus, anti-spyware, or firewall) installed.

The grid view for this pane shows you number of managed client devices that have each specific security product installed.

Most Recent Definition Updates

The chart view for this pane shows you how recently the virus and spyware definitions have been updated on your managed client devices. This information pertains to all anti-virus and anti-spyware products detected on your client devices.

You can display this information in terms of either the number (count) or percentage of devices. The colored bars represent the following update intervals:

Update Intervals

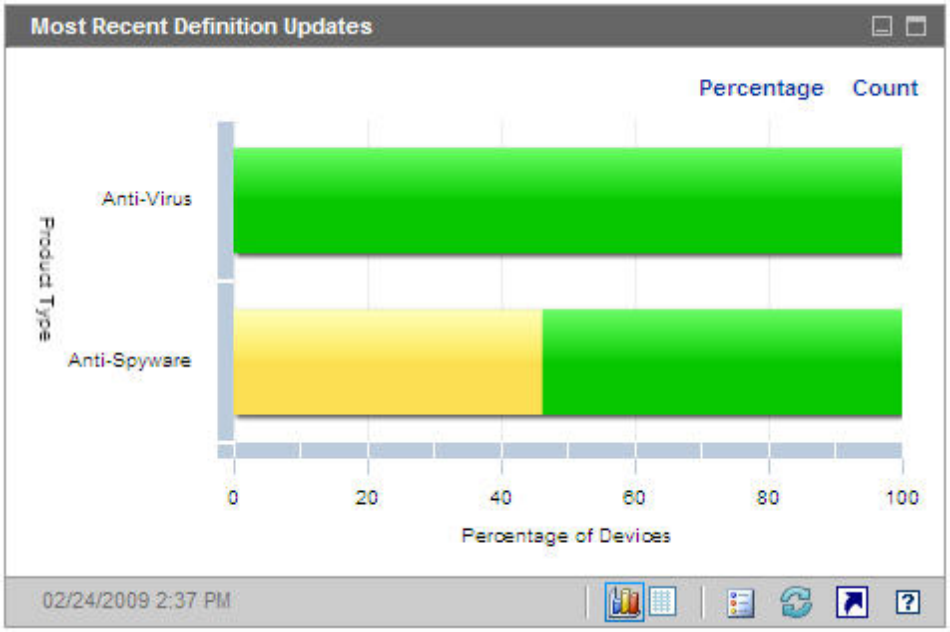
Color		Interval
	Red	More than 4 weeks
	Yellow	2 – 4 weeks
	Green	Less than 2 weeks

Color		Interval
	Gray	Never
	Blue	Update unknown

When you hover the mouse over a colored bar in the chart, a tool tip appears that shows you the number and percentage of devices that have been updated during the corresponding time interval.

Because this chart uses a logarithmic scale for the Count view, if a particular time interval contains only one device, no data is shown for that time interval in this view. This is a known limitation of logarithmic scales. However, the data is visible in the Percentage view as well as in the grid view.

Most Recent Definition Updates



The grid view for this pane shows you the same information in table format. Note that the grid view always uses device counts, not percentages.

If you click one of the colored bars in the chart view, a new browser window opens, and a filtered report is displayed. The report shows you the number of managed client devices where the anti-virus and anti-spyware definitions were updated during each time interval.

Most Recent Security Product Scans

The chart view for this pane shows you how recently your managed client devices have been scanned for viruses and spyware. This information pertains to all anti-virus and anti-spyware products detected on your client devices.

You can display this information in terms of either the number (count) or percentage of devices. The colored bars represent the following update intervals:

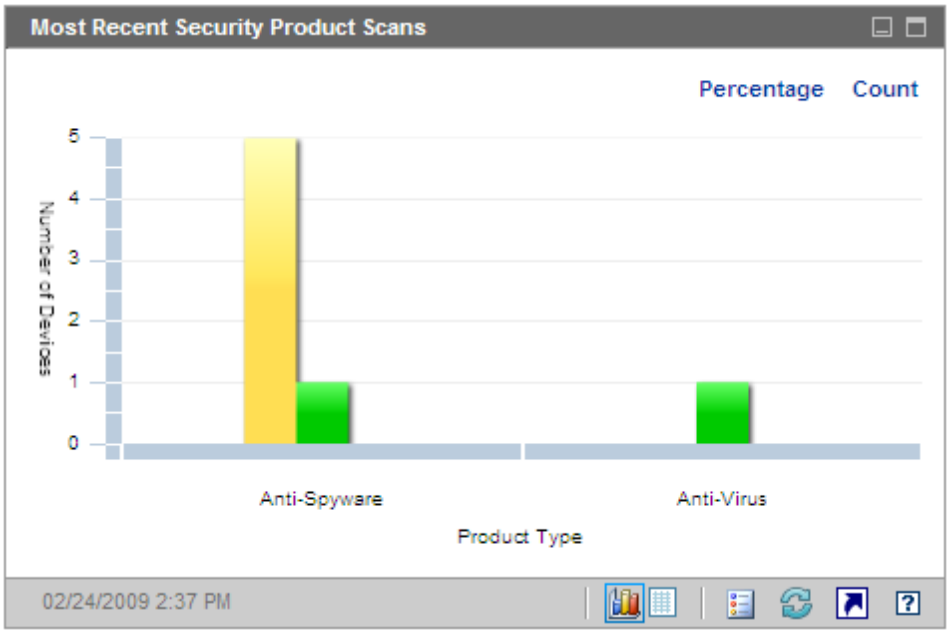
Scan Intervals

Color		Interval
	Red	More than 4 weeks
	Yellow	2 – 4 weeks
	Green	Less than 2 weeks
	Gray	Never
	Blue	Scan unknown

When you hover the mouse over a colored bar in the chart, a tool tip appears that shows you the number and percentage of devices that have been scanned during the corresponding time interval.

Because this chart uses a logarithmic scale for the Count view, if a particular time interval contains only one device, no data is shown for that time interval in this view. This is a known limitation of logarithmic scales. The data is visible in the Percentage view, however, as well as the grid view.

Most Recent Security Product Scans



The grid view for this pane shows you the same information in table format. Note that the grid view always uses device counts, not percentages.

If you click one of the colored bars in the chart view, a new browser window opens, and a filtered report is displayed. The report shows you the number of managed client devices that were most recently scanned by the pertinent security tool (anti-virus or anti-spyware) during each time interval.

Patch Management Dashboard

The Patch Management dashboard provides information about any patch vulnerabilities that are detected on managed devices in your network.

The Executive View of the Patch Management dashboard includes three information panes:

- "Device Compliance by Status (Executive View)" below
- "Device Compliance by Bulletin" on next page
- "Top Ten Vulnerabilities" on page 121

The Operational View includes the following information panes:

- "HP Live Network Patch Manager Announcements" on page 122
- "Device Compliance by Status (Operational View)" on page 123
- "Microsoft Security Bulletins" on page 124
- "Most Vulnerable Products" on page 125

You can configure the dashboard to show or hide any of these panes. See "Dashboards" on page 340.

Note: When you click Patch Management in the left navigation pane on the Home tab, the Patch Management home page is displayed. This page contains statistics and links to pertinent reports.

Device Compliance by Status (Executive View)

The chart view of this pane shows you the percentage of devices in your network that are currently in compliance with your patch policy. The colored wedges in the pie chart represent the following possible states:

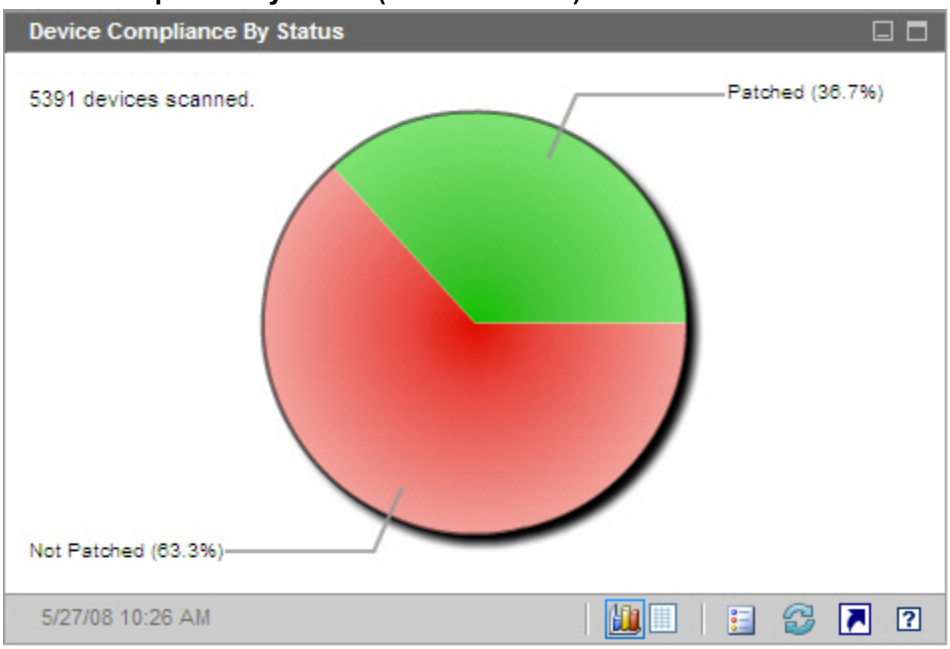
- Patched (green)
- Not patched (red)

The "Device Compliance by Status (Operational View)" on page 123 is similar but has finer-grained detail:

Device Compliance By Status Views

Executive View	Operational View
Patched	Patched Warning
Not patched	Not patched Reboot Pending Other

Device Compliance by Status (Executive View)



To see the number of devices in a particular category, rest the cursor over a colored sector in the pie chart.

If you click one of the colored wedges in the pie chart, a new browser window opens, and a filtered report is displayed. The report lists all devices in the patch compliance status corresponding to the wedge that you clicked.

The grid view for this pane shows the number of network devices in each of the compliance states shown in the pie chart.

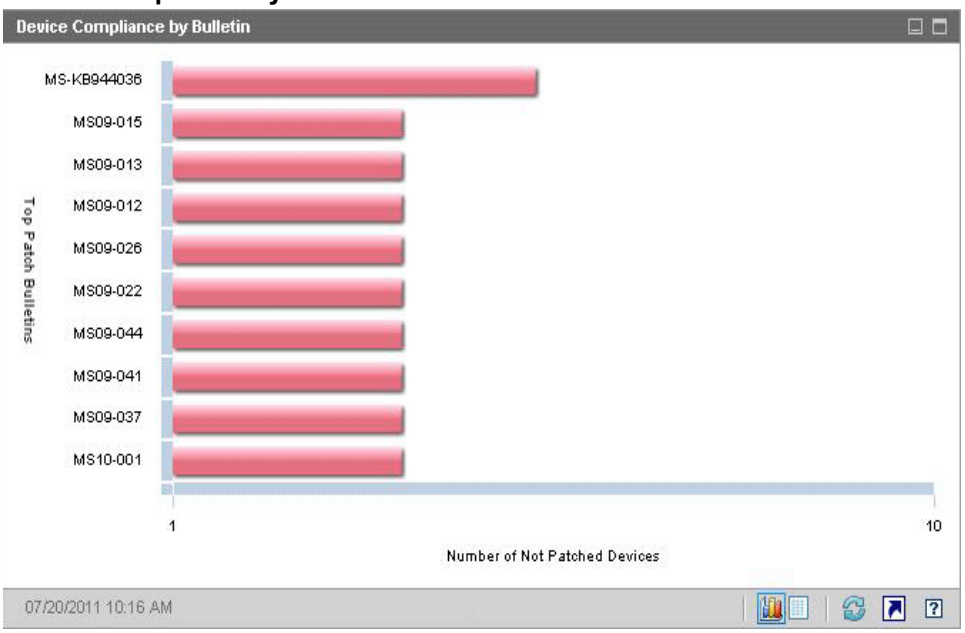
Device Compliance by Bulletin

The chart view of this pane shows you the ten patch vulnerabilities that affect the greatest number of devices in your network. The vertical axis lists the patch bulletin numbers for these vulnerabilities. The horizontal axis represents the number of devices not patched and uses a logarithmic scale.

Note: If a particular bulletin affects only one device, no data is shown for that bulletin in the chart view. This is a known limitation of logarithmic scales. The data is visible in the grid view, however.

To see the name of the bulletin and the number of devices affected, rest the cursor on one of the colored bars.

Device Compliance by Bulletin



If you click one of the colored bars in the chart, a new browser window opens, and a filtered report is displayed. This report shows which managed devices have this patch vulnerability.

The grid view provides the following information for the top ten patch vulnerabilities detected:

- Bulletin – The Microsoft Security Bulletin identifier for this vulnerability
- Description – Title of the bulletin
- Not Patched – Number of devices with this patch vulnerability

The table is initially sorted by Not Patched. To change the sort parameter, click the pertinent column heading.

To find more information about a particular bulletin, click the bulletin number.

Top Ten Vulnerabilities

The chart view of this pane shows the compliance state of the top ten vulnerabilities that affect the maximum number of devices in the network. The chart displays the number of devices that have been patched or not for each of the vulnerability. These devices are represented as follows:

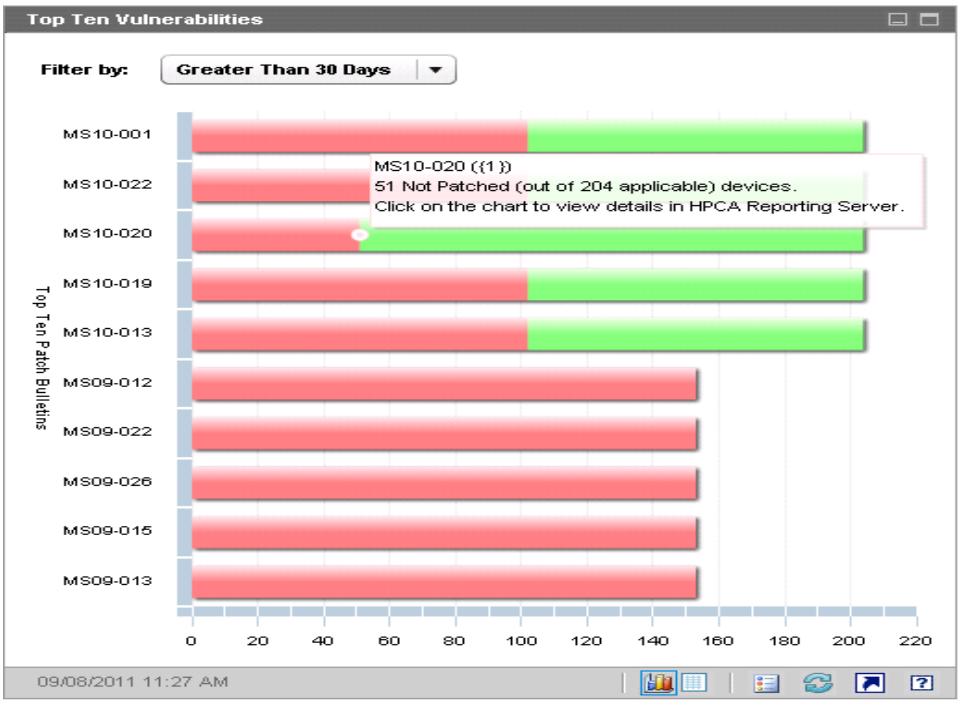
- Patched devices (green)
- Non-patched devices (red)

You can view the statistics of these devices for last 7 days, 14 days, 21 days, 30 days, and greater than 30 days. You can also filter the vulnerabilities by **Recently Released** to view statistics for top ten bulletins released by Microsoft and acquired by Patch Manager that affect the maximum number of devices in the network.

The vertical axis of the chart lists the top ten patch bulletins. The horizontal axis represents the number of devices affected by these bulletins.

To see the number of devices affected and the compliance state of a particular bulletin, position the cursor on one of the colored bars.

Top Ten Vulnerabilities



The grid view provides the following information for the top ten vulnerabilities:

- Bulletin – The Microsoft Security Bulletin identifier
- Not Patched – Number of devices not compliant with a particular bulletin
- Patched – Number of devices compliant with a particular bulletin
- Devices – Total number of devices affected because of a particular bulletin

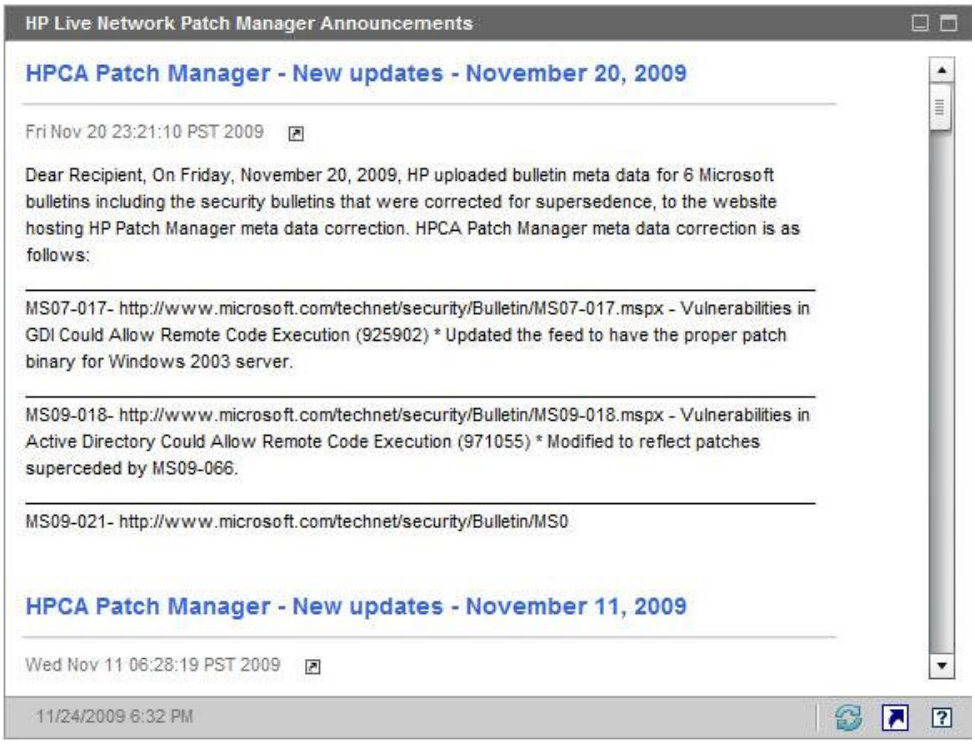
The table is initially sorted by **Devices**. To change the sort parameter, click the pertinent column heading.

To find more information about a particular bulletin, click the bulletin name.

HP Live Network Patch Manager Announcements

This pane contains the most recently published HP Live Network Patch Manager announcements. This information is provided by an RSS feed from the HP Live Network subscription site. See "Accessing HP Live Network Content" on page 127. By default, this pane is not enabled, because it requires HP Live Network credentials to be specified before it can display information. See "Dashboards" on page 340 for information about configuring your HP Live Network credentials.

HP Live Network Patch Manager Announcements



To find more information about a particular announcement, click the icon just below its title. The HP Live Network subscription support site opens in a new browser window. You must have an active HP Live Network subscription to access this site.

This pane does not have a chart view.

When you enable this pane on the Configuration tab, you can change the URL for the RSS feed, as well as the location of the HP Live Network authentication server (see "Dashboards" on page 340). You may also need to enable a proxy server (see "Configure the Connection to the HP Live Network Server" on page 305 and "Proxy Settings" on page 274).

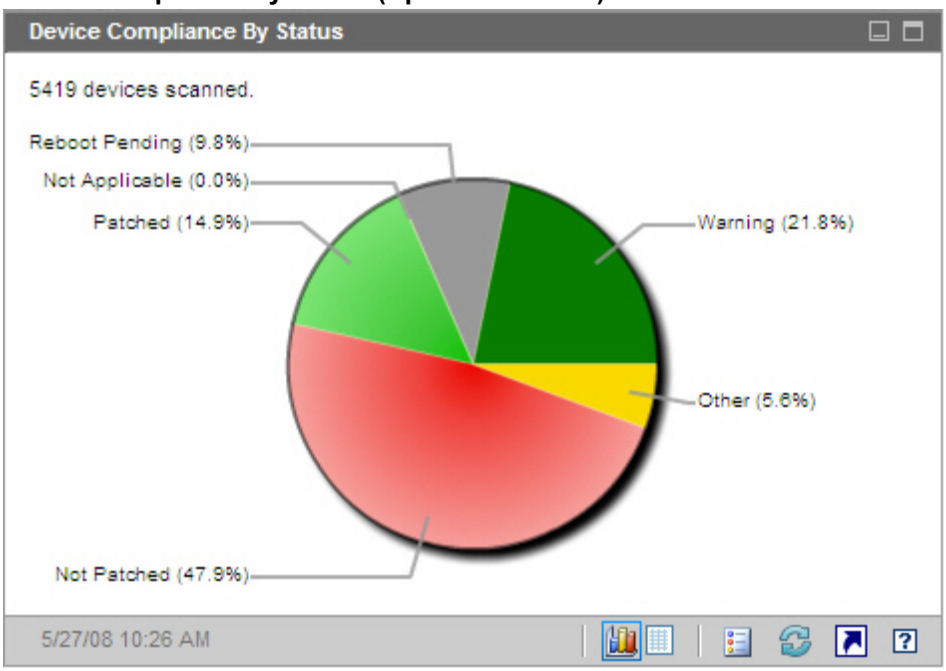
Device Compliance by Status (Operational View)

The chart view of this pane shows you the percentage of devices in your network that are currently in compliance with your patch policy. To see the number of devices in a particular category, rest the cursor over a colored sector in the pie chart.

This pane is similar to the "Device Compliance by Status (Executive View)" on page 119 pane but shows a finer level of detail and uses the same colors used by the Patch Manager:

- Patched (light green)
- Not Patched (red)
- Reboot Pending (light gray)
- Warning (dark green)
- Other (yellow)
- Not Applicable (dark gray)

Device Compliance by Status (Operational View)



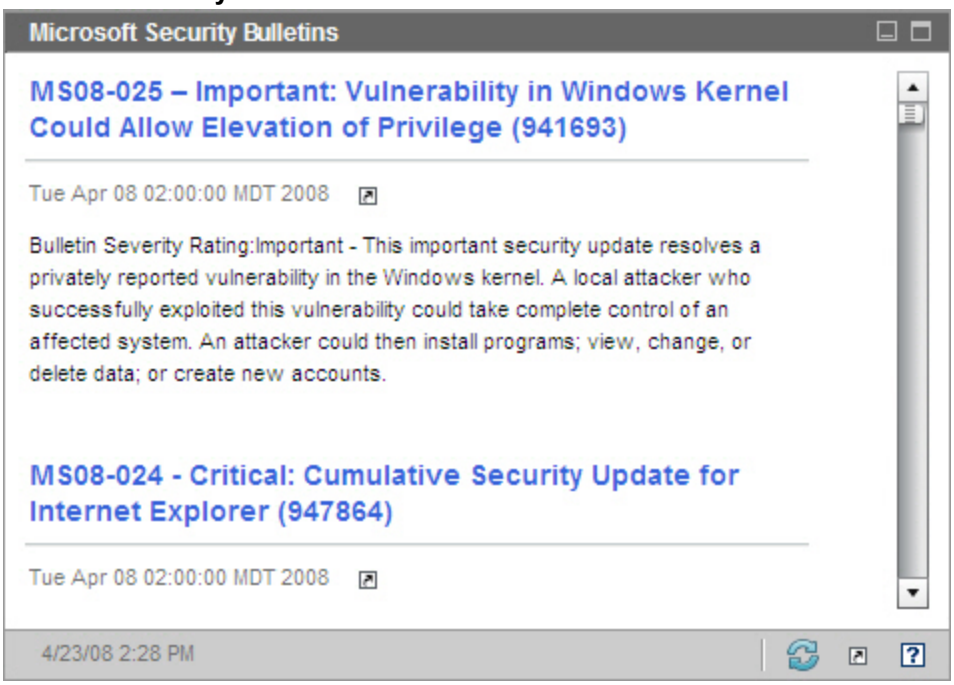
If you click one of the colored wedges in the pie chart, a new browser window opens, and a filtered report is displayed. The report lists all devices in the patch compliance status corresponding to the wedge that you clicked.

The grid view shows the number of network devices in each of the compliance states shown in the pie chart.

Microsoft Security Bulletins

This pane shows you the most recent Microsoft Security Bulletins. By default, this information is provided by an RSS feed from Microsoft Corporation. You can change the URL for the feed by using the Configuration tab (see "Dashboards" on page 340).

Microsoft Security Bulletins



To view detailed information about a particular bulletin, click the icon just below the bulletin name.

This pane does not have a chart view.

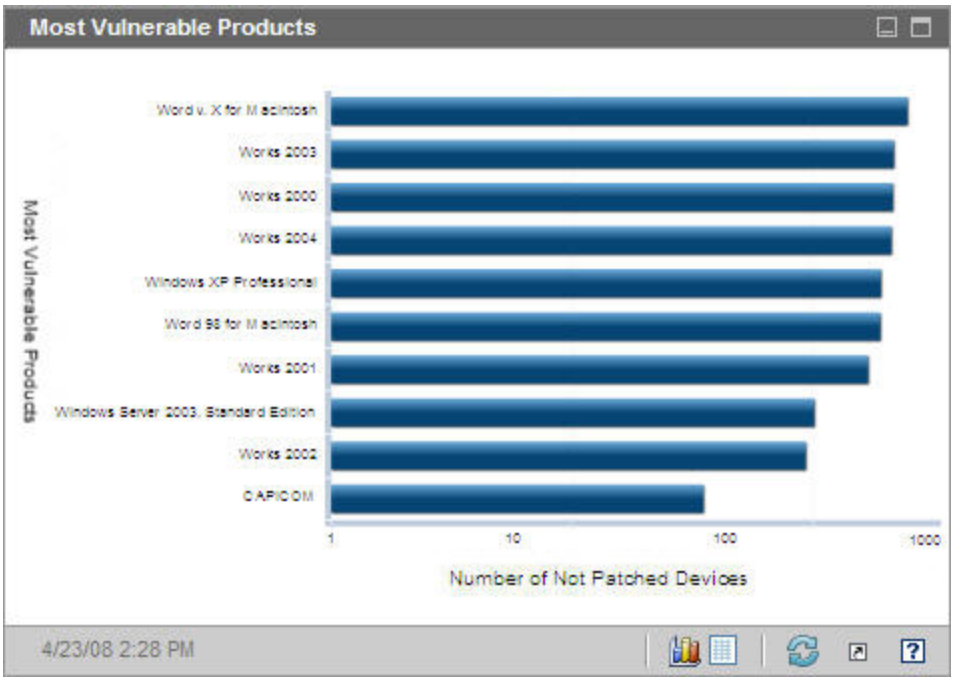
Most Vulnerable Products

This pane is disabled by default. To enable it, see "Dashboards" on page 340.

The chart view of this pane shows you the software products in your network for which there are the greatest number of not patched devices. The vertical axis lists the software products. The horizontal axis reflects the total number of not patched devices for the software product.

Because this chart uses a logarithmic scale, if the number of not patched devices for a particular product equals one, no data is shown for that product in the chart view. This is a known limitation of logarithmic scales. However, the data is visible in the grid view. To see the number of devices on which a particular software product is not patched, rest the cursor over one of the colored bars.

Most Vulnerable Products



The grid view provides the following information for each product:

- Product – Name of the software product
- Not Patched – Number of not patched devices for a particular product
- Applicable Devices – Number of devices on which this product is installed

The table is initially sorted by Not Patched. To change the sort parameter, click the pertinent column heading.

Chapter 5

RCA and HP Live Network

HP Live Network is a subscription service that enables you to obtain the most current content for RCA.

HP Live Network provides the latest content for setting profiles and the latest definitions and scanners for security and compliance management. Report enhancements can also be delivered over Live Network. When available, you can obtain these enhancements by performing an HP Live Network update. Any customizations that you have made to your reports will not be overwritten when you download the latest reports from the Live Network site.

Accessing HP Live Network Content

To obtain updated content, you must have an active HP Software Support contract with valid Live Network Subscription credentials for this content. You will then receive a user ID, password, and content server URL that you can use to configure the Live Network settings on the Configuration tab.

Note: The HP Live Network content server URL that you receive with your subscription may be different from the default URL shown on the Live Network settings page on the Configuration tab in the RCA Console. Be sure to use the URL that comes with your subscription. For more information, see "Live Network" on page 305 for details.

You *must* use current HP Passport credentials for HP Live Network Announcements to see the HP Live Network Announcements dashboard pane. To update the HP Passport credentials for HP Live Network Announcements, do the following:

1. Visit HP BSA Essentials Network web site at https://hpln.hp.com/ and complete the one time confirmation step before using the HP Live Network announcements widget.
2. If you continue to see a connection failure for the HP Live Network Announcements widget:
   a. Visit the HP Live Network RSS Feed at: https://hpln.hp.com/node/9254/feed/content/announcements
   b. Complete the one-time confirmation step if you are asked for it.

For more information about purchasing an HP Live Network subscription, visit the HP BSA Essentials Network Security & Compliance Service for Client Automation web site:

https://hpln.hp.com/group/security-and-compliance-client-automation

You will need to provide your HP Passport credentials to view this site.

License Requirements

To obtain the latest content from HP Live Network, you will need the following:

- License for RCA Enterprise Edition
- License for the RCA Security and Compliance Manager
- Active Persistent Software Support contract with valid Live Network Subscription credentials
- License for the RCA Patch Manager

If you do not have these items, the pertinent dashboards will be empty, and the applicable content will be unavailable for download and use.

The first two items are required for the vulnerability management, compliance management, and security tools management dashboards. The Patch Manager license is required for the patch management dashboard.

Note: The sample scanning services included with your HPCA software do not require HP Live Network credentials. This sample does not include a scanner for security tools management, however. You must have an active HP Live Network subscription to perform security tools management in RCA.

Updating HP Live Network Content

When RCA updates your content from the HP Live Network site (or from the file system), it uses a tool called the HP Live Network Connector (LNC).

To obtain Live Network content, you must use the "HP Live Network Connector" below and know "How to Update HP Live Network Content" on next page.

HP Live Network Connector

The HP Live Network Connector is a tool used by RCA to create a secure connection to the HP Live Network content distribution server and download the updated content. When accessing the HP Live Network content, the HP Live Network Connector first determines what content is available and then downloads the appropriate content from the HP Live Network subscription site.

A default version of the HP Live Network Connector is installed and configured when RCA is installed. It is self-updating. Any changes to the connector are automatically downloaded when you update your HP Live Network content. In certain circumstances, you may want to install a new copy of the LNC. If you want to re-install the HP Live Network Connector for any reason, you can download a new copy at any time. For more information, see "Download the HP Live Network Connector" on next page.

Note: The HP Live Network Connector performs authentication to HP Live Network and downloads content. By itself, the Connector does not install anything into the RCA infrastructure. RCA manages the loading of the updated HP Live Network content

When you update your RCA content – either from HP Live Network or from the file system – the following actions typically happen:

1. The content is copied into a temporary directory.
2. The content is loaded into the RCA database. This primes the database for processing collected data, enables RCA to deploy the pertinent services, and drives the detailed reports.
3. The RCA console is updated with relevant UI content.

When a client device with a configured security policy subsequently makes a connection to the SECURITY Domain in the CSDB, the data and scanners are deployed to that client device. At this point, the client device will be scanned. The results of the scans are then sent to the Core database.

Download the HP Live Network Connector

The HP Live Network Connector (LNC) is provided with RCA and is installed automatically when you configure the Live Network settings for the first time. The LNC is self-updating. Whenever you update your HP Live Network content, the LNC checks for and installs any available LNC updates. This way, you are always guaranteed to have the most recent version of the LNC after each Live Network update.

If you need to re-install the LNC for any reason—for example, if someone inadvertently uninstalls it—follow these steps.

To download a new copy of the HP Live Network Connector:

1. On the Configuration tab, expand the Infrastructure Management area, and click **Live Network**.
2. Click the **Download** link to the right of the HP Live Network Connector box. The HP Live Network subscription support site opens in a new browser window. You can download the LNC executable from this site. You will need your HP Live Network subscription user name and password to log in.
3. Follow the instructions on the HP Live Network site to download and install the LNC.

Note: If you install the LNC in a location other than the original installation location, be sure to update the **HP Live Network Connector** path on the Live Network configuration page accordingly. The default installation location is:

<InstallDir>`\LiveNetwork\lnc\bin\live-network-connector.bat`

How to Update HP Live Network Content

To update your HP Live Network content from the HP Live Network subscription web site, do the following:

- Use the Schedule Updates tab on the HP Live Network operations page to configure the RCA Console to periodically download updated content, or use the Update Now tab to initiate an immediate update from the HP Live Network subscription site.

  See "Live Network" on page 223 for detailed instructions.

- Use the `content-update.bat` command line utility to manually trigger an update.

  See "Use the Command Line Utility" on page 435 or for instructions.

You should always update your HP Live Network content after you install or upgrade your HPCA software to ensure that you have the most recent content available.

Note: When you download new HP Live Network content, you may simply get updates to existing services, or you may be able to access brand new services. To use any new services, be sure to explicitly entitle your client devices to these services.

Note: The display names of the services downloaded from HP Live Network have angle brackets (< >) surrounding them, uniquely identifying these as HP-supported services from the Live Network site. Be aware that if you modify the services in your environment, your changes may be lost the next time that you update your HP Live Network content.

Chapter 6

Managing the Enterprise

The Management area contains the tools you use to manage the client devices in your environment. This chapter includes the following topics:

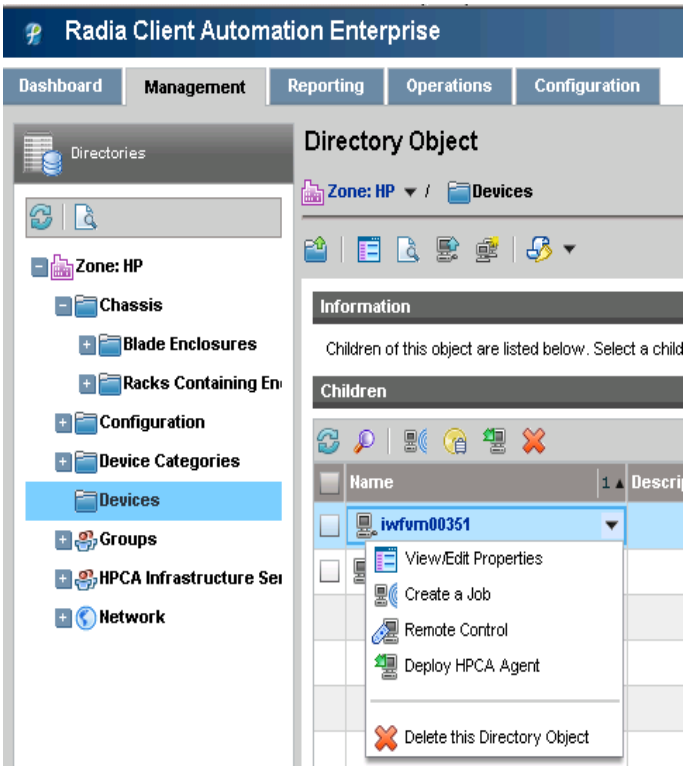
Directory Objects

From the Directories tree on the **Management** tab, you can view the objects in your configured directory services. For more information, see "Directory Services" on page 295. You can view and edit the properties of an object, search its directories, import devices, and create new groups.

When you click a directory object in the left navigation tree, you see a list of its children or members in the content pane. The content pane switches between children or members depending on the type of the selected directory object. If the directory object is a container type, you will see its children. If the directory object is a group type, you will see its members.

When you rest the cursor over the name of a child/member object in the list, a drop-down menu becomes available – click the down arrow to display the menu. The options available in the menu vary depending on the hierarchical context in which the object exists and the RCA features that are currently enabled.

Directory Object View



The following table summarizes the actions that you can take from the drop-down menu for a child object.

Actions Available from the Drop-Down Menu

Icon	Action	Description
	View/Edit Properties	View or edit the properties of this child object in a new browser window. For more information, see "Directory Object View " above.
	Create a Job	Create a Notify or DTM job for this object. For more information, see "Managing Jobs" on page 148.
	Remote Control	Access a managed device remotely. For more information, see "Controlling Devices Remotely" on page 163.
	Deploy RCA Agent	Deploy the RCA Agent to this device so that it can be managed by RCA. For more information, see "Deploying the RCA Agent" on page 147.
	OS Management	Deploy an operating system, or perform a one-time hardware maintenance operation. For more information, see "Managing Operating Systems " on page 168.
	View Out of Band Details	View the Out of Band details for a device with Intel vPro or DASH-enabled devices. For more information, see "Viewing Out Of Band Details" on page 175.
	Delete this	Delete this object from the RCA database. For more information, see

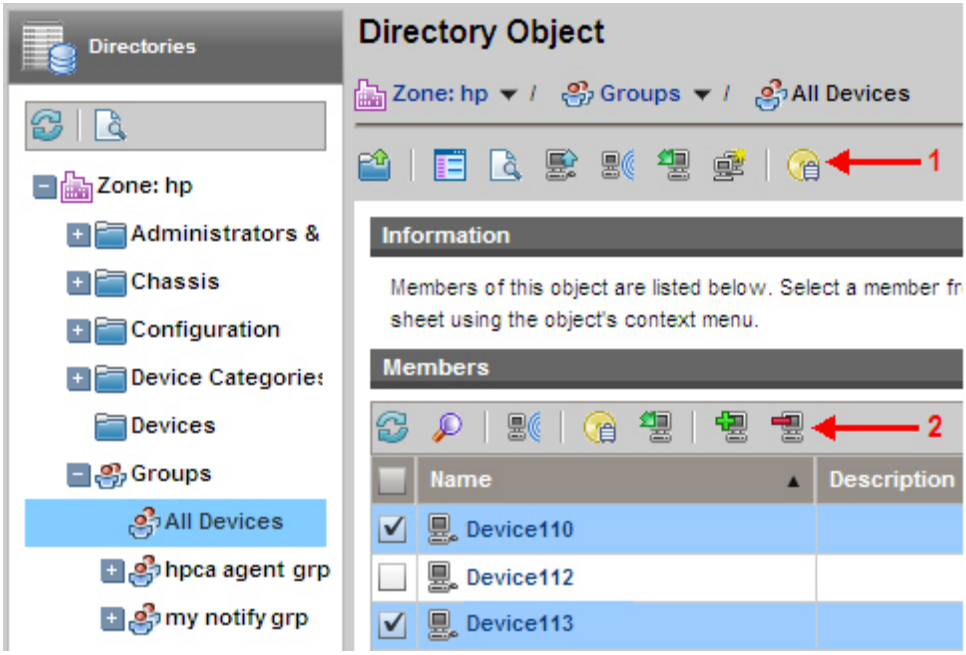
Icon	Action	Description
	Directory Object	"Importing Devices" on page 145.

In the Directory Object view, there are two toolbars:

- The upper toolbar pertains to the object selected in the Directories tree.
- The lower toolbar pertains to the selected child objects in the grid.

In the example shown in the following figure, the All Devices group is selected.

Directory Object View Toolbars

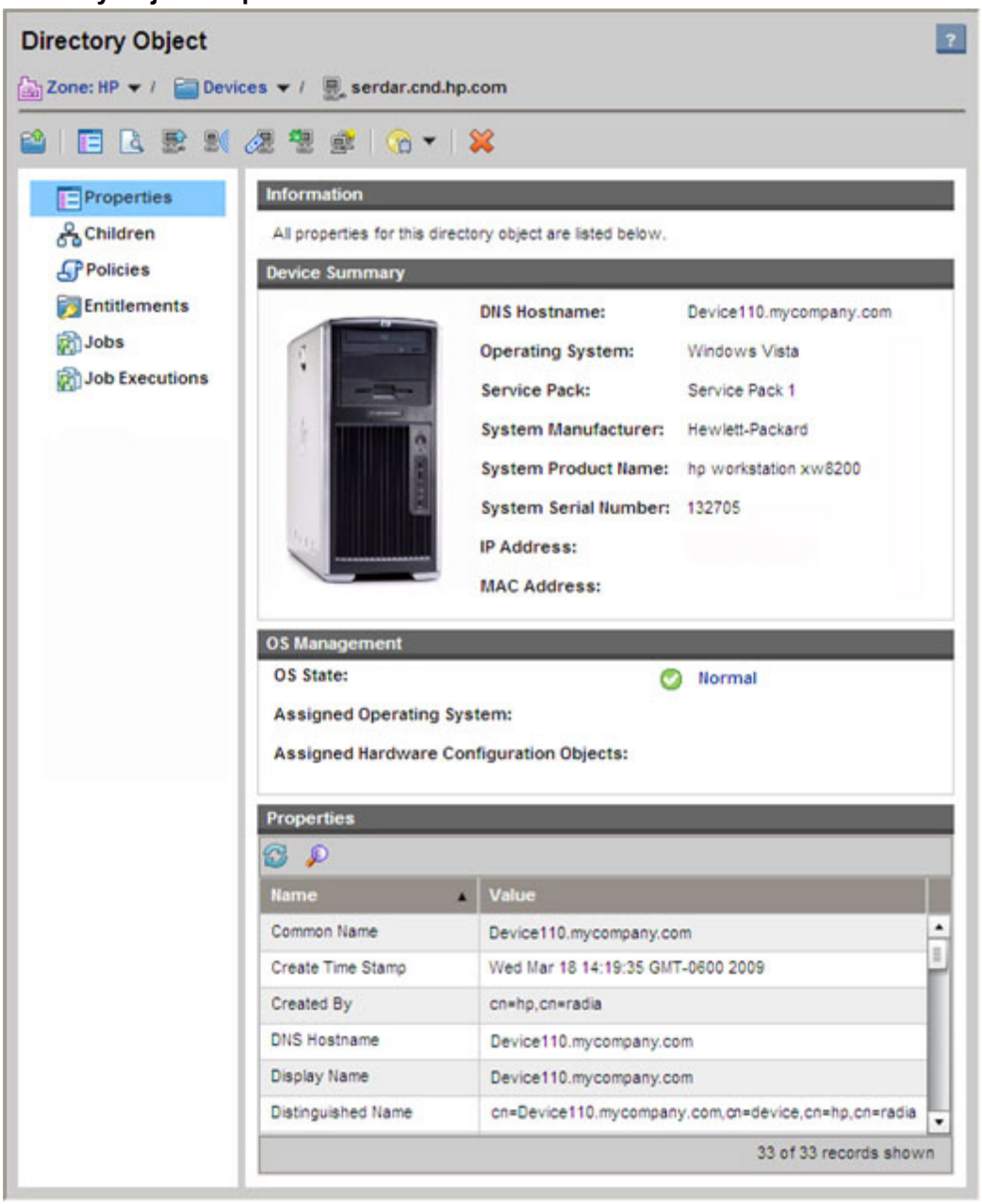


In this example, the upper toolbar (1) pertains to the All Devices group, and the lower toolbar (2) pertains to the selected Children (or Members) in the grid – in this case, Device110 and Device113.

Viewing Properties for an Object

When you select **View/Edit Properties** for a directory object, the properties of this object are displayed in a new browser window.

Directory Object Properties Window



From here, you can perform the following actions:

- Click **Children** to view the object's children. Click a child object to browse to that object in the content pane.
- Click **Members** to view the object's members. If the object has no members, this link is not present.
- Click **Policies** to view the object's local policy configuration, and to create policies for this object.
- Click **Entitlements** to view all resolved policies for this object.

- Click **Jobs** to view a list of current and past jobs for this object. If there are no jobs for this object, this link is not present.
- Click **Job Executions** to view a list of DTM job executions for this object. See "Jobs and Job Executions" on page 149 for more information.
- Click **Virtual Machines** to view a list of the virtual machines that exist on the server. This link is available only if the selected object is a VMware ESX Server. For additional information, see "Managing Virtual Machines" on page 159.

Searching for an Object

The RCA Console provides the ability to search for directory objects. This search is contextual. This means that when you initiate a search, the root of that search is the current directory object. You can initiate a search from either the main window or the Directory Object window—both contain a search button.

Note: Directory Objects that contain a large number of children may time out when retrieving a large number of records. Although the console may time out, the background process will continue to retrieve data until it reaches 10,000 records. If this happens, click the **Refresh** button to try the request again.

For directory objects with greater than 5000 child nodes, use the Search interface to navigate to a node within that list. This method will allow you to bypass possible time outs when browsing nodes with a large number of children.

To search for a directory object:

1. From the **Management** tab, **Directories** area, click the Search Directories  button.
2. From the Directory Search box, you can define the following parameters:
   - Specify the distinguished name (DN) for the search by selecting an item in the left navigation menu.
   - Select the **Scope** of the search: either the current level or the current level and all levels below it in the directory hierarchy.
   - Create a **Filter** expression by selecting an attribute, an operator, and typing in the criteria to match

     Note: When using the OBJECTCLASS filter, the only valid conditions are Equals or Does Not Equal. Also, certain directories, such as Active Directory, do not support wildcard characters included in the search strings for some attributes.
3. Click **Search**. The objects that match the criteria you specified are listed in the Search Results table.
4. Click **Reset** to begin a new search.

Managing Directory Policies

As indicated, you can create a directory object's policy and view its entitlements from the Management tab of the RCA Console.

Policy

A policy defines the services to which users and managed devices are entitled. It represents a designation of application service entitlements. Policies show which managed devices are assigned to which packages. A package is a unit of distributable software or data. Typically, to map services to users, you create users, assign users to groups, and then assign services to these groups. The policy information associated with these services determines which data are to be managed for the user, group, or computer; it determines what services should be distributed and managed for the agent. In the RCA model of policy-based management, it is possible to connect to an external Active Directory to define your policy entitlements.

Policy Types and How They Work

Before you start to manage policies for your directory objects, you should have an understanding of policy types and how they work together to determine the actual resolved policy values for a directory object.

There are three policy types.

The **Policy** type is the actual granting policy that defines the object's entitlement to services.

The **Default Policy** type is a policy that neither grants nor denies access. However, if access has been granted to a directory object, then the values in the Default Policy are used as a default template for the policy assigned to the object.

The **Override Policy** type is a policy that neither grants nor denies access. However, if access has been granted to a directory object, then the values in the Override Policy will override any equivalent attributes in the actual granting policy.

For a given application, more than one default may be encountered when resolving policy. In this case the defaults are ranked lowest to highest priority based on the `pri` attribute with the lower numeric value having a higher priority. The same applies to Override Policy.

The actual resulting policy that is returned to the Configuration Server will be the logical set union performed as an ordered overlay. In other words, same named attributes are replaced. This will be performed as follows:

1. Lowest to Highest Priority DEFAULTS (0...n occurrences)
2. Actual Granting Policy (always singular)
3. Lowest to Highest Priority OVERRIDES (0...n occurrences)

Policy Resolution Examples

This section provides examples demonstrating how the actual policy is returned to the Configuration Server when default and override policies are assigned to a directory object that has

policy entitlement to a service.

Example 1: simple override

- policy: Firefly <version=7 mode=typical>
- override: Firefly <version=8>
- OUTCOME: Firefly <version=8 mode=typical>

Example 2: simple default

- policy: Firefly <mode=typical>
- default: Firefly <version=7>
- OUTCOME: Firefly <version=7 mode=typical>

Example 3: default and override

- default: Firefly <mode=typical>
- policy: Firefly <version=7 issue=4>
- override: Firefly <version=8 mode=complete>
- OUTCOME: Firefly <version=8 issue=4 mode=complete>

Example 4: multiple defaults and multiple overrides

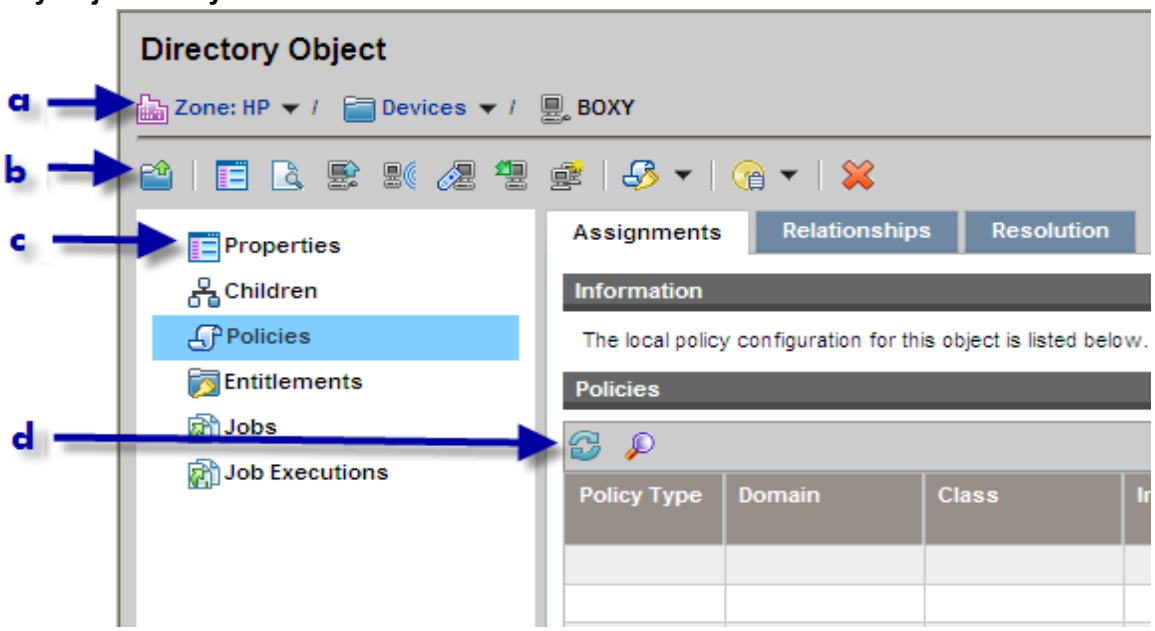
- default: Firefly <version=7> - Note: pri defaults to 10
- default Firefly <version=6 pri=5>
- policy: Firefly <mode=typical>
- override: Firefly <mode=complete> - Note: pri defaults to 10
- override: Firefly <mode=typical pri=5>
- OUTCOME: Firefly <version=6 mode=typical>

Note: Neither defaults nor overrides have any affect to policy resolutions that do not grant access to the subject (Firefly in the above example). Defaults and overrides only affect policy objects that are already granted access to an application. The effect that defaults and overrides have is only to refine the definition of that access by possibly altering a set of attributes. The set of attributes that are altered are those that contribute to the POLICY object that is present when the subject object is resolved on the Configuration Server.

How to Manage Policies for Directory Objects

From the Directory Object Properties window, you can manage the local policy configuration for a directory object by selecting the **Policies** link in the left navigation tree.

Directory Object Policy Detail



Legend

a	Path to selected directory object	
b	Directory object toolbar:	
		Browse to the parent object
		View/Edit properties of this object
		Search directories
		Import devices into the RCA device repository
		Create an HPCA job
		Start a new remote control session
		Deploy the RCA Agent
		Create a new group
		Launch the Policy Management Wizard (drop-down menu allows you to choose policy type)
		Perform an OS Management task
		Delete this Directory Object
c	Object links (see "Viewing Properties for an Object" on page 133)	

d	Policy Management toolbar:	
		Refresh
		Show/Hide filter

There are three tabs in the Directory Object Properties window when you select the **Policies** link in the left navigation tree. They allow you to view and assign policies, set defaults and overrides to policies, create relationships to other objects to influence policy inheritance, and to set resolution options that determine how the Policy Server will behave when resolving policies.

Note: When you click the **Policies** link, the RCA Console checks your permissions. If you do not have write permissions, the **Launch the Policy Management Wizard** icon will not appear on the toolbar.

The actions you can perform on these tabs are discussed in the following sections. In the examples used, we will create a policy for one device. "Directory Object Policy Detail " on previous page shows the different sections of the Directory Object Properties window. Use this figure to orient where you are in the management console when performing these tasks.

By way of recap, to navigate to the Directory Object Properties window to view and create policies, you do the following:

1. On the **Management** tab, expand the directory structure under Directories. The list of available directory services is displayed.
2. Click the directory service that you want to expand, and then the directory object of interest. In our example, it is **Zone:HP** > **Devices**. A list of the Devices directory object's children appears in the content pane.
3. To work with a device, navigate to that object, and select **View/Edit Properties** from the drop-down menu. A new browser window opens for that directory object.
4. Click the **Policies** link in the left navigation tree in the new browser window.

   As indicated in our example, the directory object we are selecting is a single device. We will create a policy for this single device.

Assignments

On the **Assignments** tab of the Directory Object Policies window, you can view the types of policies that have been assigned to a directory object.

As indicated in "Policy Types and How They Work" on page 136, there are three types of policies that can be assigned to an object, namely Policy, Default Policy, and Override Policy. You can entitle additional services to directory objects by performing the following policy type assignment procedures.

Assigning Policy to Directory Objects

1. From the drop-down menu on the **Policy Management Wizard** icon located on the Directory Object toolbar, select **Launch Policy Management Wizard (Policy)**. The list of available directory services for a given Service Domain is displayed on the right of the screen.

   This wizard allows you to entitle directory objects such as Groups or Users to services provided by the RCA Configuration Server. The tree located to the right represents the list of currently assigned services to this directory object. You can choose new services from the table or remove existing services from the tree to modify the policy configuration.

2. From the drop-down menu on the Service Domain field, select the Service Domain from which you want to select the Service.

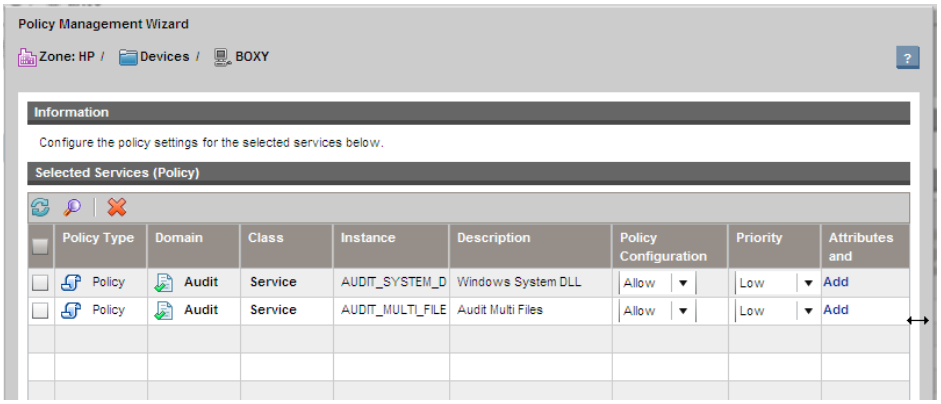
3. Select the box to the left of each service that you want to add.

   Note: If the service that you want to entitle does not appear in the Policy Management Wizard, you must wait for a few minutes, and then refresh the service list. Based on the package size and network bandwidth, the publishing process can take a few minutes to complete before the package is published as a service to the CSDB.

4. Click **Add to Selection** to move the service to the tree view on the right side of the wizard's screen.

5. Click **Next** when you have added all the services you need. A window opens displaying the selected services.

6. In this window, you will want to set the policy configuration, priority, and attributes for the selected services. The example screen shot below displays two Services from the Audit Domain.



   - Set **Policy Configuration** to either Allow or Deny.
   - Set **Priority** to Low, Medium, or High.
   - Click **Add** in the **Attributes and** column to add additional Client Automation attributes and expressions to the criteria for an object. For more information, see the *Radia Client Automation Enterprise Policy Server Reference Guide*.

> **Caution:** The **Attributes and** feature should only be used by experienced RCA Administrators who are extremely familiar with the Configuration Server Database and the RCA Infrastructure.

7. Click **Next** when you have configured the policies. A window opens displaying the summary information for the selected services.
8. Review the summary information for your configuration. Click **Commit** to save your changes.
9. Click **Close** to exit the wizard. Your newly created policies will be displayed in the Policies table on the **Assignments** tab. The policies will also be visible in the Entitlements table if you click the **Entitlements** tab.

Assigning Policy Defaults to Directory Objects

To assign policy defaults to directory objects, you follow the same procedure that you did for "Assigning Policy to Directory Objects" on previous page except that you select the **Launch Policy Management Wizard (PolicyDefault)** option from the drop-down menu of the **Policy Management Wizard** icon located on the Directory Object toolbar.

Assigning Policy Overrides to Directory Objects

To assign policy overrides to directory objects, you follow the same procedure that you did for "Assigning Policy to Directory Objects" on previous page except that you select the **Launch Policy Management Wizard (PolicyOverride)** option from the drop-down menu of the **Policy Management Wizard** icon located on the Directory Object toolbar.

Relationships

On the **Relationships** tab, you can link one object to another one for the purpose of acquiring policy inheritance from the linked object. For example, you may want a subscriber to inherit the policy assigned to an organizational unit (OU) in Active Directory although the subscriber is not a child of that OU. To do this, add a policy relationship to the device linking it to the OU and thereby inheriting the policies entitled to the OU. If a device is linked to a group by a policy relationship, the device will inherit the policies entitled to the group even if it is not a member. One typical use of policy relationships is to link entire OUs to one or more groups where policies are assigned. This type of linkage is only possible using a policy relationship since an OU cannot be a member of a group in LDAP.

This feature should be used sparingly in the directory model. Its primary goal is to represent policy relationships between two objects, that are not otherwise present in the form of parent-child or “memberOf” relationships; or when such a relationship is conditional on some dynamic criteria.

In the following example, we will add a policy relationship to a single device by linking it to another directory object.

To create relationships between objects:

1. Select the **Relationships** tab. The Policy Relationships for the selected device are listed in the displayed table. Initially, this table will be empty until you add policy relationships.
2. To add a policy relationship, click the **Add Policy Relationship** icon located on the Policy Management toolbar. The Add Policy Relationship window opens.
3. Use the search parameters or select a directory object to link to the currently selected device.
4. Select the box next to each linkable object to which you want to link the single device.
5. Click **Add** or **Add and Close** to add the relationship of the directory object(s) to the currently selected device. If you click **Add and Close**, you will exit the wizard after adding the relationship.
6. Click **Close** in the Execution Status pop-up window to close the window. All the policy entitlements of the related objects will be inherited by the originally selected device.

   The newly selected directory objects will appear in the Policy Relationships table for the originally selected device. Also, the entitlements page for the selected device will now display the policies of the directory objects to which it has been linked.

Resolutions

On the **Resolutions** tab, you can affect how a policy is resolved. For example, you may want to limit the scope of policy resolution for specific objects. To do this, use the policy resolution options displayed on this tab. These options are implemented as single-value integers that can be logically OR'd together to produce the expected behavior when the Policy Server resolves policies.

Use these flags very sparingly, as they can have a profound effect on the clarity and function of the policy model.

To set resolution options:

1. On the **Resolutions** tab, select the resolution option(s) you want to use to determine policy resolution. You can select from the following options:
   - **Secede**: Instructs the Policy Manager not to include any parent objects in the outcome. The primary use is to support semi-autonomous units within an organization.
   - **Continue**: Instructs the Policy Server to ignore all other attributes in this object. The parent object is still processed, unless **Secede** option is set.
   - **Break**: Instructs the Policy Server to end the policy resolution and return the condition to the client. In this situation, the client device should not apply policy. It can be used to implement "change control freezes" to prevent policy changes being applied to certain parts of an organization.
   - **Strict**: Instructs the Policy Server to ignore "memberOf" attributes, and only process Policy Flags, and Policy Connections.
2. Click **Save** to update the policy.
3. Click **Close** to exit the wizard.

Note: The effect of the resolution options on the policy model for the selected device will not be reflected in the entitlements page for the selected device.

How to Manage Policies for the Virtual Desktop Infrastructure

When managing virtual machines (VMs) in the Virtual Desktop Infrastructure (VDI), special attention is required for policy management of some types of VMs. In some cases, you will want a policy to deny services on a VM because it is not needed and will produce unnecessary network traffic.

A specific case is the Patch Service Domain. For certain types of VMs, you will want to set the policy configuration for the service to deny to prevent patch deployment on these virtual desktops since it is an unnecessary and expensive exercise.

The following sections provide some VDI background and describe how to configure your policy entitlement efficiently in this type of virtual environment. The sections covered include the following:

- "VDI Overview " below
- "Adding Cloned Desktops to Active Directory Group" on next page
- "Denying Patch Services to Cloned Desktops" on next page

VDI Overview

VDI is a technology for the hosting and virtualization of individual client operating systems like Windows XP Professional, Windows Vista or Linux on physical host machines. The intent is to be able to deploy, secure, and manage enterprise desktops in the data center.

The VMware View was formerly known as Virtual Desktop Infrastructure (VDI). The View uses the linked clone technology that allows multiple desktops to be deployed from a single base image. Automated desktop pools can use the linked clone feature to rapidly deploy desktops from a single parent VM. View Manager uses VMware View Composer to create and deploy linked cloned desktops from VMware vCenter Server.

The XenDesktop is the VDI solution from Citrix. XenDesktop is used to manage virtual desktop connections and assign users to dedicated or pooled virtual desktops. Provisioning Services creates and provisions virtual desktops from a single desktop image on demand, thus optimizing storage utilization and providing a pristine virtual desktop for each user each time the user logs on. The Provisioning Services VM Template is used for creating a VM-based pooled desktop group using the XenDesktop Setup Wizard.

The cloned desktops created using VMware View or the Virtual Desktops created using XenDesktop can then be managed in the RCA Enterprise Console. The cloned desktops can be grouped into a single Organizational Unit (OU) and a policy can be enforced to this OU to deny services. Only the parent VM should be excluded from this deny policy so that it will be entitled to all those services installed on it. The cloned desktops can be updated automatically from the parent VM using the VMware View to reflect the services that were installed on the parent base image.

Adding Cloned Desktops to Active Directory Group

You must create a group in AD that contains all the cloned desktops that you want to exclude from entitlement. The group is an OU. The OU is a directory object in RCA Enterprise, which you can associate with a policy that denies patch services to this OU. For more information, see "Denying Patch Services to Cloned Desktops" below.

To create a new group for cloned desktops in the Active Directory:

1. Create a new group in AD.
2. Add the cloned desktops to the group. When searching for the cloned desktops to add to this group, use the pattern used to name the devices. The pattern search string will list only the cloned desktops simplifying the task of adding them to the group.
3. Click **OK**.

Note: If you add more cloned desktops to your network, ensure that they are added to this group. It is not done automatically.

Denying Patch Services to Cloned Desktops

Now that you have created an OU in AD, you can associate a policy that effectively denies patch acquisition to the devices contained in this OU.

To deny patch services to cloned desktops:

Follow the generalized procedure outlined in "Assigning Policy to Directory Objects" on page 140. However, in this procedure, which is specific to entitling a policy to devices that *denies* a service, note the actual values you must provide to achieve this goal.

1. Select **View/Edit Properties** for the OU directory object that contains the cloned desktops.
2. From the drop-down menu on the **Policy Management Wizard** icon, select **Launch Policy Management Wizard (Policy)** to add a normal policy.
3. In the Policy Management Wizard, select **Patches** as the Service Domain.
4. Select the **DISCOVER_PATCH** and **FINALIZE_PATCH** services in the list and click **Add to Selection**.
5. Click **Next**.
6. In the Selected Services list, select all the services and specify the following changes for all of the services listed:
   - Set Policy Configuration to **Deny.**
   - Set Priority to **High.**
7. Click **Next** and **Commit** to save the changes.

This procedure has assigned a policy that denies patch services to the OU that contains the cloned desktops. Since the priority of this policy is specified as high, it will get resolved above all the other policies within its hierarchy. You can verify this by viewing the Entitlement list of policies for any one of the devices in the list.

Now when the patch connect is run on any of the cloned desktops contained in the specified OU, the patch service entitlement is not resolved, and the patch will not be installed. This does not affect other services which are entitled for the cloned desktops, and they are thus resolved.

You must ensure that only cloned desktops are contained in this OU. If any other device is added to this OU, it will also be denied patch services.

You can deny patch services through policy entitlement at any level; that is, it can be done at the container, OU, or device level.

Note: It is important to apply the policy at the correct level in the hierarchy so that its affects only the required devices and not all devices.

Service Information

After signing in to the RCA Console, you can view the services that are available from your Configuration Server. A service is a set of data managed as a unit – for example, an application. Services are created using the CSDB Editor. See the *Radia Client Automation Enterprise Administrator User Guide* for more information about services.

To view available services:

1. On the **Management** tab, click **Services**. The list of available Configuration Server Database Domains opens.
2. Click the Domain that contains the Services that you want to see.
3. To narrow the list of available services displayed, click the **Show/Hide Filter Input** button to display the filter options.
4. Click a Service to view its details.
   - The **Properties** tab shows the attributes of the Service from the Configuration Server Database (CSDB).
   - The **Reporting** tab shows summary reports for the selected Service.

You can view the summary reports for all the services in the **Reporting** tab on the Services area.

Importing Devices

Before you can deploy the RCA Agent to a device, you must import that device into RCA. You must also import any VMware ESX Server that you want to manage using RCA.

When you import a device, a directory object is created for that device. No attempt is made, however, to verify that you have specified a valid device.

To import devices:

1. On the **Management** tab, go to the Directories area, and click **Devices**.
2. Click the (Import Device Wizard) button.
3. In the **Device IP/Host Name** text box, type or paste a comma-separated list of device host names or IP addresses.

4. In the Device Classification drop-down, select the appropriate classification for the group of devices.
   - **No Preset Classification** – Devices are imported with no classification.
   - **VMware ESX Server** – Enables the Virtual Machines link in the Directory Object window for each device imported with this classification. For more information, see "Managing Virtual Machines" on page 159.
5. Click **Add**. Devices are added to the import Devices list.

   To remove a device from the list, select the check box to the left of the device and click the (Remove) button.
6. Review the list, and click **Commit**. Devices are imported into the Devices container. They are also added to the All Devices group.
7. Click **Close** to acknowledge the dialog.

To remove a device:

To remove a device that was previously imported, browse to the device object page and click the (Delete this Directory Object) button.

Managing Groups

Groups are used to perform tasks on many devices at once, such as deploying the RCA Agent or creating a job to notify devices when updated software is available. Devices are added to groups based on search criteria that you define during group creation. The following sections describe the different group management tasks available.

To create an external directory group:

Groups for mounted external directory sources (LDAP or Active Directory, for example) must be created using the tools provided by the directory service. Contact your system administrator for details.

To create an internal directory group:

The following procedure creates groups for internal directories. Groups that you create in the RCA Console are created in the internal zone under the Groups container.

1. On the Management tab tool bar, click **Create a New Group**. The RCA "Group Creation Wizard" on page 347 opens.
2. Follow the steps in the wizard to create the group.

To modify a group description or devices:

1. Use the navigation tree, and select the group that you want to modify.
2. Use the tool bar or the group context drop-down menu, and select **View/Edit Properties**. The group's directory object window opens.
3. Click the **Properties** link to view the properties page and to modify the group name or description. Click **Save** to commit any changes.
4. Click the **Members** link to view the list of devices that belong to the group.

5. Use the **Add Devices** or **Remove Devices** tool bar buttons to update group membership.
6. When you are finished, close the directory object window.

To remove a group:

1. Use the navigation tree, and select the group that you want to remove.
2. Click **Delete this Directory Object**.

   This removes only the group object. It does not remove the devices in the group.

Deploying the RCA Agent

The RCA Agent is used to manage devices in your environment. Deploy the Agent to devices using the Agent Deployment Wizard. For additional information about the RCA Agent, see the *Radia Client Automation Enterprise Application Manager and Application Self-Service Manager Reference Guide.*

You can deploy the Agent to single devices or to devices belonging to a group. Use the directory object tree to locate the devices, then use the Agent Deployment Wizard to create a deployment job.

In order for the Agent to be deployed successfully, the following may be required on the client devices:

- Windows Firewall should be disabled.
- The Agent must be reachable by the server over the network.
- If deploying to Windows 8, the Remote Registry service must be enabled.
- If deploying to Windows XP, Simple File Sharing must be disabled.
- If deploying to Windows Vista and later operating systems, access to the Administrative share (C$) on Windows Vista devices is disabled for locally defined administrators. Therefore, Windows Vista devices should be part of a domain, and the domain administrator's credentials should be specified during Agent deployment. If the devices are not part of a domain, additional steps are required to allow access for local administrators. See the following link on Microsoft's support web site for detailed steps:

  http://support.microsoft.com/kb/947232/en-us

  After making these changes, reboot the device.

To deploy the RCA Agent:

1. From the directory object tree, select the directory object that contains the devices to which you want to deploy the Agent.
2. Select the devices from the list and click **Launch the HPCA Agent Deployment Wizard**. The Agent Deployment Wizard opens.
3. At **Step 1**:
   a. Specify the credentials to use when deploying the Agent. These credentials should have adequate administrator permissions to perform the installation.

b. To install the Agent in silent mode, select the **Silent Install** check box. This will prevent an installation user interface from opening on the target device.

4. Click **Next**.
5. At **Step 2,** type the schedule information for when the Agent Deployment job should run.
6. Click **Next**.
7. At **Step 3**, review the summary information for the job.
8. Click **Submit**.

When you finish the steps in the wizard, an Agent Deployment job is created. A deployment job is complete when the Agent has been deployed to all devices included in the job. Use the **Jobs** area (see "Managing Jobs" below) to view the status of any jobs.

Managing Jobs

Use the Jobs area on the Management tab to view and manage current and past jobs. The Jobs area includes two categories:

- The **All Jobs** category lists jobs submitted by all RCA Console users.
- The **My Jobs** category lists jobs submitted by the RCA Console user who is currently signed on.

Each category contains a list of **Current Jobs** that are either running or waiting to run and **Past Jobs** that have finished running.

You can manage three different types of jobs in the RCA Console:

Types of Jobs

Job Type	Description
Notify	The RCA Console tells the target devices to connect to the Configuration Server to perform a certain action. This is a centralized (server-push) method of job management. The RCA Console uses an internal process engine to manage these types of job.
Distributed Task (DTM)	The target devices periodically synchronize themselves with the RCA Core and receive instructions to perform a particular action according to a specified schedule. You can configure and manage this schedule in the RCA Console. This is a distributed (client-pull) method of job management, because jobs can run independent of the RCA Core.
Deployment (RMP)	These jobs involve Agent or OS deployment. You can view information about RMP jobs in the RCA Console, but you cannot modify it. Deployment jobs, like Notify jobs, are managed centrally (server-push).

Current and Past Jobs

The Current Jobs page lists jobs that are running or waiting to run. The Past Jobs page lists jobs that have finished running. For each job, the following information is shown:

- **Job ID** – The unique identifier for this job. This ID is assigned by RCA when the job is created. To see the job details for a particular job, click its Job ID.
- **Type** – Notify, DTM, or RMP.
- **Display Name** – The name specified when the job was created.
- **State** – Enable, Disabled, Running, Completed, or Scheduled. Jobs that are enabled can be scheduled to run on target devices.
- **Status** – The current status of the job: Success, Failure, or Unknown (while the job is either Running or Scheduled).
- **Description** – A text description specified when the job was created.
- **Schedule** – The schedule associated with the job.
- **Target** – The target device or group where the job will run.
- **Action** – The action that is taken when the job runs on the target devices.
- **Create Time** – The date and time when this job was created.
- **Created By** – The RCA Console user who created the job.
- **Last Execution Time** – The date and time that the job was last run. If the job has never been run before, the date of 12/31/1969 is displayed.

Use the buttons at the top of the Jobs table to perform the following actions:

Jobs Table Controls

Icon	Description
	Refresh data
	Show/Hide filter input
	Delete the selected job (or jobs)
	Enable the selected job (or jobs) – applies to current DTM jobs only
	Disable the selected job (or jobs) – applies to current DTM jobs only

Jobs and Job Executions

A **job** is the framework that defines the parameters for a particular action and target device or group. A job consists of three primary components:

- Target – a device or group of devices on which the job will run
- Action – the command that will be performed
- Schedule – when the action should be executed on the target

When a job is running, waiting to run, or has finished running, a **job execution** represents an instance of that job on a particular device.

Targets

A target is a single device or a group of devices on which a job will run. This is typically an Active Directory group whose members can change over time. The target is specified when the job is created.

The Target Details window provides information about the target devices associated with one or more jobs. The window contains three tabs:

- The **Target Devices** tab contains a list of all the devices associated with this job. To view information about a particular device, select **View/Edit Properties** from the shortcut menu for that device.
- The **Job Executions on Target** tab shows you any job executions that are scheduled to run, are running, or have run for this job on this target (or target group).
- The **All Jobs for Selected Target** tab shows you all the jobs that use this target (or target group).

To access the Target Details window:

1. In the Current Jobs or Past Jobs table, click a **Job ID**.
2. In the Job Details window, click the **Properties** tab.
3. In the Target section, click the target group or device name.

You can also access the Target Details window by selecting a value in the **Target** column in either the Current Jobs or Past Jobs table.

Schedules

You can schedule a DTM task to run once at a particular time or periodically according to the parameters that you specify.

The Schedule Details window enables you to view information about the schedule associated with an existing DTM job. If this job is a current job, you can also modify the schedule.

To access the Schedule Details window:

1. In the Current Jobs or Past Jobs table, click a **Job ID** for a DTM job.
2. In the Job Details window, click the **Properties** tab.
3. In the Schedule section, click **Modify**.

To specify a schedule for a DTM job:

1. From the **Begin the task** list, select **On a schedule** or **At startup**.

   If you select At Startup, you can skip the rest of these steps.
2. Select the frequency with which this job should run: once, hourly, daily, weekly, or monthly.
3. If you selected a frequency other than “once,” specify the **Every** information to define the recurrence interval for this job.
4. Specify the **Start Date** for the job.

5. If you want to stop initiating new job executions for this job on a certain date, select the check box to the left of the **End Date** field, and specify the end date.
6. Specify the **Start Time** for the job.
7. If you want to stop initiating new job executions for this job at a certain time, select the check box to the left of the **End Time** field, and specify the end time.
8. If you want the job to start at a randomized time between your Start Time and End Time, select the **Randomize Start Time** box.

See "Create a New DTM or Notify Job" on page 154 for more information.

Job Details for DTM Jobs

When you click a Job ID for a DTM job in either the Current Jobs or Past Jobs tables, the Job Details window opens, and the following information is displayed:

- The **Summary** tab displays the ID, name, description, and creation time for the job as well as the job's current state (Enabled, Disabled, or Completed). This tab also includes a pie chart that shows you the status of the job on the target devices (Success, Failure, Warning, or Unknown).

  When a job execution for this job is running, the status is Unknown.

  A DTM job is moved to the Completed state when an End Date is used in its schedule, and this End Date has passed.

- The **Properties** tab contains information about the job, including the description, action, target, and schedule used to create the job.

  For information about the target devices associated with this job, click the target name. For more information, see "Targets" on previous page.

  To view or change the schedule for this job, click the **Modify** schedule link. You can only modify the schedule for current jobs. For more information, see "Schedules" on previous page.

- The **Job Executions** tab shows the job executions that have been scheduled for this job. This includes job execution that have already completed.

  To view more information about a particular job execution, click the **Id** for that job execution in the table. The Job Execution Details window opens. For more information, see "Job Execution Details" on next page.

The Job Details window contains slightly different information for Notify jobs. For more information, see "Job Details for Notify Jobs" below.

Job Details for Notify Jobs

When you click a Job ID for a Notify job in either the Current Jobs or Past Jobs tables, the Job Details window opens, and the following information is displayed:

- The **Summary** tab displays the ID, name, description, and creation time for the job as well as the job's current state.

Notify Job State Descriptions

State	Description	Example
Scheduled	The job has not yet started running.	A Notify job has been scheduled to run at some point in the future but has not yet started.
Running	The job has not yet reached the end state. Running jobs are included in the Current Jobs list.	A running Notify job is in the process of notifying each device.
Completed	The job has reached its end state, and all steps have been processed. Completed jobs are included in the Past Jobs list.	A Notify job is complete when all devices included in the job have been notified.

This tab also includes a pie chart that shows you the status of the job on the target devices (Running, Success, Failure, Warning, or Unknown).

- The **Properties** tab contains information about the job, including the action, target, and schedule used to create the job.

  For information about the target devices associated with this job, click the target name. For more information, see "Targets" on page 150.

- The **Job Executions** tab shows the status of the *most recent* job execution on each target. This includes job executions that have already completed.

  To view more information about a particular job execution, click the **Id** for that job execution in the table. The Job Execution Details window opens. For more information, see "Job Execution Details" below.

The Job Details window contains slightly different information for DTM jobs. For more information, see "Job Details for DTM Jobs" on previous page.

Job Details for RMP Jobs

When you click a Job ID for an RMP job in either the Current Jobs or Past Jobs tables, the Job Details window opens. The information displayed is the same as that displayed for a Notify job (see "Job Details for Notify Jobs" on previous page).

Job Execution Details

For DTM jobs, the Job Executions tab lists the most recent job execution for each job that is currently running or has finished running on all target devices. For Notify and RMP jobs, this tab lists the most recent job execution for each job that is currently running, is waiting to run, or has finished running on all target devices.

The following information is displayed:

- **ID** – The unique identifier for this job execution. Note that this ID pertains only to this execution (instance) - it is not the same as the Job ID specified in the Jobs table. To see the job details for a particular job execution, click its ID.
- **Type** – Notify, RMP, or DTM (distributed task)

- **State** – Running, Completed, or Waiting to Start (for Notify and RMP jobs). For more information, see "Job Execution States" below.
- **Description** – A text description specified when the job execution was created.
- **Summary** – A status message pertaining to the job execution.
- **Start Time** – For current jobs, this is the time this job execution is scheduled to start on the target devices. For past jobs, this is the time that the job execution started.
- **End Time** – For current jobs, this is blank. For past jobs, this is the time that this job execution stopped.
- **Job** – The Job ID of the job on which this execution is based.

You can use the buttons at the top of the table to manage existing job executions:

Job Executions Actions

Icon	Description
	Refresh data
	Show/Hide filter input
	Delete the Selected Job Executions

Note that some buttons are only available during certain job states. A job execution that has completed, for example, would not have a Resume, Pause, or Cancel button.

Click the Job ID of any job to open the Job Details window. See "Job Details for Notify Jobs" on page 151 or "Job Details for DTM Jobs" on page 151 for additional information. See "Job Execution States" below for additional information about the status of each job.

Job Execution States

RCA Console job executions can include any number of steps, depending on the job type. For example, Notify jobs include a step for each device to be notified. The execution status of those steps determines the current job execution state.

Job Execution State Descriptions

State	Description
Running	The job execution has not yet reached the end state. Running job executions are included in the Current Job Executions list.
Completed	The job execution has reached its end state and all steps have been processed. Completed job executions are included in the Past Job Executions list
Waiting to Start	The job execution is based on a job that is in the Scheduled state.

Create a New DTM or Notify Job

You can use the HPCA Job Creation Wizard to create a new DTM or Notify job. To create a new Agent deployment job, see "Deploying the RCA Agent" on page 147. To create a new OS deployment job, see "Managing Operating Systems " on page 168.

To create a new DTM or Notify job:

1. On the **Management** tab, go to the **Directories** area, expand the zone that you want to use.
2. Expand the list of **Groups**, **OU**, or **Devices** that you want to work with.
3. From the drop-down menu for the group, OU, or device, select **Create a Job**. The HPCA Job Creation Wizard opens.

   Alternatively, you can select a group, an OU, or one or more devices from the grid and then click the **Launch HPCA Job Creation Wizard** icon on the toolbar.

   > **Note:** Jobs created for a group are applied only to child devices in the group. These jobs are not applied to devices in the member groups or OUs within the group.
   >
   > Notify jobs created for an OU are applied to child devices in the OU and the member OUs. These jobs are not applied to devices in the member groups within the OU.

4. In the **Job Type** list, select **DTM** or **Notify**.

   > **Note:** You can select only **Notify** job type for an OU.

   In a DTM job, the agents on the target devices connect to the RCA Core server to get a list of jobs and then execute those jobs when the job timers expire. A DTM job is most appropriate when you want to execute this job on a regular schedule on these devices.

   In a Notify job, the RCA Core server asks the RCA Agent to perform the scan. A Notify job is most appropriate when you want certain target devices to execute the job once at a specific time – or immediately.

5. Specify a **Name** and **Description** for your job.
6. In the **Job Action Template** list, select the Job Action Template that you want to use for this. See "Job Action Templates" on page 301 for more information.
7. If you want to specify parameters for the job action that are not specified in the Job Action Template, type those in the **Additional Parameters** box.
8. Click **Next**.
9. Specify the schedule for this job. See "Schedules" on page 150 for details.
10. Click **Next**.
11. Review the settings you have specified, and click **Submit** when ready.

To view the job, click the Jobs area on the Management tab.

Note: If you modify the schedule for a DTM job, you must refresh that schedule on each of the target devices. For more information, see "Removal of Old Job Execution Records" on page 157.

Delete a Job

To delete a current or past job, select the job in the Current Jobs or Past Jobs table, and click the **Delete Selected Job** icon. Note the following:

- Notify jobs that are currently running cannot be deleted.
- For DTM jobs, the job disappears from the Current Jobs list when you click the icon, but job executions from that job remain visible in the Directory Object view for each target device (select **View/Edit Properties** to display).

  After you delete a DTM job, that job is no longer available to be downloaded to target device in subsequent agent synchronizations with the RCA Core server. Target devices that already have the deleted job can still execute the job until they synchronize with the RCA Core server.

Refresh DTM Schedules on Targets

If you modify the schedule for a DTM job on the RCA Core server, you must also refresh that schedule on each target device. You can do this by creating a job using the Refresh DTM Job Schedules sample job action template.

By default, there is a DTM_DAILY_TIMER in the Configuration Server Database (CSDB) that can be entitled to a managed device to instruct its agent to perform a synchronization with its Core server once a day for job information.

A Refresh DTM Schedules job provides another way to schedule the synchronization with the Core server. For example, a Refresh DTM Schedules job can be created to ask agents to synchronize with the Core server every 12 hours for job information. To the agent of a target device, this Refresh DTM Schedules job will be run just as any other agent job – such as a Software Connect – when the job timer expires.

Note: Before you can successfully run a Refresh DTM Schedules job on a client device, the RCA Agent on that client must have performed a prior connect operation to the RCA Core server.

Creating a Refresh DTM Schedules Job

To create a Refresh DTM Schedules job:

1. In the Management tab, **Directories** area, navigate to the object that contains the target devices for the pertinent DTM job (or jobs).
2. Select the target devices that you want to refresh.
3. Click the tool bar icon to launch the **HPCA Job Creation Wizard**.

4. To refresh immediately, select **Notify** from the **Job Type** drop-down box. To refresh on a schedule, select **DTM**.

   If you select **DTM**, when the target devices synchronize with the Core server, they will acquire this job. It will instruct them to connect back to the Core server for job information based on the schedule settings that you specify.

   If you want agents to use the new synchronization schedule sooner, it might be helpful to *also* schedule a **Notify** Refresh DTM Schedule job to instruct the agents on target devices to synchronize with the Core server at a specified time and *then* download the **DTM** Refresh DTM Schedules job.

5. Enter a name and description for the refresh job.
6. In the **Job Action Template** list, select **Refresh DTM Job Schedules**
7. Click **Next**.
8. Enter the schedule settings (see "Schedules" on page 150), and click **Submit**.

   The job is added, and the target devices will refresh their DTM job schedules based on the settings that you defined.

To view the status of the job, click the **Jobs** area on the Management tab.

Device Resolution for Notify Jobs

Devices included in a Notify Job are resolved according to the order defined in the following file:

<tomcatDir>`\webapps\em\WEB-INF\Console.properties`

By default, *<tomcatDir>* is as follows.

<InstallDir>`\tomcat`

The default order is:

```
group.target.host.attributes=ipaddress,dnshostname,displayname,cn
```

If necessary, this list can be modified. If you make changes to this file, you must restart the RCA Tomcat service.

For devices that could not be resolved, a message is displayed in the Job Details window. You can open the Job Details window by clicking the Job ID.

Device Resolution for DTM Jobs

Devices included in a DTM job are resolved in the following order:

1. ipaddress
2. dnshostname
3. displayname
4. cn

A service periodically runs to resolve target devices for DTM jobs. This service is configurable in the following file:

<tomcatDir>`/webapps/ope/config/dtm.properties`

Parameters for Device Resolution Service for DTM Jobs

Parameter	Default Value	Comment
enableTargetRefresh	`true`	Enables or disables this service
rmpProtocol	`http\://`	Can be `https\://` for SSL
rmpServer	`localhost`	RCA Portal server
rmpPort	`3471`	Portal server port to which to connect
rmpUser	`admin`	
rmpPassword		Not shown here for security
userDS	“”	User directory to which to connect
targetRefreshInterval	`360`	Default is 6 minutes (360 seconds)
targetRefreshInitDelay	`60`	Seconds to wait after startup before DTM starts the target resolution service

Removal of Old Job Execution Records

You can specify how long records of past DTM and Notify job executions are stored in the RCA database. You can also specify the maximum number of records that should be stored. This is configured in the following file:

<tomcatDir>`\webapps\ope\config\dtm.properties`

By default, *<tomcatDir>* is as follows.

<InstallDir>`\tomcat`

Use the following parameters to specify these settings:

```
dtmJobRunKeepDays=30

opeJobRunKeepDays=30

dtmJobRunKeepRecords=-1

opeJobRunKeepRecords=-1
```

The default settings are shown here. for the period of time specified by these parameters. The value of -1 indicates that there is no limit on the number of records that can be stored.

Creating Satellite Synchronization Jobs

Satellite Servers are used to allow for data caching and the distribution of configuration settings to managed devices. Satellites must be synchronized with the Core server to make the latest data available to those devices. You can perform a synchronization from the Satellite Console, or this synchronization task can be scheduled by creating a job in the RCA Console.

Note: Before you can synchronize data on a Satellite Server, you must have initially configured your Satellites. See the *Radia Client Automation Enterprise Installation and Upgrade Guide* for details.

Note: Before you can successfully run a Satellite Synchronization job on a client device, the RCA Agent on that client must have performed a prior connect operation with `COP=Y` to the RCA Core server.

To create a Satellite Synchronization job:

1. In the Management tab, **Directories** area, navigate to the object that contains the Satellite device.
2. Select the Satellite device and launch the **HPCA Job Creation Wizard** by clicking the  tool bar icon.

   Note: If you select a device that is not a Satellite server, the job will fail.
3. To synchronize a satellite immediately, select **Notify** from the **Job Type** drop-down box. To synchronize on a schedule, select **DTM**.

   If you select **DTM**, this Satellite Synchronization job will be downloaded to the Satellite only *after* the agent on the Satellite device has performed a Refresh DTM Schedule.
4. Type a name and description for the synchronization job.
5. Select the **Job Action Template** for the synchronization type you would like to schedule:
   - **Satellite Synchronization (All)**

     Select this template to synchronize both configuration settings and data.
   - **Satellite Synchronization (Configuration)**

     Use this template to synchronize only configuration settings.
   - **Satellite Synchronization (Data)**

     This template will synchronize data, only.

     Note: When the ZBASE time stamps are the same in the source and destination data, the metakit files are not created and downloaded by the Distributed Configuration Server.
6. Click **Next**.
7. Type the schedule settings (see "Schedules" on page 150), and click **Submit**.

   The job is added and the Satellite server will synchronize data or configuration settings based on the settings you defined.

   To view the status of the job, click the **Jobs** area of the Management tab.

Managing Virtual Machines

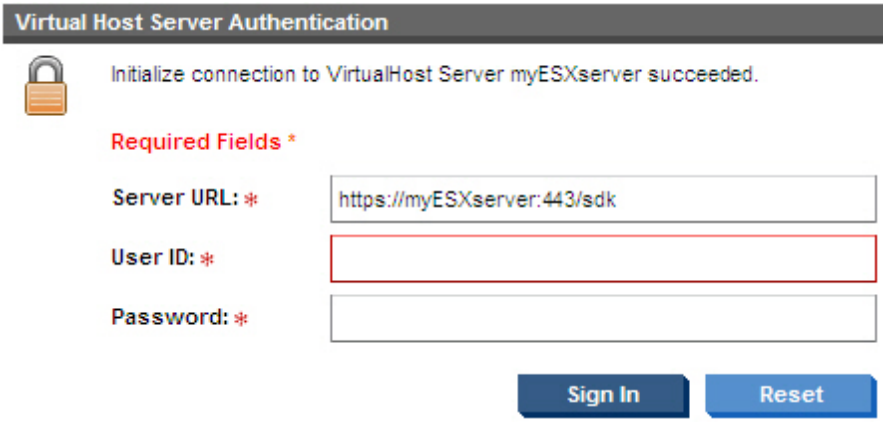
The RCA Console enables you to manage the virtual machines running on your virtual hosting servers. For example, you can create and manage virtual machines on an existing VMware ESX Server in your environment.

To manage your virtual machines:

1. On the **Management** tab, expand the zone containing the devices that you want to manage.
2. In the left navigation tree, click **Devices**.
3. In the list of devices, locate your ESX Server in the list of devices.
4. In the drop-down menu for this device, click **View/Edit Properties**. The Directory Object Properties Window opens in a separate browser.
5. In the Directory Object window for your ESX Server, click the **Virtual Machines** link in the left navigation menu.

   Note: The Virtual Machines link is only visible if this device was imported using the **VMware ESX Server** device classification. See Import Devices in the Configuration chapter for more information.

   If this is the first time you have clicked this link for this ESX Server during this RCA Console session, you will need to provide login credentials:

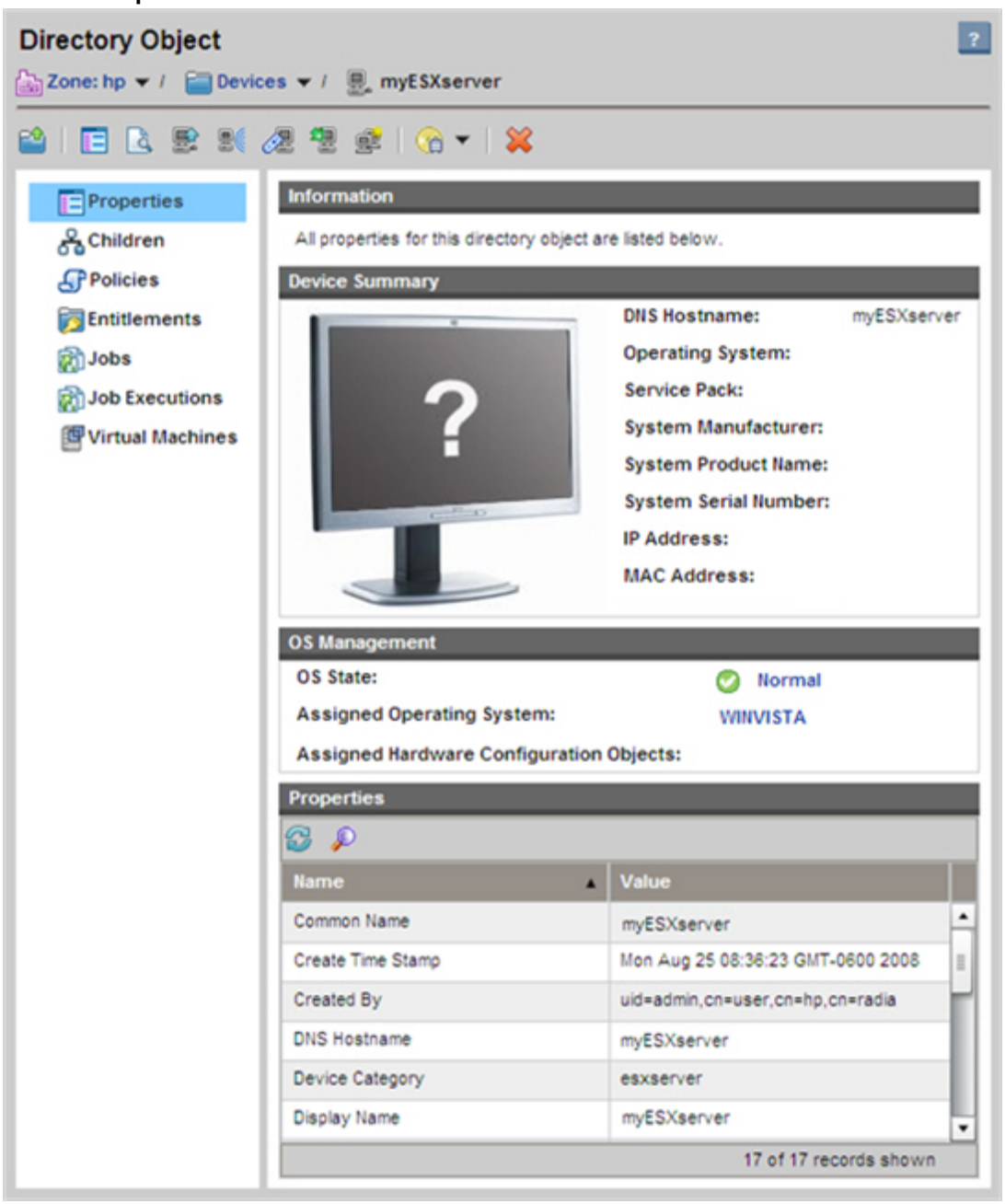


   Type the **User ID** and **Password** for the ESX Server, and click **Sign In**.

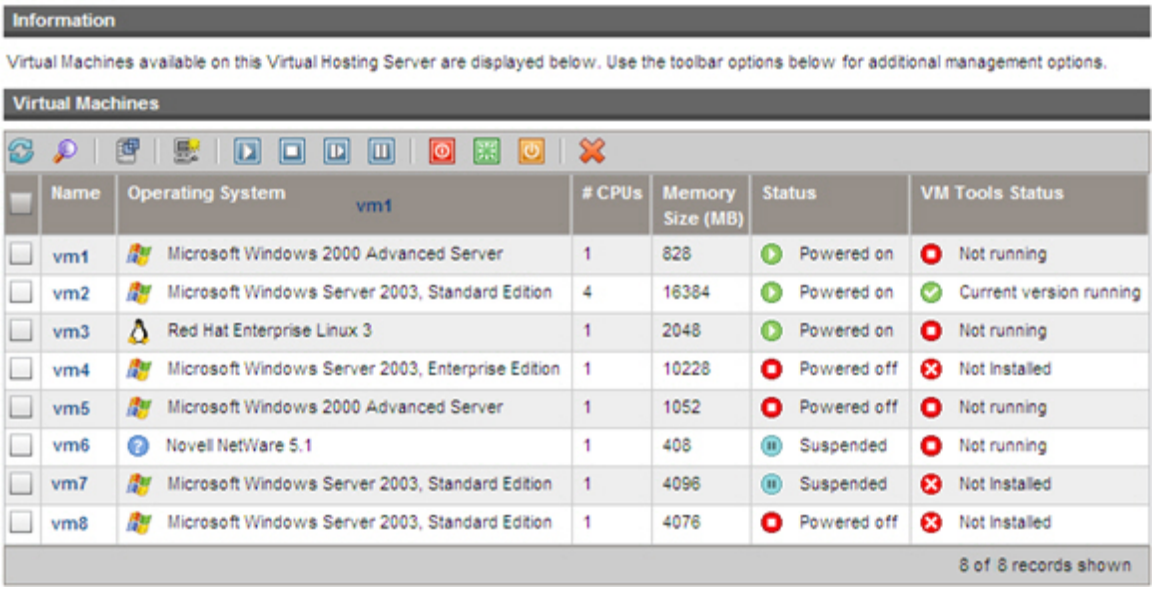
   A list of the virtual machines hosted by this ESX Server is displayed, as shown in "List of Virtual Machines Hosted by an ESX Server" on page 161.

   To view the properties for a particular virtual machine, click its name.

Device Properties for a VMware ESX Server



List of Virtual Machines Hosted by an ESX Server



The columns in the Virtual Machines list contain the following information:

Virtual Machine List Columns

Column Name	Description
Name	The name of the virtual machine
Operating System	The operating system of the virtual machine
# CPUs	The number of CPUs allocated to the virtual machine
Memory Size	The amount of memory allocated to the virtual machine
Status	The current status of the virtual machine
VM Tools Status	The current status of the VM tools on the virtual machine

Click the name of a virtual machine to open the Virtual Machine Properties window for that machine.

You can use the following controls to create and manage virtual machines on your ESX Server:

Virtual Machine Toolbar

Icon	Description
	Refresh Data
	Show/Hide Filter input
	Display VM Host System Properties
	Create New Virtual Machine
	Suspend the Selected Virtual Machines

Icon	Description
	Reset the Selected Virtual Machines
	Stop the Selected Virtual Machines
	Start the Selected Virtual Machines
	Standby OS on the Selected Virtual Machines [1]
	Reboot OS on the Selected Virtual Machines [1]
	Shutdown OS on the Selected Virtual Machines [1]
	Delete the Selected Virtual Machines
[1] Requires VMware Tools to be running on the virtual machines.	

Select the check box for each virtual machine you want to manage, and then click the appropriate virtual machine control to complete the required action.

Creating New Virtual Machines

The **Create New Virtual Machine**  control in the Virtual Machines table enables you to create a new virtual machine on the ESX Server by using the Virtual Machine Creation Wizard. This wizard prompts for information similar to the information requested by the VMware virtual machine creation wizard. You should be familiar with VMware terminology before using this wizard.

To create a new virtual machine:

1. Follow steps 1-5 under "Managing Virtual Machines" on page 159 to open the Virtual Machines list for your ESX Server.
2. Click **Create New Virtual Machine**  . The Virtual Machine Creation Wizard opens.
3. Provide the following information for the virtual machine you want to create:
   - **Data Center**: Use the drop-down list to select the data center in which to create the new virtual machine.
   - **Host System**: Use the drop-down list to select the host system for the virtual machine.
   - **Name**: Type a name for the virtual machine. Virtual machine names can be up to 80 characters long and can contain alpha-numeric characters, spaces, hyphens, and underscores. Virtual machine names must be unique within each data center and within each folder.
   - **Description**: Type a description of the virtual machine.
4. Click **Next**.
5. Use the drop-down list to select a **Data Store**. Be sure to select a data store with enough space to store the virtual machine and its virtual disk files.
6. Type the **Disk Size**. Type or use the up and down arrows to enter the Disk Size in megabytes, or use the slider tool to enter the size in gigabytes.

7. Click **Next**.
8. Select the **Guest Operating System**, and then select the **Version** and **Operating System Policy** to assign to the new virtual machine. Available policies are defined by the RCA OS Manager.
9. Click **Next**.
10. Type or use the drop-down list to enter the **Number of Virtual Processors** for the virtual machine. Note that a virtual machine cannot be assigned more processors than the actual number of logical processors on the host device.
11. Type the virtual machine **Memory Size**. Type or use the up and down arrows to enter the memory size in megabytes or use the slider tool to enter the size in gigabytes. Minimum memory size is 4MB.
12. Click **Next**.
13. Use the drop-down lists to select the **Number of NICs** (Network Interface Cards) and the **NIC #1 Virtual Network** to configure for this virtual machine.
14. Select **Connect at Power On** if you want each NIC to connect to the network when the virtual machine is powered on.
15. Click **Next**.
16. Review the summary information and click **Commit**.
17. The virtual machine is created. View the new virtual machine in the Virtual Machines list. Click the virtual machine name to open the properties window.

Controlling Devices Remotely

The RCA Console provides the capability to remotely access devices in either the internal or external repository using one of three methods:

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

The RCA Console attempts to determine the remote control capabilities of each target device and the suitable way to communicate with it. When you initiate a remote control connection to a particular target device, you can choose from the connection types that are available on that device.

For VNC and Windows Remote Desktop Connection, you must specify the port on which the remote devices will be listening for the remote connection. It is not necessary to specify a port for Windows Remote Assistance, because Windows Remote Assistance always uses a Distributed Component Object Model (DCOM) interface on port 135.

Note: Your RCA administrator can enable or disable remote control capability altogether or enable one or more specific remote control tools. See "Configure Remote Control" on page 310 for more information.

There are specific requirements that must be satisfied before each type of supported connection can be established. See "Requirements for Remote Connections" below for more information.

Accessing a device remotely

1. Click the **Management** tab.
2. Expand the zone containing the device that you want to access remotely.
3. In the left navigation pane, click **Devices**.
4. From the drop-down list next to a device name, click **Remote Control**.
   You can also choose **View/Edit Properties** and then click the  (Remote Control) icon in the Directory Object window.

   > **Note:** If the RCA Console cannot connect using Windows Remote Desktop Connection, VNC, or Windows Remote Assistance, an error message will appear when you click Remote Control.

5. For a Windows Remote Desktop Connection, specify the following:
   - **Method**: Select Windows Remote Desktop.
   - **Resolution**: Select the size of the Windows Remote Desktop Connection window on your screen.

   For a VNC connection, specify the following:
   - **Method**: Select VNC (Virtual Network Computing).

   For a Windows Remote Assistance Connection, specify the following:
   - **Method**: Select Windows Remote Assistance.
6. Click **Connect**. A new browser window opens, and your remote connection is established. For VNC connections, you may first be required to provide a VNC password.

   For Windows Remote Assistance connections, the user currently logged onto the target device must accept the connection.

Requirements for Remote Connections

The following requirements apply to any target devices that will be accessed remotely using the RCA Console:

- The remote device must be powered on.
- If the firewall is enabled, the remote access port on the remote device must be open.
- The remote device must be accessible both to the RCA Console server and to the client system initiating the request.

In addition, there are specific requirements for each type of remote access.

Requirements for Windows Remote Desktop

Windows Remote Desktop must be enabled on any target device that will be accessed remotely using this connection type. By default, this feature is not enabled.

To use Windows Remote Desktop, you must access the RCA Console using Internet Explorer (version 7, 8, or 9). This is because the Console launches a wrapper that uses an ActiveX component when this type of connection is requested.

Note: When using Windows Remote Desktop, you may be prompted to install an ActiveX control. This is required for Windows Remote Desktop to function properly. You are also prompted to connect local drives. This is not required.

For more information about Windows Remote Desktop, see the following Microsoft support document:

http://www.microsoft.com/windowsxp/using/mobility/getstarted/remoteintro.mspx

Requirements for VNC

For VNC connections, target devices must have a VNC server process running, it must be listening on the specified port, and support for URL (HTTP) based remote control sessions must be enabled.

To establish a VNC connection, the RCA Console launches the remote URL as a Java applet in your browser. For this reason, the Java Runtime Environment (JRE) version 1.5 (or later) must be installed on the system from which you are accessing the RCA Console (the system where the browser is running). You can download the JRE at www.java.com.

The port number for the remote URL must match the port on which the VNC server on the remote system is listening. By default, this port is 5800. For example:

`http://<`*RemoteSystem*`>:5800`

In this case, a connection is made to the <*RemoteSystem*> using port 5800, the VNC remote control applet opens in your browser, and then you can control the <*RemoteSystem*> remotely.

HP does not provide a VNC server program. The RCA Console, however, supports any VNC server that includes the web-based integration feature. This feature is available in UltraVNC, RealVNC, and TightVNC. VNC servers typically run on port 5800 and can be accessed through any web browser.

You can use an Application Management Profile (AMP) to distribute the UltraVNC, RealVNC, and TightVNC server software to your client systems. AMPs for the preceding applications can be obtained from the AMP Community on the HP Live Network web site. For more information about AMPs, see the *Radia Client Automation Enterprise Application Management Profiles User Guide*.

Requirements for Windows Remote Assistance

You can only create a Windows Remote Assistance connection when accessing the RCA Console from a Windows Vista, Windows Server 2008, or Windows 7 system. You can connect to target devices running the following operating systems:

- Windows XP
- Windows Server 2003
- Windows Vista
- Windows Server 2008

- Windows 7
- Windows Server 2008 Release 2 (R2) x64
- Windows 8

When you initiate a Windows Remote Assistance connection to a target device, the user of the target device must accept the connection. You cannot create a Windows Remote Assistance connection to an unattended device.

Windows Remote Assistance must be enabled on any target device that will be accessed remotely using this connection type. For instructions, consult your network administrator, or see the following Microsoft support document:

http://support.microsoft.com/kb/305608/en-us

There are three additional requirements that must be met before Windows Remote Assistance connections can be used:

- Both the system where you are accessing the RCA Console and the target devices must be joined to the same domain.
- The system where you are accessing the RCA Console (the "Expert" system in the Windows Remote Assistance interaction) must have the following software installed:
  - Java Runtime Environment (JRE) version 5 (or later)
  - If the operating system is Windows 2008 Server, the Remote Instance feature must be installed. For more information, see the following article: http://technet.microsoft.com/en-us/library/cc753881.aspx
- The Offer Remote Assistance group policy must be enabled on all target devices. You must also specify a list of "helpers" who are allowed to access the target devices. Helpers can be either users or groups and must be specified as follows:
  `domain_name\user_name`

  `domain_name\groupname`

  In order to create a Windows Remote Assistance connection to a target device, you—or a group to which you belong—must be included in this list of helpers.
- The Remote Assistance exception in Windows Firewall must be enabled on all target devices.

For additional information about Windows Remote Assistance, see the following Microsoft support document:

http://technet.microsoft.com/en-us/library/cc753881.aspx

Firewall Considerations

If there is a firewall between the server hosting the RCA Console and your remote devices, you must ensure that the appropriate ports are open.

Windows Remote Desktop Connection requires TCP port 3389.

By default, Windows Remote Assistance requires TCP port 3389 when connecting to Windows XP or Windows Server 2003 target devices. It requires port 135 (the DCOM port) when connecting to Windows Vista, Windows Server 2008, Windows 7, or Windows 8 devices.

VNC requires TCP port 5800 for the initial connection. In addition, it requires TCP ports 5900 + [as many ports as necessary, depending on the type of systems involved]. For example:

- On Windows systems, only TCP port 5900 is required.
- On a Linux system, say that the VNC Server is running at host:1. In this case, a firewall between the server and remote devices would need to allow access to TCP port 5901.

Similarly, the Java VNC viewer requires TCP ports 5800 + [as many ports as necessary, depending on the type of systems involved].

For additional information about using VNC with a firewall, refer to:

http://www.realvnc.com/support/faq.html#firewall

Remote Control Auditing

Each time that anyone in your RCA managed environment attempts to remotely connect to a managed device by using the RCA Console, a remote control audit event is logged. The following information is recorded:

- Who initiated the remote control session and when?
- What was the target device?
- What type of connection was used?

You can view the remote control audit log by opening the Remote Control report in the Administrative Reports view.

The Remote Control report contains the following information:

Time – Date and time when the remote control event occurred

Connect Status – Description of the remote control event

User – RCA Console User ID of the person who initiated the remote control event

Connection Type – VNC, Remote Desktop, or Remote Assistance

Target Host – Host name or IP address of the device that was accessed using remote control

HPCA Host – Host name or IP address of the system hosting the RCA Console

You can sort the report based on any of these items by clicking the column heading. The gray arrow indicates the sort order.

Managing Operating Systems

You can use the operating system (OS) management features of the RCA Console to install, replace, update, or repair operating systems on your client devices. You can also use RCA to perform various low-level tasks that must be completed before you can deploy an OS (for example, BIOS firmware updates, settings, and drive-configuration).

The following topics are covered here:

- "Prerequisites for OS Management" below
- "Deployment Scenarios" on next page
- "How it Works" below
- "Deploy an OS Image" on page 170
- "View the Status of OS Management Activities" on page 175

For a comprehensive discussion of OS management in RCA, see the *Radia Client Automation Enterprise OS Management Reference Guide*.

Prerequisites for OS Management

Before you can deploy an operating system (OS) using the RCA Console, the following prerequisites must be in place:

- A suitable OS image must be available.
  See chapter "Preparing and Capturing OS Images" on page 365 for instructions.
- The OS image must be published to the RCA Configuration Server Database (CSDB).
  See chapter "Publishing" on page 387 for instructions.

In some cases, you may also want to create a suitable hardware configuration object for your target device (or devices). For more information, see the *Radia Client Automation Enterprise OS Manager Hardware Configuration Management User Guide*.

After these prerequisites are in place, you can use the OS Management Wizard in the RCA Console to deploy and manage operating systems.

How it Works

You can use the OS Management Wizard to deploy an image to a single device, multiple devices that you select at the time, or an established group of devices – including Active Directory (AD) or Lightweight Directory Access Protocol (LDAP) groups.

When you deploy an OS image to multiple devices (not an established group), a new group is created under Groups in the Directories area on the Management tab. This group contains all the devices that are targets for this OS Deployment. The name of the group begins with “OS Deployment” and includes the name of the OS that will be deployed. For example:

```
OS Deployment of WINXP Service to 2 devices (2009.Mar.11 06:08:046 PM)
```

Whether you are deploying an OS to a single device or multiple devices, RCA performs the following actions:

- Assigns selected images as an OS policy on each device.
- Modifies the ROM object under each device based on the specified OS deployment options.
- Creates a job of type RMP to perform a notification. You can check the status of this job on the Current Jobs page (see "Current and Past Jobs" on page 148).

View the OS Deployment State

If the OS for a device is being managed by RCA, the OS deployment state is shown in the OS Management section of the Directory Object view for that device (select **View/Edit Properties** to display this view):

Waiting for OS Deployment – The OS deployment job is scheduled and is waiting to run.

OS Deployment In Progress – The OS deployment job is running.

Normal – The OS deployment job has successfully completed, and the OS is deployed.

Failed – The OS deployment job failed.

Unknown – The state of the OS deployment job cannot be determined.

Deployment Scenarios

How you deploy an operating system to devices in your environment depends on a number of variables. The following table describes multiple OS image deployment scenarios and instructions for deploying an operating system to those devices. For more information, see "Preparing and Capturing OS Images" on page 365.

Deployment Scenarios

Device State	Instructions for deployment
Managed (agent installed)	If the device is already managed: • Add the device to a group. • Entitle the group to an operating system (if not already entitled). • Use the OS Deployment Wizard to deploy the OS. **Note:** If you use LSB during the OS deployment process, you will not need to make preparations for PXE or the Service CD.
Un-managed (agent not installed)	If the unmanaged device has an OS installed: • Deploy the RCA agent to the device. • See instructions for Managed device above. If the unmanaged device does *not* have an OS installed: • See the instructions below for how to deploy an OS to a bare-metal device.

Device State	Instructions for deployment
Bare-metal (no OS installed)	If the device was previously managed (for hard drive recovery, for example): • Group membership and any OS entitlements should still be valid. Deploy the OS using PXE or the Service CD. If the device was not previously managed: • Boot the device with PXE or the Service CD. The device is added to RCA using a variation on the MAC address as its device name. • Add the new device to a group with OS entitlement. The device is rebooted, and the Service CD or PXE will continue with the OS deployment. **Note:** If an OS is attached to the All Devices group, the OS is installed automatically. If multiple OSs are attached to All Devices, then a choice of OS to install is presented. **Note:** LSB cannot be used for deploying an OS to a bare-metal device.

Deploy an OS Image

Five steps are required to deploy an OS from the RCA Console:

Step 1	Select the target device (or devices) or an established group that contains devices.
Step 2	Select the OS image to deploy.
Step 3	*Optional:* Select a Hardware Configuration Object to use before the OS installation. Although some target devices may be ready to have the operating system installed out of the box, there may be other situations when you need to identify and apply critical operations before proceeding with the operating system installation. Examples of the types of operations necessary are upgrading the BIOS firmware or configuring a disk array controller (DAC).
Step 4	Choose the deployment type: LSB, PXE, or CD/DVD. For LSB deployments, the RCA Agent is required. For more information, see "Deploying the RCA Agent" on page 147.
Step 5	Specify when the deployment should occur.

Each of these steps is explained briefly here. For additional information, see the chapter *"Publishing" on page 387.*

Before you attempt to deploy an OS image, be sure that the necessary prerequisites are in place. For more information, see "Prerequisites for OS Management" on page 168 and "Deployment Scenarios" on previous page.

Deploying an OS image

1. On the **Management** tab, go to the Directories area, and expand the zone that you want to use.
   - To specify one or more individual target devices, click **Devices**.
   - To specify a group, click **Groups**.

   Note: Groups used for OS deployment should have similar, compatible hardware.
2. In the Directory Object table, select the devices (or groups) that you want to use.
3. Click the **Deploy/Manage an Operating System** button. This launches the "OS Management Wizard" below. Follow the instructions in the wizard to configure and launch this OS deployment job.
   On the Management tab, monitor the groups under **OS Management** to view the status of the deployment.

OS Management Wizard

After you have selected a device or group for OS deployment, follow these steps to complete the OS Management Wizard:

Step 1 of 5: Operating System Selection

1. Choose one of the following options:
   - **Set new Operating System** – replaces the current OS
   - **Keep existing Operating System unchanged** – does not change the OS
2. Select one of the available OS images.
3. Click **Next**.

Step 2 of 5: Hardware Configuration Object Selection (Optional)

1. If you want to use a hardware configuration object, select **Use Hardware Configuration Management**. If you do not want to use a hardware configuration object, skip this step and click **Next**.
   See the *Radia Client Automation Enterprise OS Manager Hardware Configuration Management User Guide* for more information.
2. Choose one of the following options:
   - **Set new Hardware Configuration Option**
   - **Keep existing Hardware Configuration Option**
3. Select one of the available Hardware Configuration Options.
4. Click **Next**.

Step 3 of 5: Additional Options

1. Select the OS deployment method you will use:
   - **Local Service Boot (LSB)**: Select this option if you want to install LSB to deploy the OS. An advantage of LSB is that existing devices do not need to be PXE-enabled and the boot order does not need to be configured locally in the BIOS for each target device. For more information, see "Using LSB" below.
   - **Network Boot (PXE)**: Select this option if you will be using a PXE Server to install the operating system on your devices. For more information, see "Using Network Boot" on next page.
   - **CD/DVD**: Select this option if you will be using an ImageDeploy CD or DVD to install the operating system on your devices. For more information, see "Using an ImageDeploy CD or DVD" on next page.
2. Select **Emergency Mode** if you want to install (or re-install) the OS without attempting to capture and preserve any existing data – for example, in a disaster recovery scenario.
   This option enables the client devise to sense the need for management activity. If this option is not enabled, the client device requires an existing and bootable operating system, a working RCA Agent, and good general integrity (for example, no viruses) to sense this.

   For information about capturing and preserving data if **Emergency Mode** is not used, see “Defining Drive Layouts” in the *Radia Client Automation Enterprise OS Management Reference Guide* .
3. Select **Wake on Lan** if you want RCA to trigger management operations on a machine that is currently turned off.
4. Click **Next**.

Step 4 of 5: Schedule

1. Specify the **Start Date** and **Start Time** that this OS deployment job should start.
2. Click **Next**.

Step 5 of 5: Summary

The Summary page in the wizard enables you to view all the settings you have specified for this OS deployment job, including the list of target devices. Click **Submit** to create the job. A new RMP type job should appear under **Current Jobs** on the Management tab (see "Managing Jobs" on page 148).

Using LSB

The Local Service Boot (LSB) option enables RCA to assume management of the OS on devices that are not booted from the network.

When using LSB, existing machines do not need to be PXE-enabled, and the boot order does not need to be configured locally in the BIOS for each target device.

See "Deployment Scenarios" on page 169 for prerequisite instructions for OS deployment.

Note: To deploy Microsoft Windows Vista and above OS with a separate boot partition successfully, set the boot partition size to a minimum of 300 MB or double the size of your `winpe.wim` file. The recommended boot partition size is one GB.

Note: Deploying an OS through LSB is not supported on Windows CE based HP thin client models t5550 and above.

Using Network Boot

The PXE-based environment enables RCA to assume management of the OS on target devices that are booted from the network. See "Deployment Scenarios" on page 169 for prerequisite instructions for OS deployment.

Using PXE consists of configuring your DHCP server to provide clients booting from the network a boot image and a TFTP server that will supply these files.

Note: A DHCP server and TFTP server must be configured before using PXE for OS deployment. See the product documentation for configuration instructions.

When PXE is configured, make sure that your target devices boot from the network or have PXE-enabled as the primary boot device. Make the necessary configuration adjustments to ensure that this will happen (for example, with some BIOS versions, you can hit **Esc** during the reboot process and change the boot order in the configuration settings).

When you deploy an OS image using Network Boot, the target devices are rebooted using the settings that you defined on your DHCP server. The OS image is then deployed and installed on the target device. If multiple OS images are entitled to the device, you will be prompted to select the OS to install.

Using an ImageDeploy CD or DVD

An ImageDeploy CD/DVD is used to locally boot a target device that does not already have an operating system installed (a bare-metal machine). The ImageDeploy CD/DVD must be available locally at the target device.

Use the `ImageDeploy.iso` file provided with RCA to create your CD or DVD. This file is located here on the HPCA media:

`\Media\iso\roms\ImageDeploy.iso`

Since LSB cannot be used for devices that do not already have an OS installed, you must use either the ImageDeploy CD or a PXE server to boot a bare-metal machine before OS deployment.

See "Deployment Scenarios" on page 169 for prerequisite instructions for OS deployment.

Deploying an OS image using the ImageDeploy CD

1. Perform the following steps on the target device:
   a. Insert the ImageDeploy CD (or DVD) in the target device, and boot off of the CD (or DVD).
   b. Specify which SOS to boot (**Linux** or **WinPE**).
   c. From the boot source menu, select **Install from network**.
   d. When prompted, type your RCA server IP address or host name and port number in the following format:
   xxx.xxx.xxx.xxx : *port*

      For example:

      `HPCA.acmecorp.us.com:3466` or `192.168.1.100:3466`

      Note that port 3466 is reserved for OS imaging and deployment in an RCA Core and Satellite installation. In an HPCA Classic installation, port 3469 is reserved for this purpose.
   e. Press **Enter** to continue.

   The device connects to the RCA server and is added to the Devices list using a variation on the MAC address as the device name. After the ImageDeploy CD connects to the RCA server, the following messages are displayed:

   ```
   This machine has no local OS or the OS is invalid.

   The machine cannot be used and will be shut down until an
   administrator specifies Policy and performs a Wake on LAN.
   ```

2. Perform the following steps in the RCA Console:
   a. On the Management tab, follow the instructions for "Deploy an OS Image" on page 170.
   b. For the deployment method, select **CD/DVD**.
3. After the wizard completes, reboot the target device again using the ImageDeploy CD. During this reboot, the OS image is detected and deployed. This can take 10 to 15 minutes depending on the size of the image and network bandwidth. If multiple OS images are entitled to the device, you will be prompted to select the OS to install.

When the image is finished deploying, the target device reboots and starts Windows. The Sysprep process will start and initialize the new image.

Perform a One-Time Hardware Maintenance Operation

Using the RCA Console, you can create a job that uses a Hardware Configuration Element to perform special hardware maintenance operations on a client device. This may be necessary before you can install, update, or repair the OS on certain devices – for example, if you need to trigger a RAID (redundant array of independent disks) verify or re-synch after an active hot spare (AHS) has been changed.

Note: For more routine low-level operations – such as a BIOS firmware upgrade or disk array controller (DAC) configuration – you should use the normal LDS/LME management process.

For additional information, see the *Radia Client Automation Enterprise OS Manager Hardware Configuration Management User Guide.*

Performing a One-Time Hardware Maintenance Operation

1. On the **Management** tab, go to the Directories area, and expand the zone that you want to use.
   - To specify one or more individual target devices, click **Devices**.
   - To specify a group, click **Groups**.
2. In the Directory Object table, select the devices (or groups) that you want to work with.
3. In the drop-down menu for one of the selected devices (or groups), select the **Perform a one-time Hardware Maintenance** item in the OS Management submenu.
   This launches the Hardware Maintenance Wizard.
4. Select **Emergency Mode** if you want to install (or re-install) the OS without attempting to capture and preserve any existing data – for example, in a disaster recovery scenario.
5. Select **Wake on Lan** if you want RCA to trigger management operations on a machine that is currently turned off.
6. From the Available Maintenance Options list, select the hardware configuration element that you would like to use.
7. Specify the **Start Date** and **Start Time** that this OS deployment job should start.
8. Click **Next**.
   The Summary page opens. This page enables you to view all the settings that you have specified for this hardware maintenance job, including the list of target devices.
9. Click **Submit** to create the job.

A new RMP type job should appear under **Current Jobs** on the Management tab (see "Managing Jobs" on page 148).

View the Status of OS Management Activities

After you click **Submit** in the OS Management Wizard, an RPM job is created and appears in the **Current Jobs** list (see "Current and Past Jobs" on page 148).

After the OS deployment job is finished, it moves to the **Past Jobs** list.

If the OS for a device is being managed by RCA, the OS deployment state is shown in the OS Management section of the Directory Object view for that device (select **View/Edit Properties** to display this view). For more information, see "View the OS Deployment State" on page 169.

Viewing Out Of Band Details

The Out of Band Management (OOBM) features available in the RCA Console enable you to perform out of band management operations regardless of system power or operating system state.

In band management refers to operations performed when a computer is powered on with a running operating system.

Out of band management refers to operations performed when a computer is in one of the following states:

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

The RCA Console supports Out of Band Management of Intel vPro devices and DASH-enabled devices.

This option is only available when Out of Band Management is enabled. See "Out of Band Management" on page 335 for instructions. For more information, see the *Radia Client Automation Enterprise Out of Band Management User Guide.*

Viewing Out of Band details for a device

1. On the Management tab, go to the Directories area, expand the zone that you want to use, and click **Devices** (or **Groups)**.
2. From the shortcut menu for the device that you want to work with, select **Out of Band Device Details**.
   The Out of Band Device Details window opens for the selected device—provided that the device is DASH or vPro equipped, and OOBM is enabled and properly configured.

Note: You can also click the Out of Band Device Details  icon to view the OOB details for a particular device.

When Out of Band Management is enabled, this icon appears on the toolbar in the Directory Object view for any device.

Deploying the Usage Collection Agent

To deploy the Usage Collection Agent, create a job for a target device or group using the Usage Connect job template.

To deploy the Usage Collection Agent:

1. On the Management tab, click **Devices** or **Groups**.
2. Follow the instructions in "How to Manage Policies for Directory Objects" on page 137 to entitle the pertinent devices or groups to the following service:
   USAGE.ZSERVICE.CCM_USAGE_AGENT
3. Follow the instructions in "Create a New DTM or Notify Job" on page 154, and specify the Usage Connect job template.
   The schedule that you specify for this job will be the schedule used for collecting usage data.

This creates a job that will install the Usage Collection Agent on the target devices and then collect usage information from them. You can view all pending jobs by clicking Current Jobs in the Jobs area.

Managing Internet Devices

Using RCA, you can manage the devices that are outside your corporate network similar to the devices over corporate network or VPN. You can manage inventory, software, patching, and vulnerabilities for the devices. OS management is not supported on devices that are outside your corporate network.

It recommends configuring a full-service Satellite server as an access point for devices that will connect from outside the corporate network. Configuring a Core server for such an access is not recommended.

To configure RCA access for devices outside the corporate network, complete the following tasks:

Task 1:"Create a Server Access Profile" below

Task 2:"Configure the Full-Service Satellite Server" on next page

Task 3:"Configure the RCA Agent " on next page

Create a Server Access Profile

To create a server access profile for the full-service Satellite server that serves as an access point for devices:

1. Using the Radia Client Automation Administrator CSDB Editor, navigate to the **Primary File**, **Client Domain**, **Server Access Profile (SAP)** class. You see the following SAP instances for the full-service Satellite server:
   - `<Full-service Satellite server> CONFIG`
   - `<Full-service Satellite server> DATA`
   - `<Full-service Satellite server> ROMS`
2. Create a copy of the `<Full-service Satellite server> CONFIG` instance, For example, you created an instance `<Full-service Satellite server> TEST`.
3. Make the following changes in the `<Full-service Satellite server> CONFIG` instance:
   - Enable SAP = N
4. Make the following changes in the <Full-service Satellite server> TEST instance:
   - PROTOCOL = HTTPSTCP
   - PORT = 443
   - Enable SAP = Y
   - TUNLPORT = *<The port on which your Configuration server communicates to the RCA agent. The default port is 3464.>*

   HTTPSTCP protocol is only available with SSL enabled, and it recommends to use client side certification (two-way SSL) on full-service Satellite server. For more information on configuring two-way SSL, see *Radia Client Automation Enterprise SSL Implementation Guide*.

Configure the Full-Service Satellite Server

Make the following changes if the Configuration server on full-stream Satellite server does not communicate to the RCA agent on the default port, 3464.

- Check the value set for `TCP_PORT` parameter in the edmprof.dat file located at *<InstallDir>\ConfigurationServer\bin*. For example, `TCP_PORT=3909`
- Set the `AllowCONNECT` parameter in the httpd.conf file located at *<InstallDir>\ApacheServer\conf* to the same port as TCP_PORT. For example, `AllowCONNECT 3909`

You must enable SSL on the full-service Satellite server that will serve as an access point for devices from outside the corporate network.

You must expose an RCA full-service Satellite server to the public Internet in a network DMZ. This subjects the Satellite server to a greater risk of attack than in a traditional corporate environment or VPN. To avoid such risks, only the following ports should be open on the full-service Satellite server.

- 443 - required for RCA Agents to connect to the Satellite server over the Internet.
- 3464 and 3466 – required for the Satellite server to connect to the upstream server (Satellite server or Core server)
- 389 – required for the Satellite server to connect to the LDAP server for authentication

In addition, to restrict the risk of attack, the RCA services offered by the full-stream Satellite server should be limited to those required by Internet-facing clients. For example, if OS Management is only used on the local or corporate network, the full-service Satellite server in a network DMZ should not have OS Management enabled.

Note: If your environment uses load balancers to manage the load on the full-service Satellite servers that are outside the corporate network, make sure that the load balancers support the HTTP CONNECT method.

Configure the RCA Agent

Before installing the RCA agent on a device, update the [Objects] Section of `install.ini` file. The `install.ini` file is used 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.

Settings in `install.ini` override the defaults stored in `HPCAE-MgmtApps.msi`. You can create your own customized `install.ini` file. A sample `install.ini` is available in the `\Setup-Core\Media\client\default\win32` directory on the HPCA Core media.

Set the following arguments in the [Objects] section of the `install.ini` file:

- ZMASTER_ZDSTSOCK = 443
- ZMASTER_ZIPADDR = IP address of the full-service Satellite server

- ZMASTER_TUNLPORT = <*The port on which the full-service Satellite server communicates with RCA agent. The default port is 3464.*>
- Add a new argument ZMASTER_ZDEVICEN to the `install.ini` file and set the value to 092, ZMASTER_ZDEVICEN = 092

Managing Mobile Devices

Radia Client Automation (RCA) is a real-time, policy-based, desired state management client management solution that automates the administrative tasks for the physical and virtual clients devices in highly complex and ever changing environments. The client devices can be a desktop, laptop, virtual device, or a mobile device. A mobile device can either be a smartphone or a tablet. RCA supports only Android and iOS operating system-based devices. For more information on the supported operating system, see the Radia Client Automation Support Matrix available at: http://support.persistentsys.com/. For more details, contact your Persistent Support representative.

Using RCA, you can perform various Mobile Device Management (MDM) tasks, such as software management, inventory management, and security management. This chapter provides information on how you can set up RCA servers for MDM, notify end-user for the agent application download, and publish and deploy mobile applications. This chapter also describes the steps to create mobile device security profiles, such that you can protect mobile devices in your environment from unauthorized access.

Configuring RCA Servers for MDM

Complete the pre-configuration, configuration, and post-configuration tasks listed in this section to set up MDM capabilities on RCA Core and Satellite servers.

Pre Configuration Tasks

Before configuring RCA servers for MDM, you must complete the following tasks, based on the type of devices you plan to manage using RCA:

Managing Android devices

- Open the required ports on the RCA Core and Satellite servers. For more information on the ports that you must enable, see the *Radia Client Automation Enterprise Installation and Upgrade Guide*.
- You must have a valid Google account. This must be an active account and Google services, such as email or chat must have been used at least once using this account on the device.
- You must have a valid Google project number and API key. To obtain these credentials, follow the steps listed on the Google website at http://developer.android.com/guide/google/gcm/gs.html. These details are required to use the Google Push Notification services to send notification requests to the mobile device.
- You must enable the Google Cloud Messaging (GCM) for Android service. To enable this service, follow the steps listed on the Google website at http://developer.android.com/guide/google/gcm/gs.html#gcm-service.

Managing iOS devices

- Open the required ports on the RCA Core and Satellite servers. For more information on the ports that you must enable, see the *Radia Client Automation Enterprise Installation and Upgrade Guide*.
- You must have one or more full-service Satellite servers in your RCA infrastructure that are accessible from the Internet.
- You must have a SCEP server configured in your environment for a single challenge password, that does not expire. This password is required by RCA servers to authenticate the mobile devices that connect to the Apple servers.
  To implement SCEP on a Microsoft Windows 2008 server, see the Microsoft website at http://www.microsoft.com/en-us/download/details.aspx?id=1607.
- You must have OpenSSL version 0.9.8r or above installed in your environment.
- You must obtain an APNS certificate, also known as MDM certificate. RCA uses the APNS certificate to communicate with the iOS devices. Complete the following steps to generate the APNS certificate:
  a. Create a CSR using OpenSSL. Open command prompt and run the following command:
  `openssl req -new -newkey rsa:2048 -out cert.csr -config "path_openssl.cfg"`
  In this instance, *path_openssl.cfg* is the path for the OpenSSL configuration file `openssl.cfg`, which is available at the location where you installed OpenSSL.
  When you run this command, OpenSSL prompts you to provide values for a few fields, such as Country Name, Locality Name, and Organization Name. Make sure that these fields are not left blank and you provide values that are specific to your organization. The above command generates a CSR `cert.csr` and a private key `privateKey.pem`.

  b. Email this CSR to Persistent at rcamobility@persistent.co.in. Persistent then provides you with a base-64 encoded file that contains the property list.

  c. Log on to the Apple Push Certificates Portal at https://identity.apple.com/pushcert using your Apple ID. It is recommended that you log on to this web page using the Safari web browser.

  d. Click **Create a Certificate**.

  e. Click **Choose File** and browse to the property list file that you received from Persistent, and then click **Upload**. After you successfully upload the file, Apple generates the APNS certificate that you can view under Certificates for Third-Party Servers.

  f. Click **Download** to download the signed MDM certificate. The certificate is in the `.pem` format. You must convert this certificate to the `.p12` format. To convert the certificate in `.pem` format to a certificate in `.p12` format, open the command prompt and run the following command:
  `openssl pkcs12 -export -out <cert.p12> -inkey <privateKey.pem> -in <cert.pem>`
  In this instance,
    - *cert.p12* is the certificate file in `.p12` format that OpenSSL generates. You must provide the complete path where this file must be stored.
    - *privateKey.pem* is the key that you obtained while generating the CSR. You must provide the complete path where this key is stored.

- *cert.pem* is the certificate you downloaded from the Apple website. You must provide the complete path where this file is stored.When you run this command, OpenSSL prompts you for a password. Make sure that you do not provide a blank password. This password is required when you set up Satellite servers for MDM.

Save a copy of this certificate on each Satellite server that you want to use for MDM.

Configuring RCA Servers for Android Devices

RCA uses the Google Cloud Messaging (GCM) service to send connection requests from the RCA servers to the Android-based mobile devices. The requests are first sent to the Google servers, and then the Google servers forward these messages to the mobile devices. For more information on GCM, see the Google web site at http://developer.android.com/guide/google/gcm/index.html.

Complete the following steps to configure the RCA servers to use the Google servers for sending notifications to the Android device users:

1. Log on to the RCA Core Console and click **Configuration** tab.
2. Expand Mobile Management, click **Vendor Configuration**, and then click **Android**. The Notification Settings view opens in the details pane.
3. Enter the details for the following fields and click **Save**:

Field	Description
GCM API Key	The API key provides RCA servers authorized access to Google services. Enter the API key for server apps that you received when you configured API access on the Google APIs Console page at https://code.google.com/apis/console. A sample GCM API Key appears as follows: Key for server apps (with IP locking) API key: AIzaSyAS0yrMCGrgdzjbsdc8ZwVnFTyzV6_EB7Q
GCM Project ID	The Project Number is required to validate that the RCA Android application is registered to send messages to the mobile device. Enter the project number that you received as a part of URL when you created your Google API project. For example: 4915162343 in the `https://code.google.com/apis/console/#project:4915162343` URL.

Configuring RCA Servers for iOS Devices

To manage iOS devices, you must complete the following tasks:

1. **"Task 1: Enable SSL" on next page**
2. **"Task 2: Add MDM Server" on next page**
3. **"Task 3: Set up MDM Server Properties" on next page**

Note: This document explains the certificate-related procedures—Certificate Signing Request

(CSR) generation, certificate conversion, and Apple Push Notification service (APNS) UID creation using OpenSSL on Windows platform.

Task 1: Enable SSL

You must enable SSL on the RCA Satellite server that you will be setting up for MDM. For more information on how to enable SSL on the RCA Satellite server, see the *Radia Client Automation Enterprise SSL Implementation Guide*.

Task 2: Add MDM Server

Full-service Satellite servers are required to manage the iOS mobile devices. Complete the following steps to add an existing full-service Satellite server as an MDM server:

1. Log on to the RCA Core Console and click **Configuration** tab.
2. Expand **Mobile Management** in the left-navigation pane and then click **Vendor Configuration>iOS**. The iOS settings page opens.
3. Click **MDM Configuration** tab.
4. Click **Add New MDM Server** icon. The MDM Server Creation Wizard opens.
5. Enter the details for the following fields and click **Save**:

Field	Description
Name	Name of the Satellite server. The Satellite server is referenced using this name on the MDM Configuration page.
Description	Description of the Satellite server.
Full-Satellite Server URL	Select the Satellite server that you want to set up for MDM.

Task 3: Set up MDM Server Properties

After you identify and add the Satellite server that provides the MDM functionality, you must configure the Satellite server properties, such that these servers can process the jobs that an administrator creates for mobile devices.

MDM Satellite Server Settings for APNS

You must configure the APNS settings on each Satellite server set up as MDM server.

Complete the following steps:

1. Open command prompt and run the following command:
   `openssl exe x509 -in <cert.pem> -text`
   In this instance,
   cert.pem is the certificate you downloaded from the Apple website during APNS generation

process.
This command provides a UID that you must add in each MDM Satellite server properties file.

2. Modify the `mdm.properties` file for each Satellite server that you have set up for MDM:
   a. Navigate to the directory `<InstallDir>\tomcat\webapps\mdm\WEB-INF\classes`.
   b. Open the file `mdm.properties` in a text-editor.
   c. Provide the UID that you generated in step 2 of this procedure as the value for the `mdm.Topic` property. For example, if the following output is displayed when you run the command in step 2: `Subject: UID=com.apple.mgmt.External.b66302d9-7fb2-44e7-8a23-6d7b6e9b0b6e, CN=APSP:b66302d9-7fb2-44e7-8a23-6d7b6e9b0b6e, C=IN`, the UID value is `com.apple.mgmt.External.b66302d9-7fb2-44e7-8a23-6d7b6e9b0b6e`. Set the value for the property as `mdm.Topic=com.apple.mgmt.External.b66302d9-7fb2-44e7-8a23-6d7b6e9b0b6e`.
   d. Restart the `HPCA Tomcat Server` service.

MDM Satellite Server Common Properties

Complete the following steps to configure the common properties that are shared across all MDM Satellite servers:

1. Log on to the RCA Core Console and click **Configuration** tab.
2. Expand **Mobile Management** in the left-navigation pane and then click **Vendor Configuration>iOS**. The iOS settings page opens.
3. Enter the details for the following fields and click **Save**:

Field	Description
SCEP Name	The name of the certificate authority that SCEP server uses to issue certificates.
SCEP URL	The URL of the SCEP server. If you have implement SCEP server on Microsoft Windows, enter the URL in the following format: http://*SCEP_hostname*/certsrv/mscep/mscep.dll, where *SCEP_hostname* is the hostname of the SCEP server.
Single Challenge Password	The enrollment challenge password that you obtain from the SCEP server administrator. To obtain password on a SCEP server implemented on Microsoft Windows Server 2008, open the URL http://*SCEP_hostname*/CertSrv/mscep_admin/ in a web browser, where *SCEP_hostname* is the hostname of the SCEP server.
MDM Configuration Profile Name	The name of the profile that a mobile device user views during the device enrollment process. This profile contains details of the SCEP server certificate and the APNS certificate.

Field	Description
Security Configuration Payload Display Name	The name of the security profile. This profile contains details on the security policies that an administrator has applied on the device. Note that end-users cannot remove a security profile that you have entitled to the device.
Security Configuration Payload Description	The description of the security profile.

MDM Satellite Server-Specific Properties

Complete the following steps to configure Satellite-server specific properties:

Note: You can also modify these properties by logging on to the RCA Satellite Console of the Satellite server that you have identified as an MDM server. Click **Configuration** tab, and then click **iOS MDM Settings** in the left-navigation pane.

General Settings

1. Log on to the RCA Core Console and click **Configuration** tab.
2. Expand **Mobile Management** in the left-navigation pane and then click **Vendor Configuration>iOS**. The iOS settings page opens.
3. Click **MDM Configuration** tab.
4. Click the URL for the full-service Satellite server. The Configuration tab view opens.
5. Click **iOS MDM Settings** and then click **General Settings**.
6. Enter the details for the following fields and click **Save**:

Field	Description
Socks Proxy: These settings are required only if your enterprise has blocked the ports required to connect to APNS. You can then route the access to APNS using a SOCKS proxy.	
Socks Proxy Enable	Select if the Satellite server connects to the APNS through a SOCKS proxy server. To send notification messages to mobile devices, Satellite servers require access to the APNS.
Socks Proxy Host	Enter the hostname of the SOCKS proxy server.
Socks Proxy Port	Enter the port number of the SOCKS proxy server.
Key Store: These settings are required to modify the certificate settings that are required to	

Field	Description
connect the iOS operating system-based devices with APNS.	
Certificate File Path	Specify the path for the root certificate of the certification authority that you used to enable SSL on the Satellite server. Make sure that the certificate is not a self-signed certificate. For example, specify the path in the following format: `C://Certificates//certificate.crt` You must store the certificate locally on the Satellite server.
MDM Certificate Path	Specify the path to the APNS certificate. Make sure that you provide the certificate in `.p12` format. For example, specify the path in the following format: `C://Certificates//certificate.p12` For more information on how to convert a certificate in `.pem` format to `.p12` format, see "Pre Configuration Tasks" on page 179. You must store the certificate locally on the Satellite server.
MDM Certificate Password	Specify the password that you provided while converting the certificate in `.pem` certificate to a certificate in `.p12` format.

Advanced Settings

The MDM server component on the full-service Satellite server manages the iOS mobile devices. This component includes the following sub-modules that aid in managing and processing the jobs for a mobile device:

- Staging Manager: This module processes all commands required to run an agent connect job.
- Persistent Store: A persistent data store that stores the push notification jobs created by an administrator, the timer-based jobs, and jobs created when an end-user manually connects to the RCA servers. The jobs exceeding the existing job processing limit of the Staging Manager are added in this data store. The jobs are processed using the First In, First Out principle, with the priority-set jobs processed first as an exception. A priority is set for a job in the following scenarios:
  - The device sends a notification to the Staging Manager to run a connect.
  - The job was not completed because of one of the following reasons, and added to the Persistent Store for a retry:
    - The device is switched off.
    - The Apple gateway is too busy to process the request.
    - The device is not on a corporate network.
    - The port on the device is not enabled for accepting the incoming messages from APNS.

- The device is password protected and is currently in locked mode. A few connects, for example security connect do not run if the device is in locked mode. The device sends a "NotNow" message when a notification request is sent.

If a job is not successful at the first instance, it is added to the processing queue for another try, before it is permanently removed from the job queue. A status flag is used to track if the job is added for a retry.

If the device receives a delayed notification, after the job has already been moved out of the Staging Manager, it sends a message to the Staging Manager requesting the tasks to be performed. The Staging Manager searches for the job in the current processing queue, and then in the Persistent Store. If the Staging Manager is not processing maximum number of permissible requests, it adds the job in the current processing queue and sends a notification to the Notifier module to connect to the APNS. If the Staging Manager is processing maximum number of permissible requests, the job is added in the Persistent Store with a high priority.

- Job Processor: This module polls the Persistent Store and sends the jobs to the Staging Manager.
- Notifier: This module sends requests to the APNS, to be sent to the iOS mobile devices.
- Command Processor: This module performs all the post-processing of the tasks that are run by the Staging Manager. For example, after you run an audit connect job, this module sends the data received from the device to the Reporting server database.

You can modify the properties for each sub-module by configuring the Advanced Settings of the MDM server.

To modify the Advanced Settings, complete the following steps:

1. Log on to the RCA Core Console and click **Configuration** tab.
2. Expand **Mobile Management** in the left-navigation pane and then click **Vendor Configuration>iOS**. The iOS settings page opens.
3. Click **MDM Configuration** tab.
4. Click the URL for the full-service Satellite MDM server. The Configuration tab view opens.
5. Click **iOS MDM Settings** and then click **Advanced Settings**.
6. Enter the details for the following fields and click **Save**:

Field	Description
Server FQDN	The fully qualified domain name (FQDN) of the Satellite server.
Server Port	The port that the Satellite server uses for communications. If you select HTTPS in the Server Method list, you must specify the SSL port that you use for HTTPS communications. The default SSL port is 443.
Server Method	Select the HTTP/HTTPS protocol for Satellite server communications. If you enable HTTPS, the communication between Satellite Server and the built-in iOS MDM agent on the device is SSL-based.

Field	Description
	The communications between the Satellite server and the RCA agent are HTTP even if you select the HTTPS method. The communications between the Satellite server and APNS are always SSL-based.
Number of Maximum Concurrent Connections	Specify the maximum number of device connections that the Staging Manager processes at any instance.
Notifier Interval in Minutes	Specify the time (in minutes) that Notifier module must wait before sending requests to the APNS. The Notifier waits only if it is processing maximum number of permissible requests.
Number of Notifier Workers	Specify the number of workers that can send notification request to the APNS. The workers share load based on the current number of device connections.
Number of Command Processor Workers	Specify the number of workers for performing post-processing tasks.
Staging Manager Sleep Period in Minutes	Specify the time (in minutes) Staging Manager must sleep before polling the Persistent Store.
Staging Maximum Inactivity Time	Specify the maximum time (in minutes) a job can stay in the Staging Manager without any response from the device. After the maximum inactivity time lapses, the job is moved out of the Staging Manager and added to the Persistent Store, with a status flag set to true.
Persistent Store Polling Interval in Minutes	Specify the time (in minutes) after which the Staging Manager polls the Persistent Store for jobs.
Maximum Number of Concurrent Jobs to be run	Specify the number of parallel threads that can add jobs to the Staging Manager.
Maximum Number of Record to be Processed from the Persistent Store per Polling	Specify the maximum number of jobs that the Staging Manager must select for processing from the Persistent Store per poll.

Post Configuration Tasks

After you have configured the RCA servers, you must run a synchronization between the Core and Satellite servers in your environment. You must synchronize the Satellite servers with the Core server after you modify any configurations.

You might receive the following error message during Satellite synchronization:

```
Synchronization Failed
```

To resolve this problem, see the workaround mentioned for the problem "Core and Satellite: Satellite synchronization fails from SSL enabled Core" in the Known Problems section of the *Radia Client Automation Enterprise Release Notes*.

Modifying RCA Satellite Server Configuration File

You can optionally modify the Mobile server configuration file in a full-service Satellite server. The values in this configuration file are set by default. If you want to modify these parameters, edit the `ConfigServerAdapter.cfg` file.

1. Using a text-editor, open the file `ConfigServerAdapter.cfg` available at the location `<InstallDir>\MobileServer\etc`.
2. Modify the following parameters and save this file:

Parameter	Description
`http-port`	The HTTP port that Satellite server uses for communications with RCA Core server and RCA agents.
`max-threads`	Maximum number of threads that must run on a Satellite server to process the mobile device jobs.
`ds-refreshtime`	Directory service refresh time in seconds.

Enabling Administrators to Notify End-users for Agent Installation

To manage a mobile device, an agent is installed on the device that connects to the RCA servers to perform policy resolution and maintain the desired state. Based on the device platform, mobile users can download the agent application from Google Play or App Store.

The RCA agent for mobile devices is a light-weight application that enables RCA servers to communicate with the mobile device. Using the Email Notification settings, you can send an email to the mobile device user to download the mobile agent. The following sections list the prerequisites and the steps to configure email notification settings.

Prerequisites

The following prerequisites must be met before you configure RCA to send an email notification to the end-user:

- The directory service, in which the mobile device user is listed, must be configured for use with RCA. To make sure that the directory service is configured for use with RCA, perform the following steps on RCA Console.
  a. Click the **Configuration** tab.
  b. Expand **Infrastructure Management** and then click **Directory Services**.
  c. Select the Directory Service that the mobile device user is a part of to open the **Directory Service Properties** window.

d. Click the **Properties** tab in the **Directory Service Properties** window.

e. Click **UI Settings**.

f. Select the **Used for Authentication** check box.

- The directory service user must have a valid email ID.

Configuring Email Notification Settings

Note that RCA currently supports only SMTP-based mail servers for sending email notifications.

1. Log on to the RCA Core Console and click **Configuration** tab.
2. Expand Mobile Management in the left-navigation pane and click **Email Notification Settings**. The Notification Settings view opens in the details pane.
3. Enable the Socks Proxy settings only if your enterprise is configured to use SOCKS proxy. Enter the details for the following fields:

Field	Description
Proxy Enable	Select this check box if your enterprise is configured to use a SOCKS proxy.
Proxy Host	Enter the IP address or fully qualified domain name (FQDN) of the SOCKS proxy server.
Proxy Port	Enter the port number of the SOCKS proxy server.
User Name	Enter the user name that the RCA servers use to authenticate to the SOCKS proxy server. The entries in this field are required only if the proxy server requires a username and password.
Password	Enter the password for the user name you provided to authenticate RCA servers to the SOCKS proxy server.
Confirm Password	Re-enter the password.

4. Enter the details for the following fields under Email Server Details. These settings are required to configure access to the mail server used in your environment.

Field	Description
SMTP Host	Enter the IP address or fully qualified domain name (FQDN) of the SMTP mail server.
SMTP Port	Enter the SMTP port number.
Basic Authentication	Select this check box if the mail server requires authentication.
User Name	Enter the user name RCA servers will use to authenticate to the mail

Field	Description
	server. This field is available only if you select the Basic Authentication check box.
Password	Enter the password for the user name you provided to authenticate the RCA servers to the mail server. This field is available only if you select the Basic Authentication check box.
Confirm Password	Re-enter the password. This field is available only if you select the Basic Authentication check box.
Enable SSL	Select if the mail server is configured to use the SSL protocol for SMTP connections.
Enable TLS	Select if the mail server is configured to use the Transport Layer Security (TLS) protocol for SMTP connections.

5. Enter the details for the following fields under Mail Details, and then click **Save**. These settings enable you to configure how the agent installation email appears to the mobile device user.

Field	Description
Sender Name	Enter the name that should appear in “From” field when the user receives an email.
Sender EmailID	Enter the email ID that is used to send emails to the user or user groups.
Subject	Enter the subject for the installation mail that is sent to the user. For example, you can set this value as RCA Mobile Agent Installer.
Body	Enter the email body text. Provide the following details in the email text: ▪ Agent download URL: The Google Play URL from where the mobile device user can download the Android or iOS agent. ▪ RCA sever IP or hostname: The IP address or hostname of the full-service Satellite server to which the RCA agent will connect to fetch the entitlement policies. ▪ Port: The port number through which the mobile device connects to the RCA server IP address you provided. ▪ Install instructions: Instructions on how to install the RCA mobile agent. For more information on how to install the agent application on a mobile device, see: ○ For Android operating system-based devices: "Installing the RCA Agent on Android Devices" on page 200 ○ For iOS operating system-based devices: "Installing RCA Agent on iOS Devices" on page 201

Field	Description
	▪ Registration instructions: Instructions on how to register the mobile device to the RCA servers.

Creating Mobile Connect Job

After you have configured the Email Notification settings, create a job for the user or group of users to whom you want to send the email notification.

To create a job, complete the following steps:

1. Log on to the Core Console, click **Management** tab, and then click the directory service that you have added to RCA.
2. Navigate to the user for which you want to create a job.
3. Select the user and click **Launch HPCA Job Creation Wizard** to open the HPCA Job Creation Wizard.
4. From the Job Type list select **Notify**.
5. Enter a Name and Description of the job.
6. From the Job Action Template list, select **Mobile Email Connect**, and then click **Next**.
7. Review the information on the Job Confirmation Summary page and click **Submit**.

Provisioning Mobile Applications

Using RCA you can publish mobile applications and entitle these applications to user or user groups. You can also upgrade or uninstall an application installed on a mobile device.

Publishing Mobile Applications

Use the RCA Administrator tools to publish packages for the Android and iOS platform.

Note: For iOS operating system based devices, RCA supports software management of in-house applications only. You must enroll for iOS Developer Enterprise Program to create in-house applications. For more information on how to obtain the membership, see the Apple website at http://developer.apple.com/programs/ios/enterprise.

Complete the following steps to publish mobile applications to the CSDB:

1. Open the Radia Client Automation Administrator Publisher.
   a. From the computer where you have Administrator Tools installed, click **Start**>**All Programs**>**Radia Client Automation Administrator**>**Radia Client Automation Administrator Publisher**.
   b. Enter the user ID and password, and click **OK**. The default user ID is `admin`. The default password is `secret`. The Radia Client Automation Admin Publisher window opens.

2. Select **Mobile Application** from the Publishing Options drop-down list, and click **OK**. The Edit page opens.
3. Under Select Mobile application to publish, select the folder that contains the application file that you want to publish:
   - For Android devices, select `.apk` file to create the package.
   - For iOS devices, select `.ipa` file to create the package.
4. Click **Next**. The Configure page opens.
5. Under the Package Information area, enter the following details:

Field	Description
Name	The name of the package. An instance with the value you provide in this field is created in the PACKAGE class of the MOBILE domain. This is a mandatory field.
Display Name	The friendly name of the package. This is a mandatory field.
Domain	The domain in which this instance is stored. The MOBILE domain is selected by default for mobile applications. It is recommended that you do not change the value for this field.
Description	Description of the package.
Release	The version number of the application that you are packaging. This value is pre-populated from the application manifest file; you must not modify this value. For Android only: An application can be upgraded only if a new version number is available for the application.
Class	The class for which this package instance is created.

6. Under the Limit package to systems with area, select the operating system for the device on which you want to deploy the application. Note that if you do not select any operating system, the application can be distributed to all devices with supported operating system. The Hardware settings are not applicable for mobile applications.
7. Click **Next**. The Service Information window opens. You can create a new service or use an existing service to deploy the package. Select **Use existing** if you want to publish update for an existing application. Select **No service** if you do not want to associate this package with a service.
8. Click **Create new** and enter the values for the Name, Display Name, Web URL, and Author field. The Name and Display Name fields are mandatory fields.
9. Click **Next**. The Publish window opens.
10. Review the Summary section to verify the service information you provided in the previous steps. When you are finished, click **Publish**.
11. Click **Finish** when the publishing process is completed to exit the Publisher.
12. Click **Yes** to confirm that you want to close the Publisher window.

13. The mobile application is published as a service in the CSDB. You can then entitle this service using Policy Management Wizard to a user or a user group.

For more information on publishing applications, see the *Radia Client Automation Enterprise Administrator User Guide*.

Updating an Application

You can provide update for an application that is already published in the CSDB. Follow these instructions based on the application for which you are providing an update:

- Updating applications for Android devices: Republish the application to the CSDB if a new version of the application is available. The application version is stored in the application manifest file. You must link this new package with the existing service that was used to deploy the package.
- Updating applications for iOS devices: You can provide update for an application in the following scenarios:
  - New version of the application is available: Republish the application to the CSDB if there is a change in the application version. You must link this new package with the existing service that was used to deploy the package.
  - Provisioning Profile has expired: Each iOS package (`.ipa` file) contains an application and a provisioning profile. This provisioning profile expires every 12 months. If the provisioning profile expires, the end-user will not be able to access the application. In such scenarios, an administrator must rebuild the application with the renewed provisioning profile, and publish it to the CSDB. You must link this new package with the existing service that was used to deploy the package.

Deploying Mobile Applications

Complete the following steps to entitle a mobile application to a mobile user or a user group:

1. Log on to the RCA Core Console.
2. Click **Management**, and then click the directory service that you have added to RCA.
3. Navigate to the user or user group for which you want to create the policy.
4. Select the user or a user group, and click **Launch Policy Management Wizard (Policy)** to open the Policy Management Wizard.
5. In the Service Selection page, select **Mobile domain** from the Service Domain list.
6. Select the service that you want to entitle to this user or user group and click **Add to Selection**.
7. Click **Next**. The Policy Configuration page opens.
8. Click **Next**. The Confirmation Summary page opens.
9. Click **Commit** to assign this policy to the selected users or group.

Managing Mobile Device Security

To manage security on a mobile device, you can create and deploy security profiles that enable securing the data on a mobile device if the device is lost or stolen. These profiles can also prevent unauthorized access to the device.

By default, RCA provides a pre-configured Wipe security profile that you can use to remotely wipe the device data. Note that you can apply the Wipe security profile only if RCA can contact the device. You cannot modify or delete this profile.

Caution: If you entitle Wipe security profile to a device, all device data is lost and the device is reset to factory settings.

You can also create new profiles that enable you to set the password settings or send commands to lock the device. The Security profile is published as a service in the CSDB. You can then entitle this service using Policy Management Wizard to a user or user group.

After you entitle the security profile, the device receives the new entitlements only when the next automatic timer is triggered on the mobile device.

A notification appears on the mobile device only if user intervention is required. For example, if the security profile is configured to set the user password, an RCA security connect notification appears in the notifications panel on the mobile device indicating the changes that are pending from the user.

Note: If you entitle more than one security profile to a user, the profile that imposes maximum security will be enforced on the device. For example, if you entitle following profiles to a user:

- At user level: Simple password value=true; Alphanumeric Password Value=true; Minimum Password Length=7
- At group level: Simple password value=false; Alphanumeric Password Value=true; Minimum Password Length=5; Number of complex characters in a password: 2

The resulting security profile that is enforced on the user is:

Simple password value=false; Alphanumeric Password Value=true; Minimum Password Length=7; Number of complex characters in a password: 2

Creating Android Security Profile

Complete the following steps to create a security profile for Android device:

1. Log on to the RCA Core Console and click **Operations** tab.
2. Expand **Mobile Management** in the left-navigation pane and click **Security**. The Security view opens in the details pane.
3. Click **Create a New Profile**, and then click **Android**. The Profile Creation Wizard opens.

4. In the Define Profile page, enter the details for the following fields, and click **Next**:

Field	Description
Display Name	The display name for the profile. The service will be referenced in the CSDB Editor using this name.
Description	The description of the profile.

5. In the Configure Profile Parameters page, enter the following details, and click **Submit**:

Field	Description
Password Settings: These settings are available only when you select the Password Required check box.	
Password Required	Select this check box if the managed mobile device user must have a password set for the mobile device.
Minimum Password Length	Enter a value for the minimum length of the password.
Password Strength	Select the type of characters the user must use when creating the password. The password quality and the password length determine the total password complexity.
Maximum Failed Password Attempts	Enter a value that defines the maximum number of times a user can enter a wrong password, after which the device is reset to factory settings.
Screen Settings: This setting determines the time a device can remain in idle state.	
Maximum Inactivity Time Lock	Enter the time (in minutes) the device can remain in idle state, after which the device is locked automatically. The maximum inactivity time set on the device overrides the Maximum Inactivity Time Lock value that you set in the profile, if the inactivity time already set on the device is greater than this value. An end-user might not be able to view the Maximum Inactivity Time Lock value that you set in the profile on the device because of device limitations.
Operational Settings: These setting can be applied only if RCA can contact the device. At any instance, you can apply only one of the operational settings. All other settings on this page are disabled.	
Reset Password	Select this check box to reset the password for the device.
Lock Now	Select this check box to lock the device.

Creating iOS Security Profile

Complete the following steps to create a security profile for iOS device:

1. Log on to the RCA Core Console and click **Operations** tab.
2. Expand Mobile Management in left-navigation pane and click **Security**. The Security view opens in the details pane.
3. Click **Create a New Profile**, and then click **iOS**. The Profile Creation Wizard opens.
4. In the Define Profile page, enter the details for the following fields, and click **Next**:

Field	Description
Name	The display name for the profile. The service will be referenced in the CSDB Editor using this name.
Description	The description of the profile.

5. In the Configure Profile Parameters page, enter the following details, and click **Submit**:

Field	Description
Password Settings: These settings are available only when you select the Password Required check box.	
Password Required	Select this check box if the managed mobile device user must have a password set for the mobile device.
Allow Simple Password Value	Select if the password must not contain any special character.
Alphanumeric Password value	Select if the password must contain alphanumeric characters.
Minimum Password Length	Enter a value for the minimum length of the password.
Number of Complex Characters in Password	Enter the number of non-alphanumeric characters that the password must contain.
Maximum Password Age	Enter the time (in days) after which the user must change the password.
Time Before Auto-lock	Enter the time (in minutes) the device can remain in idle state, after which the device is locked automatically.
Password History	Enter the number of passwords that the device remembers. A user cannot set a new password that matches the passwords available in the history list.
Grace Period for Device Lock	Enter the time (in minutes) for which the user is not required to enter the password again, if the user unlocks the device within the time you specify.
Maximum Failed Password Attempts	Enter a value that defines the maximum number of times a user can enter a wrong password, after which the device is wiped.

Field	Description
Restriction Settings: These settings are available only when you select the Restriction Settings Required check box.	
Restriction Settings Required	Select if you want to restrict the features a user can access on a device.
Allow Installing Apps	Select to allow the user to install applications on the device. By default, this setting is enabled.
Allow use of iTunes Store	Select to allow the user to use the iTunes store on the device.By default, this setting is enabled.
Allow Backup	Select to allow the user to create a backup on an iCloud account. By default, this setting is enabled.
Allow Document Sync	Select to allow the user to sync documents with an iCloud account. By default, this setting is enabled.
Allow Photo Stream	Select to allow the user to use the Photo Stream functionality. By default, this setting is enabled.
Operational Settings: These setting can be applied only if RCA can contact the device. At any instance, you can apply only one of the operational settings. All other settings on this page are disabled.	
Clear Password	Select this check box to reset the password for the device.
Lock Now	Select this check box to lock the device.

Modifying Security Profiles

You can modify an existing security profile. You must re-deploy the profile such that the changes are implemented in the device.

Complete the following steps to modify a security profile:

1. Log on to the RCA Core Console and click **Operations** tab.
2. Expand Mobile Management in left-navigation pane and click **Security**. The Security view opens in the details pane.
3. Click the name of the profile you want to modify. The profile window opens. Modify the settings in the Properties tab and then click **Save**.

Connecting RCA Servers to RCA Agents

The RCA agent on a mobile device must connect to the RCA servers, such that the desired state is always maintained for the mobile user. You can schedule a timed event when the mobile device connects to the RCA servers, or send a notify message to the mobile device to connect to the RCA servers. The connection can also be initiated manually from the mobile device, where the mobile device user triggers a software connect, audit connect, or a security connect.

Scheduling Timed Events

The RCA agent timers are run immediately after the agent install is complete. Note that all connects for software management, inventory management, and security management are run at this instance.

If the agent identifies that the mandatory applications defined in your entitlements are not installed on the mobile device, the message `RCA Software Connect->Installations are pending` appears in the Notifications Panel. You can then install the required applications.

By default, the agent timer runs once every day.

To modify the timer schedule, complete the following steps:

1. Log on to the RCA Core Console and click **Configuration** tab.
2. Expand Mobile Management in the left-navigation pane and click **Timer Settings**. The Timer Settings view is displayed in the details pane.
3. Specify the number of hours or days after which the timer should run, and then click **Save**.

To avoid simultaneous agent connections to the RCA servers, the hour-based timer is not run exactly after the number of hours you specify; instead a random number is added to the time you enter:

- If you specify the frequency between 0-6 hours, a random number between 0-3 hours is added to the actual time.
- If you specify the frequency between 6-12 hours, a random number between 0-6 hours is added to the actual time.
- If you specify the frequency between 12-24 hours, a random number between 0-12 hours is added to the actual time.

For example, if you set the timer to be run every 5 hours, a random number 2 is added. As a result, the timer is run after 7 hours for that device.

The new timer settings are applied only when the next timer-based connect starts. The timer-settings are not provided to the mobile agent as part of the user-initiated or push notifications.

Note that the when you schedule a timer-based event, all agent connects, Software connect, Audit connect, and Security connect are initiated at that instance.

Sending Notification from the Server

You can create a Notify job for a user or group of users to send a notification message to connect to the RCA server.

The following procedure shows how you can schedule a Mobile Audit Connect notify job:

1. Log on to the Core Console, click **Management** tab, and then click the directory service that you have added to RCA.
2. Navigate to the user or user group for which you want to create the job.

3. Select the user and click **Launch HPCA Job Creation Wizard** to open the RCA Job Creation Wizard.
4. From the Job Type list select **Notify**.
5. Enter a Name and Description for the job.
6. From the Job Action Template list, select the predefined mobile template. For example, select **Mobile Audit Connect** to schedule an Audit connect.
7. Select the platform from the OS Type list under Action Parameters.
8. Select the type of device from the Device Type list under Action Parameters, and then click **Next**.
9. Set the job schedule details and click **Next**.
10. Review the information on the Job Confirmation Summary page and click **Submit**.

For more information on how to schedule a job, see "Managing Jobs" on page 148 .

Limitations

This section provides the list of known limitations in RCA for MDM:

- *For iOS only*: You can publish and manage in-house mobile applications only. You cannot publish and distribute the applications that you download from App Store.
- *For Android only*: You can publish and manage free and in-house mobile applications. To distribute the paid applications available on Google Play, you must have an appropriate license agreement with the application vendor.
- For a single user, RCA cannot manage multiple types of devices on the same platform; you can manage only a single phone and a single tablet for that user. For example, you cannot manage two iPhone devices or two iPad devices for the same user.
- After a device has registered successfully with RCA servers, you cannot change the directory service for the user. The end-user must reinstall the agent and then register again with the new directory service.
- The RCA agent works in the following screen layouts:
  - For Android devices, the RCA agent works in portrait mode for phones, and in landscape mode for tablets.
  - For iOS devices, the RCA agent works in portrait mode for iPhone and iPad.

  Screen auto-rotation is not supported in the current release.
- On Android phones with small display screen size, the text in the Notification Panel appears truncated when opened from an application that supports portrait mode. To view the complete text, open Notification Panel from an application that supports landscape mode.

Using the RCA Agent on Mobile Devices

This chapter lists the prerequisites and tasks that a mobile device user must perform to install the Radia Client Automation (RCA) agent. The chapter also lists the steps to manually connect to the RCA servers.

Note: As an administrator, you can provide this help on you company's intranet, such that the mobile device users can access this help.

This chapter uses touch-based mobile devices as an example in all client-side procedures. The steps may vary if the RCA mobile agent is installed on a keypad-based device.

Installing the RCA Agent on Android Devices

You must install the RCA agent application when you receive an email from your enterprise administrator. The application runs primarily in the background and becomes active only when communication between the device and RCA server is initiated, to manage the device as per your enterprise policies set by the administrator. The RCA agent connects automatically to an RCA server to receive the latest entitlements.

Agent Prerequisites

The mobile device must meet the following prerequisites before installing the RCA mobile agent:

- If the device is accessing RCA servers from a corporate Wi-Fi, open the port 5228 (outbound) on the RCA agents to allow communication with the Google Cloud Messaging service.
- The device must have access to the Internet.
- The following requirements are specific to Android devices:
  - The mobile device must have a Secure Digital (SD) card.
  - A Google account must be configured and accessed at least once on the Android device. For example, xx@gmail.com.

Installing the Agent

Complete the following steps to install the agent:

1. Download the agent installer from Google Play on your device. The email that you received from your administrator contains the URL from where you can download the RCA mobile agent installer. After the download is complete, the file download details appear in the Notifications Panel.
2. Navigate to the file `RCAMobileAgent.apk` and click this file to start the installation. The RCAMobileAgent confirmation prompt appears that confirms the device features that this application accesses.
3. Tap **Install** to continue with the installation.
4. Tap **Done** to close the confirmation prompt. RCA Agent is listed on the Applications screen.

Registering the Mobile Device

To register the mobile device with the RCA servers, complete the following steps:

1. Tap **RCA Agent** listed on the Applications screen. The RCA Agent License screen appears.
2. Tap **I Agree** to continue with the installation. The RCA Server Details screen appears.
3. Enter the RCA server name or IP address in the Server field. You can obtain this value from the agent installation email that you received from your administrator.
4. Enter the port number in the Port field. You can obtain this value from the agent installation email that you received from your administrator.
5. Tap **Next**. The Authentication screen appears.
6. Enter your directory service logon name in the User Name field. This logon name is the name using which you log on to your corporate network. For example, if you log on to your corporate network as `Americas\ssimpson`, `ssimpson` is the directory service log on name.
7. Enter the password for the directory service logon name in the Password field.
8. Tap the down arrow for the Directory Source drop-down list, and then tap the domain name to which your logon name is associated with. For example, if you log on to your corporate network as `Americas\ssimpson`, `Americas` is your domain name.

   Note: If your administrator has provided a different display name when configuring this directory service with RCA, the domain name you use may not appear. Contact your administrator to identify your directory source.
9. Tap **Register** to start the registration process. The registration process can take a few minutes to complete.

After the registration process is successful, the Activate Device Administrator screen appears. Tap **Activate** to allow the RCA agent to collect the information listed on this screen.

Installing RCA Agent on iOS Devices

You are expected to install the Radia Client Automation (RCA) agent application when you receive an email from your enterprise administrator. The application runs when communication between the device and RCA server is initiated, to manage the device as per your enterprise policies set by the administrator. The RCA agent connects to the RCA server when you accept the application alerts in the Notification Center to receive the latest entitlements.

Agent Prerequisites

The mobile device must meet the following prerequisites before installing the RCA mobile agent:

- The device must be activated, and must have access to the Internet.
- If the device is accessing RCA servers from a corporate Wi-Fi, open the port 5223 (outbound) on the RCA agents to allow communication with the Apple Push Notification service (APNS).

Downloading the Agent

You can download the agent installer from the App Store. The email that you received from your administrator contains the URL from where you can download the RCA mobile agent installer.

Registering the Mobile Device

To register the mobile device with the RCA servers, complete the following steps:

1. Start the agent application installation:
   a. Tap the **Radia Client Automation Agent** icon on the Home screen to start the installation. The Radia Client Automation End User License Agreement screen appears.
   b. Tap **Accept** to continue with the installation.
2. Enter the RCA server name (or IP address) and port number in the Server and Port fields. Your administrator will provide this information to you before you can register.
3. Tap **Next**. The RCA Registration screen appears.
4. Enter your enterprise directory service logon name in the User field. This logon name is the name you use to log on to your corporate network.
5. Enter the password for the directory service logon name in the Password field.
6. Tap the domain name to which your logon name is associated with, from the Directory Services view. For example, if you log on to your corporate network as `Americas\ssimpson`, `Americas` is your domain name.

   Note: If your administrator has provided a different display name when configuring this directory service with RCA, the domain name you use may not appear. Contact your administrator to identify your directory source.
7. Tap **Enroll** to start the enrollment process. The Install Profile screen appears. During enrollment, the RCA agent installs RCA profile that contains certificates to authenticate your device connection with RCA and Apple servers. Tap **More Details** to view the certificates, RCA server details that your device connects to, and the administrative rights that an administrator has on your device.
8. Tap **Install** to start the profile installation process. A warning screen appears that provides you the information on what changes are made during the agent installation.
9. Tap **Install** to continue the installation process. After the registration process is successful, the Profile Installed screen appears.
10. Tap **Done** to complete the registration process.

On the Home screen, tap the **Radia Client Automation Agent** icon. A message box appears confirming the device connection to the RCA server. Tap **OK** to initiate this connection. If your administrator has set up device management policies, you will receive the required software applications and security settings entitled to your device.

At regular intervals, set by your administrator, RCA agent requests connection to RCA servers to obtain the latest entitlements. To access RCA servers, RCA agent issues notifications that you can view in the Notifications Center on your device. You must accept these notifications, such that the RCA agent can successfully connect to the RCA servers. Make sure that the RCA agent application is enabled for notifications. You can view the notification settings for your device using **Settings**>**Notifications**. Additionally, based on the alert style that you have set for the

notifications, the RCA agent notifications appear in the Notification Center, or as a pop-up message.

If the device is locked when the notification is issued, the notification appears on the locked screen. After unlocking the device, you can view the notification in the Notifications Center on your device.

Manually Connecting to the RCA Server

Note: RCA agent connects to RCA server automatically on a regular basis to receive the latest entitlements. You will normally not run this agent manually, but only at the direction of your RCA administrator.

To connect manually to the RCA servers, complete the following steps:

1. Search for the RCA Agent application:
   a. Android devices: Open **Applications** screen, tap **RCA Agent** icon.
   b. iOS devices: On the Home screen, tap **Radia Client Automation Agent** icon.

   The RCA Agent screen opens with the options to initiate one of the agent connects.
2. Tap one of the available icons, under Applications, Device Info, or Security Profiles to initiate the connection with the RCA servers.
   - Software Management: Tap **Applications** icon to retrieve the latest software entitlements from the RCA servers. A notification message appears if there is a new application, an update to an existing application, or if the application must be deleted.
   - Inventory Management: Tap **Device Info** icon to send the latest inventory details about your device to the RCA servers, such as software and hardware details.
   - Security Management: Tap **Security Profiles** icon to retrieve the latest security profile settings, if entitled to your device. You cannot delete any security profile that is entitled to your device.

Uninstalling the RCA Agent

Complete the following steps to uninstall the RCA agent:

Android Device

1. On the home screen, tap **Settings**>**Security**>**Device administrators**.
2. Tap **Radia Client Automation** to disable it.
3. On the home screen, tap **Applications** >**Downloaded**.
4. Tap **RCA Agent**. The App info screen opens with the Uninstall option.
5. Tap **Uninstall**.

iOS Device

Note: When you uninstall the RCA agent and the Radia Client Automation configuration profile, all the applications that are managed using RCA are uninstalled from your device.

1. On the home screen, tap **Settings**>**General**.
2. Tap **Profiles**. The Profiles screen appears that lists all the Configuration and Provisioning Profiles installed on your device.
3. Under Configuration Profiles, tap the **Radia Client Automation** configuration profile, and then tap **Remove**.
4. On the Home screen, tap and hold the **Radia Client Automation Agent** icon. The delete symbol icon appears on left-top corner of the icon.
5. Tap the delete symbol to remove the agent.

Chapter 7

Using Reports

The Reporting area contains summary and detailed reports of many kinds. The following topics are discussed in this chapter:

Reports Overview

On the Reporting tab in the RCA Console, there are links to several collections of reports as described in "Types of Reports" on page 207.

Each collection contains groups of reports that focus on a particular type of data or a specific audience. These reports also provide the data used to populate the dashboards.

The following reports are available in all editions of RCA:

Report Pack	Report Type	Description
rpm.kit	Patch Management	Devices in and out of compliance with patch policy
rim.kit	Inventory	Devices currently managed by RCA

The following reports are available only in RCA Enterprise:

Report Pack	Report Type	Description
vm.kit	Vulnerability Management	Security vulnerability information, including vulnerability definitions and the results of client device scans
compliance.kit	Compliance Management	Compliance management information, including Secure Content Automation Protocol (SCAP) compliance rules and the results of compliance scans on managed client devices
stm.kit	Security Tools Management	Security tools management information, including anti-virus, anti-spyware, and software firewall installation and configuration.
hpca.kit	HPCA Management	Audit reports

Report Pack	Report Type	Description
mobility.kit	Mobility Management	Mobile device management reports.

For additional information about report packs, see the *Radia Client Automation Enterprise Reporting Server Reference Guide*

Note: In order to view the Reporting section's graphical reports, a Java Runtime Environment (JRE) or Java Virtual Machine (JVM) is required. For more information, go to:

http://java.com/en/index.jsp

Navigating the Reports

When you click the Reporting tab, the Reporting home page is displayed. The home page provides a snapshot of the enterprise with respect to compliance management, vulnerability management, security tools management, inventory management, and patch management (if installed and enabled), and usage management (if enabled).

There are three ways to find more detailed information on the Reporting home page:

- Use Report Quicklinks to open frequently requested reports.
- Use Quick Search to find inventory information about a specific device or service. This feature *only* applies to inventory reports – for example, Managed Devices – and does not apply to vulnerability management reports or compliance management reports.
- Use the links in the Reporting Views section of the left navigation tree to open a specific report. A Reporting View defines the set of reporting windows to display for the current data set and initial settings related to each window (such as minimized or maximized, and the number of items per window). When you first access the reports, the Default View is applied. The current view is listed on the right of the Global Toolbar. You can change or customize your Reporting View.

The following actions are available on the Reports page when a report is displayed:

Report Actions

Icon	Description
	Go back one page in the reports view.
	Return to the Reports home page.
	Refresh the data. A refresh also occurs when you apply or remove a filter.
	Add this report to your list of favorites.
	Email a link to this report.

Icon	Description
	Open a “quick help” box or tool tip. This applies only to filters.
	Print this report.
	Collapses the data portion of the report view.
	Expands the data portion of the report view.
	Show the graphical view of this report
	Show the grid (detailed) view of this report.
	Export report contents to a comma-separated value (CSV) file. The data in this file is actually delimited by tabs, not commas. The file extension is CSV, however.
	Export report contents to a Web query (IQY) file.

Items that appear in blue text in a report have various functions:

- Show Details – drill down to greater detail pertaining to this item
- Launch this Reporting View – open a new report based on this item
- Add to Search Criteria – apply an additional filter to the current report based on this item
- Go to Vendor Site – go to the web site of the vendor who posted this bulletin

When you rest your mouse over a blue text item, the tool tip tells you what will happen when you click the item.

Note: By default, the reports use Greenwich Mean Time (GMT). Individual report packs can be configured to use either GMT or local time.For more information, see the *Radia Client Automation Enterprise Reporting Server Reference Guide*.

Types of Reports

The following types of reports are available in the RCA Console:

- "Infrastructure Management Reports" on next page
- "Inventory Management Reports" on next page
- "Application Management Profiles Reports" on page 209
- "Settings Management Reports" on page 209
- "RCA Management Reports" on page 210
- "Patch Management Reports" on page 210
- "Usage Management Reports" on page 211
- "Vulnerability Management Reports" on page 211

Infrastructure Management Reports

The Infrastructure Management reports show detailed information about Satellite server synchronization status. Expand the Infrastructure Management reporting view to see the reports listed under Metadata Synchronization and Satellite Cache Reports.

The **Metadata Synchronization Status** report shows the start and end time for metadata synchronization. This report also includes the status of the metadata synchronization and lists the domains that are synchronized.

The **Cache Detail Report** shows the free disk space, cache location, and number of services available for each Satellite server.

Inventory Management Reports

Inventory Management reports display hardware and software information for all devices in RCA. This includes reports for HP specific hardware, device components, blade servers, TPM Chipset information and SMBIOS information, and Self-Monitoring, Analysis, and Reporting Technology (S.M.A.R.T.) Alerts.

Expand the Inventory Management Reports reporting view to see the report options. To be included in these reports, devices must be entitled to AUDIT.ZSERVICE.DISCOVER.INVENTORY. Certain data is only available after RCA is fully configured. See "Device Management" on page 307 for configuration details.

A typical Managed Devices report includes the following table headings:

- **Details** – opens a Device Summary page for this device.
- **Last Connect** – when the device last connected.
- **RCA Agent ID** – device name.
- **RCA Agent Version** – the currently installed Management Agent version.
- **Device** – device name.
- **Last Logged on User** – the last user account used to log on to the device. If multiple users are logged on, only the last to log on is recorded—switching between currently logged on users does not affect this.
- **IP Address** – device IP address.
- **MAC Address** – device MAC address.
- **Operating System** – operating system installed on the device.
- **OS Level** – current operating system level (for example, Service Pack 2).

Inventory Management Reports consist of the following report options:

- Executive Summaries
- Operational Reports
- Hardware Reports
- Software Reports
- Readiness Reports
- Power Utilization

For more information on these reports, see *Radia Client Automation Enterprise Inventory Manager Reference Guide*

Application Management Profiles Reports

The Application Management Profiles reports show detailed information about Application Management Profiles (AMPs). AMPs include a set of tools that enable you to deploy and manage complex software products that are typically required on the managed clients and servers in a Client Automation environment.

The Application Management reports allow you to drill down and see detailed AMP information by device and service.

Expand the Application Management reporting view to see the report options. Under Application Management, there are the following reports:

- **Job Status by Device** - Displays detailed AMP information ordered by device. This report includes profile deployment status for each device and scheduled deployment job information.
- **Job Status by Service** - Displays detailed AMP information ordered by the Service ID of the AMP. This report includes a description of the service, the number of devices on which the service is deployed, as well as AMP deployment status and scheduled deployment job information

Settings Management Reports

The Settings Management reports show settings profile information for those devices on which a settings profile has been deployed. A settings profile consists of configuration settings for a specific software installed on a managed device in your environment. Once settings profiles have been created and deployed, it is possible to see summary reports about the software giving administrators visibility to the run-time data of this software.

The Settings Management reports allow you to drill down and see detailed settings profile information by device, profile service ID, and category when you click on individual columns in the provided reports.

Expand the Settings Management reporting view to see the report options. Under Settings Management, there are the following reports:

- **Profile Status by Device** - Displays detailed profile information ordered by device for each device that has the software installed. This report includes profile deployment status for each device and scheduled deployment job information.

- **Profile Status by Service** - Displays detailed profile information ordered by the Profile Service ID of the settings profile. This report includes a description of the service, the number of devices on which the service is deployed, as well as profile deployment status and scheduled deployment job information.
- **Profile Status by Category** - Displays detailed profile information ordered by the type of software. This report allows you to view a list of categories along with profile deployment status and scheduled job deployment information for each category. Categories are broad descriptions of software functionality.
  Examples include HP Power Management, Wireless Settings, and Security settings. Each category may have profiles, which are specific configurations for that category's settings. For example, the HP Power Management category could have power profile settings for Low, Medium, or High.
- **Acquisition Details** - Displays the status of the content updates from HP Live Network.

RCA Management Reports

The RCA Management Reports contain management information for various RCA functions. Expand this view to see the following reporting options:

- **Live Network** - Under this option, you can view the Acquisition History report. It displays a list of acquisition events, the date of each acquisition, acquisition details (allows you to drill down to another report), acquisition sources, and acquisition status.
- **Auditing** - Under this option you can view the Remote Control report. It contains an entry for each remote control session attempted from the RCA Console to a managed client device.

Patch Management Reports

Patch Management Reports display patch compliance information for managed devices and acquisition information for patches and Softpaqs.

- **Executive Summaries** – Executive Summary reports offer pie or bar charts to provide a visual snapshot of patch-compliance for the devices and bulletins being managed in your environment. The reports summarize compliance for all devices, for devices by patched-state, for bulletins, and bulletins by vendors. From the summary reports you can drill down to the detailed compliance reports which offer additional filtering.
- **Patch Compliance Details** - The RCA Agent sends product and patch information to RCA. This information is compared to the available patches to see if managed devices require certain patches to remove vulnerabilities. Compliance reports show only the information applicable to detected devices in your environment.
- **Acquisition Reports**– Acquisition-based reports show the success and failures of the patch acquisition process from the vendor's web site. They include the following reports:
  - **Acquisition Summary** report shows the number of bulletins, patches, and errors for each acquisition session. In addition, it provides links to the acquisition reports for all bulletins and patches. The date and time of the publishing session is also listed.
  - **Acquisition by Bulletin** report shows a summary of the bulletin’s acquisition. From this report, you can click on the number for Applicable Patches to see the files associated with the bulletin. Note that one bulletin may have multiple patches based on platform.

  - **Acquisition by Patch** report shows a summary of each patch's acquisition. You can click on an item in the Product/Release column for a specific bulletin to drill down for full details on the patch. The icon in the Severity column indicates the severity for Windows patches.

- **Research Reports** – Research-based reports display information about the patches acquired from the software vendor's web site. Research-based reports offer a Filter bar.

For details on using the Patch Management reports, see the *Radia Client Automation Enterprise Patch Management Reference Guide*.

Usage Management Reports

Usage Management Reports show usage information for devices that have the Usage Collection Agent installed. Use the "Deploying the Usage Collection Agent" on page 176 to install the collection agent and begin collecting usage data.

- **Top 10 Used Products Reports** – Displays the usage for the top 10 products that are used by the User Accounts and the Computer Accounts.
- **Executive Summaries** – Display graphical representation of devices collected and usages by vendor and product.
- **Device Reports** – Display usage specific information such as details of devices and users using the application.
- **Monthly Usage Reports** – Display usage information by vendor, product, and application in a month.
- **Inventory Reports** – Display inventory information by vendor, product, and application.
- **Operational Reports** – Display the number of devices from which data has been collected or has not been collected in last 30 days.

For details on using the Usage Management reports, see the *Radia Client Automation Enterprise Application Usage Manager Reference Guide*.

Note: After the Usage Collection Agent is deployed, Usage Time collection begins right away. Focus Time collection does not begin until the next time the user logs on.

Note: Most logical folders (Program Files, for example) are machine-related and not associated with an individual user. Therefore, Usage Management Reports, Device Reports, and the Usage by User report may contain [undefined] in the User Name column.

Depending on the Usage Settings defined in the Configuration tab, Reporting section, some or all usage data may be obfuscated.

Vulnerability Management Reports

The Vulnerability Management reports are organized in three groups:

- **Executive Summaries** – These reports provide a snapshot of vulnerability management activities and trends in your environment.

- **Vulnerability Reports** – These reports contain vulnerability definitions and detailed information about vulnerabilities detected in your environment.
- **Device Reports** – These reports contain information about vulnerabilities detected on specific devices in your environment.

You can filter many of these reports or drill down for additional detail. In any report that lists vulnerabilities, for example, you can drill down using the OVAL identifier or CVE identifier for a particular vulnerability to access a link to the pertinent vendor bulletin (if available). Vendor bulletins typically contain remediation information and sometimes include software patches.

Note: When you drill down into a report for more detailed information, the data may be filtered in a different way than the data displayed in a summary level report. See "Filtering Reports" on page 216 for more information.

These reports are displayed on the Reporting tab. Some of the reports are also available from the "Vulnerability Management Dashboard" on page 91.

Compliance Management Reports

The Compliance Management reports are organized in three groups:

- **Executive Summaries** – These reports provide a snapshot of your environment from the compliance management perspective. Use these reports to quickly assess the following:
  - How many client devices are in or out of compliance
  - Which compliance rules are most frequently violated
  - Which client devices are the most noncompliant
- **SCAP Reports** – These reports show the number of client devices that are currently in or out of compliance with each Secure Content Automation Protocol (SCAP) benchmark included in your scans.
- **Device Reports** – These reports show you the results of the most recent compliance scan for each scanned client device. They also show you which client devices were not scanned.

You can filter many of these reports or drill down for additional detail. See "Find Information about Compliance Failures" on page 59 for more information.

Note: When you drill down into a report for more detailed information, the data may be filtered in a different way than the data displayed in a summary level report. See "Filtering Reports" on page 216 for more information.

These reports are displayed on the Reporting tab. Some of these reports are also available from the "Compliance Management Dashboard" on page 104.

Security Tools Management Reports

The Security Tools Management reports are organized in four groups:

- **Executive Summaries** – These reports tell you when your anti-virus and anti-spyware definitions were last updated on your managed client devices and when these devices were last scanned for viruses and spyware.
- **Product Reports** – These reports contain information about the anti-virus, anti-spyware, and firewall products detected on your client devices.
  - For each type of product, you can view a list of all products detected and a list of devices where these products were found.
  - For anti-virus and anti-spyware tools, you can view the date of the last definition update and scan for each pertinent device.
  - For firewall products, you can view a list of the firewall rules.
- **Device Reports** – These reports tell you whether each type of security tool is installed, enabled, or both on each client device.
- **Profile Reports** –These reports show you the status of your remediation jobs for the security tools installed on the managed devices in your environment. They indicate if the jobs to turn on the security tool, to update definitions, and to schedule a scan executed successfully or not. The remediation options are determined by template profiles that you can configure through the RCA Console. See "Security Management" on page 248. A profile consists of configuration settings for a security tool in your environment. Once profiles have been created and deployed, it is possible to see summary reports about the remediation. The Profile Reports allow you to drill down and see detailed profile information by service and device when you click on individual columns in the provided reports. Under Profile Reports, there are the following reports:
  - **Profile Status By Service** – Displays information about the profile, links to profile devices with the number of tasks performed, and the status of the performed task.
  - **Profile Status By Device** – Displays information about the device, the number of profiles executed, and the number of successful and failed profiles.
  - **Profile Status By Category** – Displays detailed profile information ordered by the type of template. It displays information about the devices, the number of profiles executed, and the number of successful and failed profiles.

The Security Tools Management reports are displayed on the Reporting tab. Some of the reports are also available from the Security Tools Management dashboard.

You can filter many of these reports or drill down for additional detail. See "Find Information About Security Tools" on page 60 for more information.

Note: When you drill down into a report for more detailed information, the data may be filtered in a different way than the data displayed in a summary level report. See "Filtering Reports" on page 216 for more information.

These reports are displayed on the Reporting tab. Some of these reports are also available from the "Security Tools Management Dashboard" on page 113.

The following reports include summary statistics about the state of the security tools on your managed client devices:

- Product Summary (under Executive Summaries)
- Discovered Products (under Product Reports > All Products)

- Devices Scanned (under Device Reports > Scanned Devices)

These statistics are also displayed when you expand the **Discovered Security Product Statistics** banner in the Device Detailed View for a particular scanned device. To display this view, follow these steps:

1. Open the **Device Reports** > **Scanned Devices**.
2. Click the **Details** icon for a particular device.
3. In the Device Details section, click the **Details** icon again.

Virtualization Management

You can publish, deploy, and update virtual applications in your RCA environment. Using the Virtualization Management reporting options, you can view the current status for the VMware ThinApp and Microsoft Application Virtualization applications that are deployed on the RCA agents.

VMware ThinApp Reports

The VMware ThinApp Reports enable you to drill down and see detailed information about the ThinApp services that are installed in your RCA environment. Expand the VMware ThinApp Reports view to see the following reporting options:

- ThinApp Services: Lists all VMware ThinApp applications that are published to the RCA CSDB. It also shows the services that are AppSync enabled. When these services are deployed to a client, they will be automatically updated according to the notify schedule.
- Managed ThinApp Services: Lists all VMware ThinApp Applications that have been deployed to clients.
- ThinApp Update Activity: Lists the ThinApp Applications that have had updates applied by the ThinApp Updater service.

Microsoft App-V Reports

The Microsoft App-V Reports enable you to drill down and see detailed information on the App-V services that are installed in your RCA environment. Expand the Microsoft App-V Reports view to see the following reporting options:

- **Published App-V Services**: Lists all Microsoft App-V applications that have been published to the RCA CSDB. You can also view the date when these applications were published.
- **Managed App-V Services**: Provides detailed information on the Microsoft App-V applications that have been deployed to clients. You can view the number of subscribers, number of times the application was installed, uninstalled, verified, updated, or repaired.

Mobile Device Management Reports

The Mobile Management reports provide hardware and software related information for mobile devices managed using RCA. The reports include information on the device platform, applications downloaded and installed on the device, and the type of devices that are managed (smartphones or tablets) using RCA.

Note: For mobile devices, the columns in the inventory reports and the reports accessible from the Dashboard tab are populated based on the mobile device capability. For example, the RCA Agent Version, IP Address, and MAC Address columns are shown blank for any mobile device in the **Reporting**>**Inventory Information**>**View Managed Services** report.

The Mobile Management reports include the following reporting options:

- Executive Summaries: The Hardware Summary report provides details on the managed mobile devices by platform and by vendor. These reports can be viewed in bar graph view or a detailed view.
- Operational Reports: These reports provide details on the number of mobile device connections and service events sent by the mobile device to the RCA server. The Managed Devices report provides the number of devices that have connected in the last 24 hours, 30 days, and 12 months. The Managed Services report provides the number of service events that are sent in the last 24 hours, 30 days, and 12 months.
- Hardware Reports: These reports provide hardware specific information for the mobile devices in your RCA environment. This section includes the following reports:
  - Hardware Summary: Displays details for the managed mobile devices that are filtered based on the platform, platform version, vendor, and device model.
  - Managed Devices: Displays details for the mobile devices that are managed using RCA. The details include last connect time, device ID, operator name, and platform details.
  - Devices by Platform: Displays details for the managed mobile devices that are filtered based on the platform.
  - Devices by Vendor: Displays details for the managed mobile devices that are filtered based on the vendor.
  - Devices by Device Type: Displays details for the managed mobile devices that are filtered based on the device type, such as tablet or a smartphone.
- Software Reports: These reports provide information related to the services that you have entitled to the mobile devices in your environment. This section includes the following reports:
  - Managed Service Reports: This section includes the following reports:
    - Service Summary: Provides the summary of the services that have been entitled to the mobile devices. This report shows the number of users for each service, and whether the service has been downloaded or installed on the mobile device. The Download column is updated when a subscriber downloads a service, but does not install that service. Whenever a service is installed, the value in the Download column is decreased, and the value in the Install column is updated.
    - Managed Services: Displays details for services entitled to the mobile devices, such as number of users, number of downloads, and number of uninstall attempts.
    - Pending Services by Device: Displays the details of the service entitled to the mobile user that has been downloaded on the mobile device, but has not been installed.
  - Managed Software Reports: The Manage Software by Product report in this section contains the details for the devices where each software application is installed.

- Security Reports: The Security Details Reports contains details on current security settings on the device. The security profile on a mobile device can be enabled only when the device administrator is activated on the mobile device. To verify the devices that have not activated the device administrator, check the Enabled column. A true value indicates that the device administrator (security administration) is activated. A false value indicates that the device administrator has not been activated on the mobile device. The other columns in this report, such as Minimum Password Length and Maximum Screen Lock Time provide the current security settings on the device even if the device administrator is disabled. This report also provides the number of remote wipe commands that have been attempted on a device.
- Registration Reports: The PUSH Registration Detail Reports provides the current registration status for a device. For iOS devices, the reports are populated only if the registration is successful, after all the profiles have been installed. For Android devices, this report contains details related to the push notification mechanism between the RCA servers, Google servers, and the mobile device. The GCM process does not guarantee a 100% data delivery to the mobile device. To verify if the mobile device is receiving messages from the Google servers, check the PUSH Registration Status column in this report. A true value indicates that the messages are delivered to the mobile device. A false value indicates that the message delivery has failed. The error message for the message delivery failure is listed in the Registration Error column. The following table lists the possible error messages and cause if the push notification fails for a mobile device:

Error	Cause
SERVICE_NOT_AVAILABLE	This error can occur if one of the following conditions are true: ▪ Auto-sync is not enabled on the mobile device. ▪ Mobile device does not have Internet access.
ACCOUNT_MISSING	The Google account ID is not configured on the mobile device.

Drilling Down to Detailed Information

Many reports enable you to drill down to very detailed information about a particular device, vulnerability, compliance benchmark, or security product.

Whenever you see the Details () icon in the data grid, you can click it to display more detailed information.

You can also drill down to more detailed information by clicking the device counts in certain columns in some reports.

Filtering Reports

Many reports contain large amounts of data. You can apply one or more filters to a report to reduce the amount of data displayed. If you apply a filter, that filter will remain in effect until you explicitly remove it.

There are three basic types of filters:

- Directory/Group Filters enable you to display data for a specific device or group of devices.
- Inventory Management Filters enable you to display data for a group of devices with common characteristics, such as hardware, software, operating system, or RCA operational status.
- Report specific filters apply only to data available within a specific Reporting View. For example, Patch Management filters apply only to Patch Management reports.

A filter only works if the type of data that it filters appears in the report.

If you attempt to apply a filter that does not pertain to the data in the current report, the filter will have no effect. Conversely, if the data in a report does not look correct, check to ensure that an incorrect filter has not been applied.

Because they contain small amounts of data to begin with, most Executive Summary reports cannot be filtered.

Apply Filter to a Report

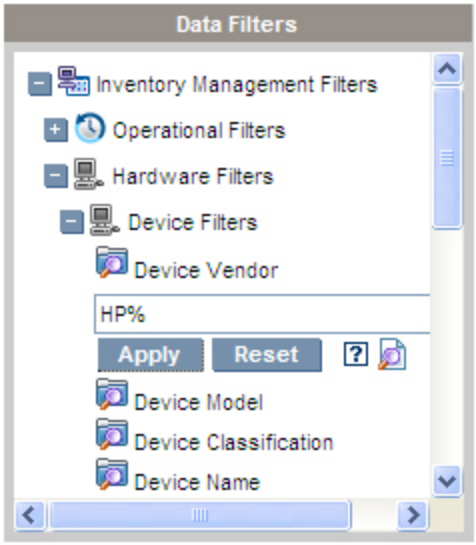
To apply filter to a report, follow these steps:

1. In the Data Filters section of the left navigation tree, expand the filter group that you want to use.
2. *Optional*: For the specific filter that you want to apply, click the  (show/hide) button to show the filter controls:
3. Specify the filter criteria in the text box, or click the  (criteria) button to select the criteria from a list (if available—not all filters have lists).
   You can use wildcard characters when creating filters. The following table describes the characters you can use to build search strings.

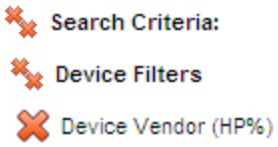
   Special Characters and Wildcards

Character	Function	Device Vendor Filter Example	Records Matched
* or %	Matches all records containing a specific text string	HP*	All records that begin with “HP”
		%HP%	All records that contain “HP”
? or _	Matches any single character	Not?book	All records that begin with “Not” and end with “book”
		Note_ook	All records that begin with “Note” and end with “ook”
!	Negates a filter	!HP*	All records that do not start with “HP”

   For example, if you specify HP% in the text box for a device related filter, the filter will match all devices whose Vendor names contain HP.



4. Click the **Apply** button. The report will refresh. To remove the filter, click the **Reset** button. When you apply a filter to a report, the filter is listed in the report header:



A filter is in effect until you explicitly remove it. Click the (Remove) icon to the left of the filter name to remove a filter from the current report.

Note: You can also create an "in-line" filter by clicking a data field in the report currently displayed. For example, if you were viewing a Vulnerability Definitions report, and you wanted to see only those vulnerabilities with High severity, you would click the (High Severity) icon in the Severity column.

Device Groups for Data Roll-Up

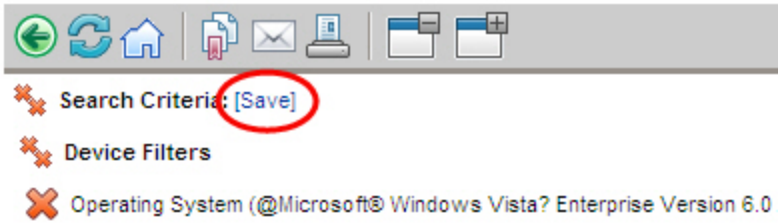
The RCA Console provides a mechanism for defining specific groups of devices for the purpose of performing data "roll-up" operations—where information about these devices is retrieved from the RCA database and then aggregated (rolled up) over a specified period of time.

This is useful, for example, if you are using another HP Software product that communicates with RCA and consumes data delivered in the form of RCA reports—or the database tables used to populate the reports.

To perform the actual data roll-up, you would create a DTM job using an appropriate job action template, such as the HPCA Nightly Summary template. Be sure to specify the job schedule such that data roll-ups are performed at least 24 hours apart. See "Create a New DTM or Notify Job" on page 154 for more information.

To create a data roll-up device group::

1. On the Reporting tab, open a report that lists devices. For example:
   Inventory Management Reports > **Hardware Reports** > **Detail Reports** > **Managed Devices**
2. Apply the filter criteria that you want to use. Make sure that the devices that you want to see are included in the report. See "Filtering Reports" on page 216 for more information.
3. Click the **[Save]** link located to the immediate right of the **Search Criteria** heading in the upper left hand corner:

   The Reporting Filter Save Wizard opens.
4. Enter a **Display Name** for your device group. This name will be used by other HP Software products that consume the roll-up data. You may type up to 32 characters.
5. Enter a **Description** for your device group. This information is for the benefit of the people who will view the roll-up data. You may type up to 255 characters.
6. Select **Use for Rollup Reports** if you want to use this device group for data roll-up operations.
7. Select **Overwrite Existing** if you want to replace an earlier version of your saved device group with this one.
8. Click **Create**. Your device group is saved and is now available to use.

Chapter 8

Operations

The Operations tab allows you to manage infrastructure tasks, view the status of component services, and perform some patch management tasks. Additional details are described in the following sections.

The Satellite Console Operations tab provides Server Status and Support information as described in the following sections.

Infrastructure Management

Infrastructure Management operations are described in the following sections:

Server Status

Server Status displays the currently installed license information as well as a list of the component services that are controlled by the RCA server. These component services handle different aspects of RCA processing. The Server Status **Summary** table allows you to see which of these services are enabled.

The Satellite Console Server Status page displays additional properties.

- Upstream Server
- Apache Server cache usage

- Apache Server cache capacity
- Proxy Server static cache usage
- Proxy Server dynamic cache usage
- Synchronization status

The Satellite Console's Server Status page includes a **Tasks** area that enables you to update the data caches.

- **Reviewing the status of component services**
  a. On the RCA Console, click **Operations** tab and click **Server Status**.
  b. View the Summary table that lists the component services and their status.
- **Synchronizing Satellite Now**

  The Satellite server's contents (operating systems, patches, and operating system images) must be synchronized with an upstream host.

  Note: Before you can cache and synchronize data on a Satellite Server, you must have initially configured Satellites. See the *Radia Client Automation Enterprise Installation and Upgrade Guide* for details.

  Running the synchronization will synchronize the content that is used by the services that are enabled on the Satellite. For example, if the Satellite is a full-service Satellite, it will synchronize:

  - RCA agent maintenance
  - Configuration metadata
  - Apache Server cache resources for Patch Manager Gateway binaries and Security and Compliance Gateway binaries (requires Apache Server cache service to be enabled)
  - Proxy Server cache resources for software, patches, operating system, security, and audit.

  Satellite server synchronization can be scheduled by creating a job on the Core server. See "Creating Satellite Synchronization Jobs" on page 157 for additional information.
- **Flushing Apache Server Cache**

  You can flush the resource cache when:

  - There are critical new resources to download from an upstream server and the current Apache Server cache usage is close to capacity
  - The Apache Server cache contains outdated or corrupt files.

  Caution: This option flushes entire Apache Server cache and could result in the accidental deletion of important files.

  Note: The dynamic cache for the Integration Server-based Proxy server is automatically flushed according to the `-dynamic-maxsizeMB` attribute set in the `rps.cfg` file available at `<Installdir>\ProxyServer\etc`.

Support

The Support area displays the currently installed license information and also allows you to generate and download a compressed (zipped) file that contains configuration files, log files, and operating system information.

These files can then be available for Persistent Support should they be needed for troubleshooting.

Download Log Files

When working with support, you may be asked to supply log files. Use the link provided to download and save a compressed file of current server log files.

To download log files:

1. In the Troubleshooting area, click the link **Download Current Server Log Files**. A new window opens.
2. When the log files are prepared, click **Download logfiles.zip.**
3. When prompted, click **Save** to store the compressed file on your computer.
4. Specify a location to store the file and click **OK**.
5. The log files are downloaded to your computer and saved in a single ZIP formatted file.

> **Note:** Internet Explorer security settings may prevent these files from being downloaded. It recommends adding the RCA console URL to your trusted sites or modifying your Internet Explorer settings to not prompt for file downloads.

Live Network

Use the Live Network settings to specify how and when the HP Live Network content is updated. You can set up a schedule for automatic updates or initiate an immediate update. You should always perform an update after you install or upgrade your HPCA software to ensure that you have the most current content.

See "Accessing HP Live Network Content" on page 127.

Whether you choose to schedule automatic updates or initiate an immediate update, you must specify the content source for the update. You have the following choices:

- **From the HP Live Network**
  The live network content source is retrieved from the HP Live Network content server and published to the RCA infrastructure. By default, this path is:

  <InstallDir>`\LiveNetwork\lnc\bin\live-network-connector.bat`

  This path is configured automatically by RCA. You do not need to specify this path unless you have downloaded a new copy of the HP Live Network Connector and installed it in a different location.

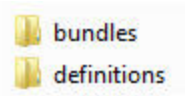
  To use this option, you must have an active HP Live Network subscription. This is not included in your HPCA software. See your Persistent representative for details.

It is possible to select content type (premium or basic) depending on your access rights.

Note: If you select a content type to which you do not have rights (for example, premium content), the entire acquisition will fail. This means that no content types will be updated including the ones covered by a basic support contract (basic content). Be sure you select just those content types to which you are entitled to avoid acquisition failure.

- **From the File System**
  A copy of the live network content is published from a location in the file system on the system where the RCA Core is installed. You must specify the path of the folder that contains the content, and you must manually download these items from the HP Live Network content server before you can initiate an update.

  The folder structure from the file system location specified must exactly match the folder structure that is created when the HP Live Network Connector downloads content, as shown here:

  The subdirectories under each of these folders must also match exactly.

  In some cases, HP Live Network updates only a subset of the content. In this case, some of these directories may not be delivered during a Live Network update.

  For more information about using this option, see "Run the HP Live Network Connector Manually" on page 439.

- **From the Configuration Server Database**
  The content previously published to the CSDB are loaded into the Reporting database.

  See "Move HP Live Network Content from a Test Environment to a Production Environment" on page 441.

Schedule Automatic Live Network Updates

Use the following procedure to establish a schedule for automatic HP Live Network updates from the content source of your choice.

To schedule automatic HP Live Network content updates:

1. On the Operations tab, expand the Infrastructure Management area, and click **Live Network**.
2. Click the **Schedule Updates** tab.
3. In the Updates section, select the content source.
4. Specify the schedule for automatic updates:
   a. **Schedule**—Select Once, Hourly, Daily, Weekly, or None

   b. None is what the RCA Console shows when nothing is currently scheduled to execute—for example, when a previously scheduled Once task has already completed. You can specify None if you do not want to schedule anything new or if you want to stop an existing

schedule. If there is a recurring schedule, the most recently saved schedule is shown (for example, Hourly, Daily, or Weekly).

c. **Start Time**—Time of day to start the updates.

d. **Start Date**—Date to start the automatic updates. Click the (calendar) button, and select the date.
When the **Schedule Updates** tab is displayed, the time and date fields show the time and date of the last saved schedule. For example, if a previously scheduled Once update has already completed, the Schedule will be set to None, and you can see the time and date of the last update in the Start Time and Start Date fields.

e. If you selected Hourly, Daily or Weekly for the **Schedule**, specify the update interval in the **Every** box.
For example, if you select Daily, with an **Every** interval of two, this will run an update every two days.

5. Click **Save** to implement your changes.

Note: If you leave this tab, any information that you entered before clicking **Save** will be lost. Be sure to click **Save** if you want to keep this information.

Note: You can use the Reset button to restore the most recently saved settings.

Update the HP Live Network Content Now

Use the following procedure to update your HP Live Network content now. This does not affect any schedule that you have established for automatic updates.

To update the HP Live Network content immediately:

1. On the **Operations** tab, expand the **Infrastructure Management** area, and click **Live Network**.
2. Click the **Update Now** tab.
3. Select the content source for this update. This will not affect any automatic updates that are currently scheduled.
4. Click the **Update Now** button. A request is issued to update your content from the content source that you specified.

An update is an asynchronous process that requires some time to complete. You can use the acquisition reports to view the results of an update or check its status.

View the Results or Status of an Update

You can use the RCA reports to check on the status of an HP Live Network content update. You can access the reports that display this information in one of the following ways:

- Click the **Reporting** tab from **Operations** > **Infrastructure Management** > **Live Network**. This is the most convenient way to view the status of the content updates from this location.

- Click the **Reporting** tab in the RCA Console. Go to **RCA Management** > **Live Network** > **Acquisition History**.
- Click the **Reporting** tab in the RCA Console. For vulnerability, compliance, or security tools content update status, go to one of the following respectively:
  - **Vulnerability Management** > **Vulnerability Reports** > **Acquisition Details**
  - **Compliance Management** > **SCAP Reports** > **Acquisition Details**
  - **Security Tools Management** > **Product Reports** > **All Products** > **Acquisition Details**

Note: If the configuration information related to HP Live Network is incomplete or incorrect, the update will fail. This will be reflected in both the report and the log file:

<InstallDir>`\VulnerabilityServer\logs\vms-server.log`

There will be no other indication in the RCA Console that the update has failed, however.

Database Maintenance

The Database Maintenance area shows all of the devices that have reporting data stored in RCA. Use the Maintenance toolbar to clean up reporting data for devices that may no longer be in your database.

To remove device reporting data:

1. In the Maintenance area, select the devices for which you would like to remove reporting data.
2. Click the Delete Reporting Data button.
3. The reporting data is removed from your database.
   After reporting data is removed for a device, the data is not available when generating any reports.

Note: If you are deleting reporting data for an actively managed device, to avoid reporting data discrepancies, you should remove then re-deploy the Management Agent on that device.

Software Management

Use the Software Management tools on the Operations tab to manage the catalog of software services (applications) that are available to be deployed to managed client devices. After a software service is added to the HPCA software library, end-users of the client devices can install, update, or remove software to which they are entitled by "Configuring the Application Self-Service Manager" on page 403.

The Software Library page lists the software services that have been published into RCA. You can use the tools on this page to import or export software services. The import and export tools are useful for moving a software service from one RCA server to another—for example, if you want to move a service from a test environment to a production environment

Note: To view or modify settings for a particular software service, see the "Software Details

Window (Operations Tab)" on page 228.

Software Library Tools

Button	Description
	**Refresh Data** – Refreshes the data in the Software Library table.
	**Export to CSV** – Creates a comma-separated list of software services that you can open, view, and save.
	**Import Service** – Imports a software service into RCA. See "Import a Software Service" below. After you import a software service, you can entitle groups or specific managed client devices to that service. You can then deploy the service to those devices.
	**Export Service** – Exports a published software service in a binary file format called a **service deck**. See "Export a Software Service" below. After you export a software service, you can copy the service deck to another RCA server, and then import the service there.

Import a Software Service

RCA can import software services into the Software Library. To import a service, the service import deck must be located in the `ServiceDecks` directory on your RCA server. By default, this directory is:

<InstallDir>`\Data\ServiceDecks`

This is useful if you have created a testing environment. When you have approved a particular service in your test environment, export that service to the `ServiceDecks` directory on your production RCA server (see "Export a Software Service" below). Then use the Import Service wizard to import that service to your production Software Library, and deploy it to managed devices.

To import a service:

1. Click **Import Service**  to launch the "Service Import Wizard" on page 348.
2. Follow the steps in the wizard to import the service into the Software Library.

Note: Only those services in the `ServiceDecks` folder that contain the word SOFTWARE in their names are available for import. For example:

PRIMARY.SOFTWARE.ZSERVICE.ORCA

Export a Software Service

Published software services can be exported to the `ServiceDecks` directory on your RCA server. By default, this directory is:

<InstallDir>`\Data\ServiceDecks`

Exported services can be copied to any other RCA server and then imported into that server's Software Library (see "Import a Software Service" on previous page).

To export a service:

1. Select the check box in the first column to select the software to export as a service.
2. Click **Export Service** to launch the "Service Export Wizard" on page 348.
3. Follow the steps in the wizard to export the service to the ServiceDecks directory on your RCA server machine.

Software Details Window (Operations Tab)

Click the Service ID of any software service in the Software Library to open the Software Details window. Use the Software Details window to view or modify settings for a particular software service.

The following settings are available in the Software Details window:

- **Display Name**
  Name of this software service. This is the "friendly" name that is used in the RCA console. This is a required field.
- **Software Category**
  Specify a category that will help define the type of software. The Software Category is displayed in the Software Library and is available as a sort option.
- **Catalog Visibility**
  Specify whether to display the software in the catalog on the managed client device. Displaying software in the catalog allows the end user to install, update, or remove the software.
- **Reboot Settings**
  Specify whether a reboot is required for the managed client device after the software is installed, and whether to prompt the end-user for the reboot.
- **Author**
  The software author (for example, Hewlett-Packard).
- **Vendor**
  The software vendor (for example, Hewlett-Packard).
- **Web Site**
  An informational URL for the software.
- **Pre-uninstall Command Line**
  Command to run before software is removed from a device. For example, some registry keys may need to be removed before running the software removal command.
- **Install Command Line**
  Command to run to install the software.
- **Un-install Command Line**
  Command to run after the software is removed from a device.

Note: Be sure to click **Save** after making any changes to the software settings.

Out of Band Management

Out of Band (OOB) Management is enabled using the Configuration tab. See "Configuration" on page 253 for OOB Management settings and Preferences.

For additional information on using OOB Management, see the *Radia Client Automation Enterprise Out of Band Management User Guide.*

The following sections describe the OOB Management tasks available in the console:

Provisioning and Configuration Information

Your vPro and DASH devices must be provisioned before you can discover and manage them. It is possible to provision vPro devices through the RCA console if the devices did not automatically become provisioned when originally connected to the network.

The provisioning of vPro devices through the RCA console is described in Setting Up vPro and DASH Devices chapter of the *Radia Client Automation Enterprise Out of Band Management User Guide*. This option does not appear on the Operations tab under Out of Band Management if you have selected to manage DASH devices only since it is not relevant for this type of device.

See the Setting Up vPro and DASH Devices chapter of the *Radia Client Automation Enterprise Out of Band Management User Guide* for complete details.

DASH Configuration Documentation

Provision DASH-enabled devices according to the documentation accompanying the device. For DASH-enabled devices from Hewlett-Packard, DASH configuration information is documented in the "Broadcom NetXtreme Gigabit Ethernet Plus NIC" whitepaper.

To access this documentation:

1. Go to www.hp.com.
2. Select **Support and Drivers** > **Product Support and Troubleshooting**.
3. Type a product that supports this NIC, for example, the dc7900.
4. Select one of the dc7900 models.
5. Select **Manuals (guides, supplements, addendums, etc)**.
6. Scroll to the White papers section and select **Broadcom NetXtreme Gigabit Ethernet Plus NIC** whitepaper.

DASH Configuration Utilities

The DASH Configuration Utility (BMCC application) is part of the Broadcom NetXtreme Gigabit Ethernet Plus NIC driver softpaq, which is found in the drivers section for each product that supports this NIC.

To access this utility:

1. Go to www.hp.com.
2. Select **Support and Drivers** > **Drivers and Software**.
3. Type a product that supports this NIC, for example, the dc7900.
4. Select one of the dc7900 models.
5. Select an operating system.
6. Scroll to the Driver-Network section and select to download the **Broadcom NetXtreme Gigabit Ethernet Plus NIC Drivers**.

Device Management

The Device Management area allows you to manage multiple OOB devices.

On the Operations tab, under Out of Band Management, click **Device Management**. The Device Management window opens. Using the icons on the toolbar of the device table, you can perform the following tasks on multiple devices:

- Refresh data
- Reload device information
- Discover Devices
- Power on and off and reboot devices
- Subscribe to vPro alerts
- Manage common utilities on vPro devices
- Deploy System Defense policies to selected vPro devices
- Deploy heuristics worm containment information to selected vPro devices
- Deploy agent watchdogs to selected vPro devices
- Deploy agent software list and system message to selected vPro devices

Click the hostname link in the device table to manage an individual OOB device. A management window opens that has several options in its left navigation pane. The options available are dependent on the type of device you selected to manage.

See the Device Management chapter of the *Radia Client Automation Enterprise Out of Band Management User Guide* for complete details.

Groups Management

The Groups Management option allows you to manage groups of vPro devices as defined in the Client Automation software. You can perform OOB operations on Client Automation groups that contain vPro devices. You can manage groups of vPro devices to perform various discover, heal, and protect tasks. These include power management, alert subscription, and deployment of System Defense policies, agent watchdogs, local agent software lists, and heuristics.

On the **Operations** tab, under Out of Band Management, click **Group Management**. The Group Management window opens. From the icons on the toolbar of the group table, you can perform the following tasks on multiple groups:

- Refresh data
- Reload group information
- Power on and off and reboot groups
- Subscribe to vPro alerts
- Deploy agent software list and system message to selected vPro groups
- Provision vPro device groups
- Deploy and undeploy System Defense policies to selected vPro devices
- Deploy and undeploy agent watchdogs to selected vPro groups
- Deploy and undeploy heuristics worm containment information to selected vPro groups

To drill down to manage individual devices within a group, click the group name link under the Description column of the table. The Device Management window opens displaying a list of devices belonging to the selected group. You can manage multiple or individual devices within the group. See Managing Devices.

See the Group Management chapter of the *Radia Client Automation Enterprise Out of Band Management User Guide* for complete details.

Alert Notifications

For vPro devices, you can view the alerts generated by provisioned vPro devices if you have an alert subscription to the device. Monitoring alert notifications gives you a good idea of the health of the devices on your network.

See the Alert Notifications chapter of the *Radia Client Automation Enterprise Out of Band Management User Guide* for complete details.

Patch Management

Use the Patch Management tools on the Operations tab to manage the catalog of patch bulletins that are available to be deployed to managed devices.

Patch Library Operations

The Patch Library page lists the bulletins that have been published into RCA. You can use the tools on this page to import or export bulletins. The import and export tools are useful for moving a patch from one RCA server to another—for example, if you want to move a patch from a test environment to a production environment.

Note: To view or modify settings for a particular patch, see the "Patch Details Window (Operations Tab)" on page 234.

Patch Library Tools

Button	Description
	**Refresh Data** – Refreshes the data in the Patch Library table.
	**Export to CSV** – Creates a comma-separated list of patches that you can open, view, and save.
	**Import Service** – Imports a patch into RCA. See "Import a Patch Service" below. After you import a patch, you can entitle groups or specific managed client devices to that service. You can then deploy the patch to those devices.
	**Export Service** – Exports a published patch in a binary file format called a **service deck**. See "Export a Patch Service" on next page. After you export a patch, you can copy the service deck to another RCA server, and then import the patch there.

Import a Patch Service

RCA can import patches into the Patch Library. To import a patch, the decks (namely, the `xpi`, `xpc`, and `xpr` files) and the `zip` file must be placed in the `ServiceDecks` directory on your RCA server. Also, copy the `PRIMARY.PATCHMGR.ZSERVICE.DISCOVER_PATCH.*` files. These contain the catalog and the Agent information. If these files are not copied, or if they are old files, the import of bulletins will fail with the message - "Import Failed - Ensure the bulletin is exported recently and latest `PRIMARY.PATCHMGR.ZSERVICE.DISCOVER_PATCH.*` files are copied."

By default, this directory is:

<InstallDir>`\Data\ServiceDecks`

This is useful if you have created a testing environment. When you have approved a particular patch in your test environment, export that bulletin to the ServiceDecks directory on your production RCA server (see "Export a Patch Service" on next page). Then use the Import Service wizard to import that patch to your production Patch Library, and deploy it to managed devices.

To import a patch service:

1. Click **Import Service**  to launch the "Service Import Wizard" on page 348. This displays a list of the `xpi` files present in the `ServiceDecks` directory.
2. Follow the steps in the wizard to import the service into the Patch Library.

Note: PRIMARY.PATCHMGR.ZSERVICE.DISCOVER_PATCH.xpi need not be explicitly selected. They are implicitly selected when a bulletin is selected for import. If only the agent or catalog files need to be moved to the target server, then PRIMARY.PATCHMGR.ZSERVICE.DISCOVER_PATCH.xpi can be selected.

Export a Patch Service

Published bulletins can be exported to the ServiceDecks directory on your RCA server. By default, this directory is:

<InstallDir>\Data\ServiceDecks

To export a patch service:

1. Select the check box in the first column to select the bulletin(s) to export as a service. Use the grid options to search for bulletins based on type, name, and so on.
2. Click **Export Service** to launch the "Service Export Wizard" on page 348.
3. Follow the steps in the wizard to export the bulletin(s) to the ServiceDecks directory on your RCA server machine.
   This creates the following files for each exported bulletin in the ServiceDecks directory of your server:
   - PRIMARY.PATCHMGR.ZSERVICE.[BULLETIN NAME].xpi
   - PRIMARY.PATCHMGR.ZSERVICE.[BULLETIN NAME].xpr
   - PRIMARY.PATCHMGR.ZSERVICE.[BULLETIN NAME].xpc
   - PRIMARY.PATCHMGR.ZSERVICE.[BULLETIN NAME].zip
   - PRIMARY.PATCHMGR.ZSERVICE.DISCOVER_PATCH.xpi
   - PRIMARY.PATCHMGR.ZSERVICE.DISCOVER_PATCH.xpr
   - PRIMARY.PATCHMGR.ZSERVICE.DISCOVER_PATCH.xpc
   - PRIMARY.PATCHMGR.ZSERVICE.DISCOVER_PATCH.zip

   For the metadata-based patch distribution model, the zip file contains the binaries that are present in the gateway cache and some of the metadata information. These binaries are also moved to the target server during the export/import operation. The Agent and Catalog information are present in the PRIMARY.PATCHMGR.ZSERVICE.DISCOVER_PATCH.* files. These files also need to be moved explicitly to the target machine. For Redhat bulletins, the data of the dependant bulletins are present in the zip file.

   Exporting a service automatically exports the latest agent, catalogs, and other related files that are needed for the discover process.

   For import, all of the files with the PRIMARY.PATCHMGR.ZSERVICE.*[BULLETIN NAME]* stem along with PRIMARY.PATCHMGR.ZSERVICE.DISCOVER_PATCH.* should be copied to any other RCA server and then imported into that server's Patch Library. See "Import a Patch Service" on previous page.

Patch Details Window (Operations Tab)

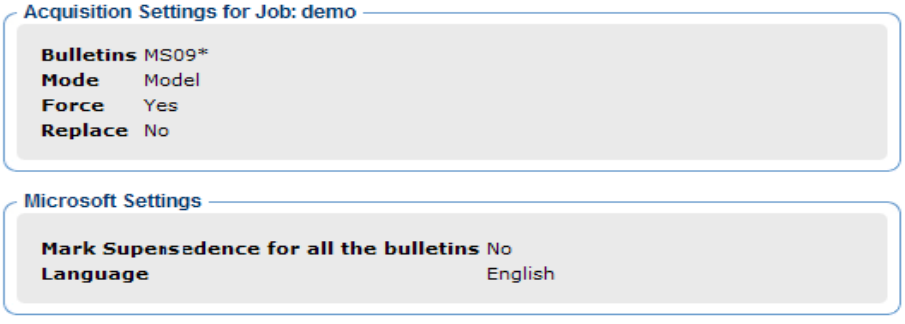
Click the Bulletin name for any patch in the Patch Library to open the Patch Details window. Use the Patch Details window to view the following properties of a particular patch:

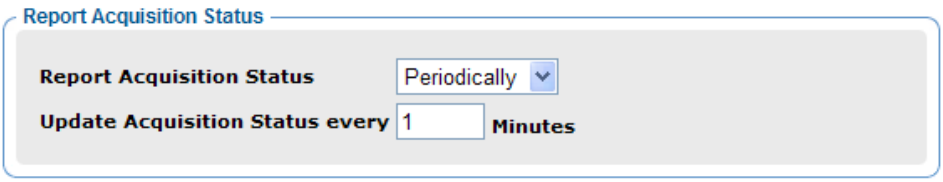
- **Bulletin Type**
  Type of patch (for example, Security Updates).
- **Vendor**
  The software vendor (for example, Microsoft).
- **Bulletin**
  Bulletin name assigned by the vendor. Typically a sequential code.
- **Description**
  Any descriptive text that the vendor has included with the bulletin.
- **Vendor Posted**
  Date this bulletin was originally posted by the vendor.
- **Vendor Revised**
  Most recent date that this bulletin was revised by the vendor.
- **Bulletin Information**
  URL for information about this bulletin on the vendor's web site.
- **Other Information**
  URL for any related information on the vendor' web site.

Note: The information displayed in this window is read-only and cannot be modified.

Start Acquisition

1. From Operations, expand **Patch Management** and click **Start Acquisition.**
2. Select a file by clicking on its name.
3. Confirm the settings for this acquisition.





- **Report Acquisition Status**: In addition to the acquisition log, you can specify how frequently you want to update the current acquisition status that is displayed when you View Acquisition Jobs.
- **Update Status Information every**: If you specified **Periodically** in the Report Acquisition Status field, select how frequently you want to update the status file.

4. Read the notice on your agent update settings, and click **Submit** to begin your acquisition.

To check the status of the acquisitions:

- Use the Reporting tab to look at the Patch Acquisition Reports.
- Use the Operations tab, Patch Management area to **View Acquisition Jobs.**

Perform Synchronization

The patch information that has been sent to the RCA Configuration Server DB must be synchronized with the Patch SQL database for assessment and analysis. The RCA Configuration Server DB and the Patch SQL database house identical information for the set of classes and instances that are synchronized.

- Each class in the PATCHMGR Domain becomes a table in the Patch SQL database. The corresponding table is named nvd_classname.
- Each attribute in each class becomes a column in its table. The corresponding column name is nvd_attributename. Expressions and connection variables are not replicated.
- Each instance in the class becomes a record in the corresponding table.

This synchronization occurs automatically after a patch acquisition and in normal RCA operations.

However, there may be times when you need to run the synchronization manually. For example, synchronize the databases manually after an import of patch information from a different RCA server. Also, synchronize the databases manually if you switch the SQL database configured for Patch Management after some acquisitions have taken place.

You can synchronize the databases manually using the RCA Core Console.

To synchronize the databases:

1. From Operations tab, expand the **Patch Management** tasks, and click **Perform Synchronization**.
2. Click **Submit**.

Agent Updates

When you run a patch acquisition, you can also download the latest Version and updates to the Patch Agent files. The Patch Agent files include the scripts to perform product discovery and

management. These files are received from the Patch Update web site provided by HP. After download, the files are published to the PATCHMGR Domain and connected to the DISCOVER_ PATCH Service instance.

Use the Agent Updates task to determine the status of updates.

To view the Agent Updates, from the Console **Operations** tab, select **Patch Management** > **Agent Updates**.

Agent files are distributed when the DISCOVER_PATCH Service is processed on the Patch Manager target device. This is accomplished through a connection in the DISCOVER_PATCH Service to the PATCH Instance in the AUTOPKG Class. In turn, the AUTOPKG.PATCH Instance connects to the agent maintenance packages created when you selected **Publish** or **Publish and Distribute**. If you have selected to publish only (not to distribute), you will need to create connections from the appropriate instance in the PACKAGE Class to the AUTOPKG.PATCH Instance. Use the Admin CSDB Editor to do this. An example is shown below.

Create connections to the published package

Note: AIX, HP-UX and Solaris are not currently supported.

Agent Updates has the following values:

- **None**: The agent updates will not be published to the PATCHMGR Domain.
- **Publish, Distribute**: This is the default value. Publish the updates to the PATCHMGR Domain and connect them to the DISCOVER_PATCH Instance to distribute the updates to your Patch Manager-managed devices.
- **Publish**: The updates will be published to the PATCHMGR Domain, but will not be connected for distribution to Patch Manager-managed devices. You will need to create these connections.

There are two parameters that control which agent updates you download.

- **Operating System**: Specify which operating systems to acquire the agent updates for. The default is to download all operating systems. Valid values are **Windows** and **Linux**.
- **Version**: Select the Patch Manager version for which you would like to acquire the agent updates. You can publish only one version to a Configuration Server; one Configuration Server cannot host multiple versions of the agent. If piloting, create a separate Configuration Server for the other version.

  Caution: Never choose an agent version that is lower than the version of Patch Manager that is first installed or currently implemented in your enterprise.

  To update to the current version, specify **Version 9**.

  Migrating customers are advised to set the **Publish and Distribute** option and set the Agent Updates Version to **Version 9**. This ensures the successful migration of Windows and Linux Patch Agents to Version 9.

  Note that when patches are acquired from Microsoft Update, the Source column in the report will show “Microsoft Update” instead of “Microsoft.”

Caution: To accommodate Microsoft Update technologies, your target devices must have the Windows Update Agent installed. The Patch Manager acquisition process automatically acquires the latest Windows Update Agent required to perform vulnerability scans and patching when leveraging Microsoft Update Catalog technologies. The DISCOVER_ PATCH Service will automatically apply the current Windows Update Agent to the managed device on the next agent connection.

Note: Windows Update Agent (**WUA**) uses the Automatic Updates Windows service, which must be set to either **Automatic** or **Manual** on target devices. The Automatic Updates service can be in a stopped state because WUA will start it as needed.

Acquisition History

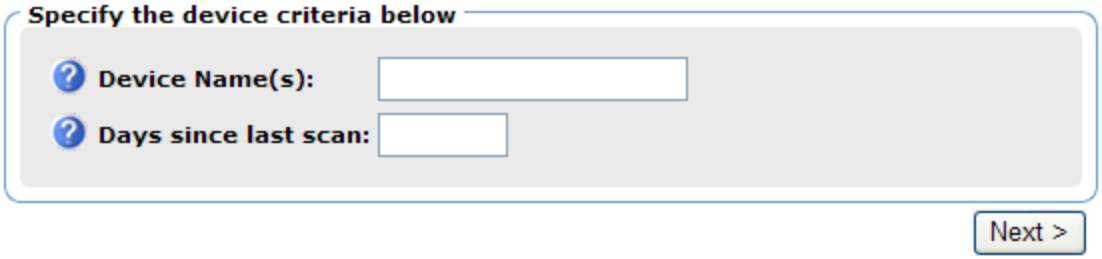
Select a patch acquisition status page to view details from previous acquisitions.

Delete Devices

You can delete Patch Manager compliance data for specific devices using the Operations tab of the console.

To remove compliance data from the Patch Manager ODBC database:

1. Click the **Operations** tab and expand the **Patch Management** tasks.
2. Click **Delete Devices**.



3. Specify device-selection criteria for the devices to remove. You may:
   - Specify a single device or multiple devices in a comma-separated list.
   - Use wildcards.
   - Specify the number of days since the last vulnerability scan was performed on the device. This may be used to remove compliance information for devices who are no longer reporting compliance data to the Patch Manager Infrastructure components.
4. Click **Next**. The console allows you to preview the devices that match the selection filters before removing them from the database.
5. Click **Delete** to remove the devices from the Patch Manager ODBC database.

Caution: Take care when removing devices from this database; this operation cannot be undone.

Gateway Settings

The Patch Manager Gateway is used to obtain and cache the patch binary files when the **Patch Metadata Download** option is enabled on the **Patch Management > Distribution Settings** page. The Patch Metadata Download option is only available when patching Microsoft devices using Microsoft Update Catalog data feed.

The **Patch Management** > **Gateway Settings** area of the Operations tab allows you to review and manage the cache of patch files stored on the Gateway.

Note: The Patch Gateway operations described in the following sections are available on the Core server only, not the Satellite server.

Preload Gateway Cache option

- If the Preload Gateway Cache option is turned off, the Gateway caches the patch files as they are requested by Agents.
- If the Preload Gateway Cache option is turned on, the Gateway caches the patch files when the patches are acquired. This is the default setting.

The following Gateway Operations are available from the area of the Console:

- "Cache Statistics" below
- "Cache Content Details" on next page
- "Export URL Requests" on next page
- "Import URL Requests" on page 240

Cache Statistics

Use the Cache Statistics page to see statistics on the patch files currently cached on the Gateway, as well as hit, miss and error information that lets you gauge how well the Gateway is satisfying the patch requests of the Agents. The counters for the hit, miss and error information can be reset.

To access the Cache Statistics page:

1. From the Console **Operations** tab
2. Select **Patch Management** > **Gateway Settings** > **Cache Statistics**.

Gateway Cache Statistics

- **Total cache size**: Total size in megabytes of all patches in the Gateway cache.
  When the cache size exceeds the Maximum Cache Size configured for the Patch Gateway Operations on the Patch Distribution Settings page, the patches that are older and least used will be deleted.
- **Number of files**: The number of active files in the patch gateway cache available for download.
- **Cache Hits**: The number of requests that have been fulfilled since the last counter reset.

- **Cache Misses**: The number of requests that required a download from the Vendor since the last counter reset.
- **Cache Download Errors**: The number of download errors the gateway encountered since last counter reset. The error can be found in the `HPCA-PATCH-3467.log` file.
- **Hit Ratio**: The ratio between requests fulfilled from cache, and the total number of requests.
- **Cache Counter Reset On**: The date and time when the cache counter statistics were reset.
- **Reset Cache Counter Statistics**: Click this entry to reset the counters for cache hits, misses and download errors.

Cache Content Details

Use the Cache Content Details page to view the current set of patch binary files cached on the Gateway, by Bulletin number.

To access the Cache Content Details page:

1. Select **Operations** tab from the Console
2. Select **Patch Management** > **Gateway Settings** > **Cache Content Details**.

Gateway Cache Content Details

The Cache Content Details page displays the cached bulletins by number. Click on a Bulletin Number to see the list of binaries cached for that bulletin. Double-click a binary file to see more details.

Export URL Requests

If the Gateway Server cannot connect to the Vendor download site, the unfulfilled agent request files can be exported and then imported into another Gateway Server with internet connectivity.

The Export URL Requests operation allows you to see and filter the list of unfulfilled URL requests and import the list into another Patch Gateway Server.

When you export the URL, you are prompted to save the contents as an XML file with a name of your choice. The XML file contains the patch URLs selected during the export.

To access the Export URL Requests page:

1. Select **Operations** tab from the Console
2. Select **Patch Management** > **Gateway Settings** > **Export URL Requests**.

To export a list of unfulfilled URL requests:

- Use the **List Display Settings** area to filter the unfulfilled list into the ones you want to export.

Note: The Export URL Request will only list the URL requests made when the INTERNET option is set to N in patch.cfg. Export URL Request is meant only for an environment where the Internet is not made available to the server hosting the primary Patch Gateway. The Export

URL Request list (of unfulfilled URLs) that is created a Gateway without internet access can be downloaded after using Import URL Requests on another Gateway server that has Internet connectivity. Later the downloaded files can be copied back to the gateway folder on the primary Patch Gateway server.

List Display Settings

Type a **URL Filter Expression** to filter the list of all unfulfilled patch requests by URL name. Wildcards are accepted. Click **Apply** to apply the filter.

Use the **Page Count** drop-down to set the required number of URL listings to include on a single page.

To return to the full list of URLs, reset the entry to * and click **Apply**.

Requested URLs

The Requested URLs area enables you to view the following details for unfulfilled URL request by an agent:

- The URL column displays the unfulfilled URL requests.
- The Hits column displays the number of times the URL was requested.
- The Date column displays the date when the URL was last requested.

Gateway URL Request Export

The Gateway URL Request Export enables you to view the number of unique unfulfilled URLs requested since the last data export.

If there are unfulfilled URL Requests listed on this page, click **Submit** to download an export file of these current unfulfilled requests.

Import URL Requests

The URLs exported from the Export URL Request operation can be imported into a different Patch Gateway Server using the Import URL Requests page. After the import URLs request process is complete, the binaries downloaded from the vendor site are stored in the Patch Gateway Server. These files should be copied to the Patch Gateway Server from where the URLs were exported. By default, the binaries are stored in the following location:

<InstallDir>`\Data\PatchManager\patch\gateway\dbver0`

To access the Import URL Requests page:

- Select **Operations** tab from the Console.
- Select **Patch Management** > **Gateway Settings** > **Import URL Requests**

To import URL requests:

1. Copy the file saved after using the Export URL Requests task to the local drive of the gateway where you want to import the URL requests.
2. In the **Request file to import** area, click **Browse** to locate the XML file that was saved from the Export URL Requests tasks.
3. Click **Submit** to start importing the unfulfilled requests in the specified file
4. The Gateway URL Request Import page displays the URLs being imported, their completion status, and the % completion.

OS Management

Use the OS Management tools on the Operations tab to manage the catalog of operating systems that are available to be deployed to managed devices.

The OS Library page lists the operating systems that have been published into RCA. You can use the tools on this page to import or export operating systems. You can also create a deployable CD (or DVD) for any operating system in the library.

The import and export tools are useful for moving an operating system from one RCA server to another—for example, if you want to transfer an OS from a test environment to a production environment.

Note: To view or modify settings for a particular operating system, see the "OS Details Window (Operations Tab)" on page 243.

OS Library Tools

Button	Description
	**Refresh Data** – Refreshes the data in the OS Library table.
	**Export to CSV** – Creates a comma-separated list of operating systems that you can open, view, and save.
	**Import Service** – Imports an operating system into RCA. See "Import an OS Service" below. After you import an operating system, you can entitle groups or specific managed client devices to that OS. You can then deploy the OS to those devices.
	**Export Service** – Exports a published operating system in a binary file format called a **service deck**. See "Export an OS Service" on next page. After you export an operating system, you can copy the service deck to another RCA server, and then import the OS there.
	**Create CD Deployment Media** – Downloads OS images that you can then burn to a DVD for operating system deployment. See "Create Deployment Media" on next page.

Import an OS Service

RCA can import operating systems into the OS Library. To import a service, the service import deck must be located in the `ServiceDecks` directory on your RCA server. By default, this

directory is:

<InstallDir>\Data\ServiceDecks

This is useful if you have created a testing environment. When you have approved a particular service in your test environment, export that service to the ServiceDecks directory on your production RCA server (see "Export an OS Service" below). Then use the Import Service wizard to import that service to your production OS Library, and deploy it to managed devices.

To import a service:

1. Click **Import Service** to launch the "Service Import Wizard" on page 348.
2. Follow the steps in the wizard to import the service into the OS Library.

Note: Only those services in the ServiceDecks folder that contain the word OS in their names are available for import. For example:

PRIMARY.OS.ZSERVICE.WIN732

Export an OS Service

Published operating systems can be exported to the ServiceDecks directory on your RCA server. By default, this directory is:

<InstallDir>\Data\ServiceDecks

Exported services can be copied to any other RCA server and then imported into that server's OS Library (see "Export an OS Service" above).

To export a service:

1. Select the check box in the first column to select the OS to export as a service.
2. Click **Export Service** to launch the "Service Export Wizard" on page 348.
3. Follow the steps in the wizard to export the service to the ServiceDecks directory on your RCA server machine.

Create Deployment Media

You can use the Create CD Deployment Media tool to download images that can then be burned to a DVD for operating system deployment.

The OS Library lists all operating systems that have been published to RCA.

To download an operating system image for DVD deployment:

1. On the Operations tab, go to **OS Management** > **OS Library**.
2. Select an operating system from the OS Library.
3. Click the **Create CD Deployment Media** button to launch the CD Deployment Wizard.
4. Review the summary information, and click **Download**. The OS image begins to download in the background.
5. Click **Close**.

View the download progress in the OS Library. Click the **Refresh** button to see the current status in the CD Creation Status column.

When the download is complete, the OS image is stored, by default, in:

<InstallDir>`\Data\ServiceDecks\CDDeployment`

If this directory is empty, the CD Creation Status column is blank for all operating systems listed.

Note: This feature is intended for use with DVDs, typically to store multiple images. Do not span your resources over multiple CD-ROMs or DVD-ROMs.

Caution: Your DVD-ROM must be in Joliet format.

OS Details Window (Operations Tab)

Click the Service ID of any operating system in the OS Library to open the OS Details window. Use the OS Details window to view or modify settings for a particular operating system.

The following settings are available in the OS Details window:

- **Display Name**
  The name of the OS that appears on the OS Library page. This is a required field.
- **Author**
  The OS author.
- **Vendor**
  The OS vendor.
- **Web Site**
  An informational URL for the OS.

Note: Be sure to click **Save** after making any changes to the OS settings.

Usage Management

Use the Usage Management section to configure usage collection filters.

See the *Radia Client Automation Enterprise Application Usage Manager Reference Guide* for more information about collecting and analyzing usage data and handling of renamed devices using RCA.

Collection Filters

Use the Collection Filters page to create and manage usage collection filters.

Usage collection filters determine what usage data is made available by the Usage Collection Agent for reporting. When the Usage Collection Agent is deployed to a device, all usage data for all applications is collected and stored locally. The usage filters that you create and enable determine which local usage data is then sent to RCA.

If a filter is enabled after a Usage Collection Agent has already been deployed, all of the usage data defined by the filter that was collected and stored locally is then sent to RCA for reporting.

For example, if the Usage Collection Agent is deployed in May, and a filter is enabled for Microsoft Word, all usage data for Microsoft Word is sent to RCA based on the schedule that you defined. Then, in June you decide to create and enable a new filter for Microsoft Excel. The next time that usage data is sent to RCA, it will include all Excel usage data that was collected and stored locally from the date the Usage Collection Agent was first installed in May until the current date in June. Usage will continue to be sent thereafter for both applications.

Usage data is stored locally on managed devices for 12 months.

For usage collection filter configuration instructions, see:

- "Configuring Usage Collection Filters" below
- "Defining Usage Criteria" on next page

See "Deploying the Usage Collection Agent" on page 176 to deploy the Usage Collection Agent and define a collection schedule.

Configuring Usage Collection Filters

RCA contains pre-configured collection filters by default. You can use these filters as models for creating new filters, or you can modify these filters to suit your needs.

Use the "Usage Collection Filter Creation Wizard" on page 349 to create new usage collection filters. Use the Filter Details window to modify existing filters.

Caution: Configuring filters to collect usage data based on wildcard characters can cause the collection of a large amount of data that can, over time, create severe reporting performance issues as the database grows in size. It strongly recommends that you create filters to collect data only for those applications that you want usage information for. Avoid collecting usage data for all applications.

To create a collection filter:

1. On the Collection Filters page, click the **Create New Filter** toolbar button. This launches the "Usage Collection Filter Creation Wizard" on page 349.
2. Follow the steps in the wizard to create and enable the new collection filter.

To enable collection filters:

1. In the Filter list, select the filters that you want to enable by clicking the box to the left of the filter description.
2. Click the **Enable Selected Items** toolbar button.
3. Click **OK** to enable the selected filters. A status dialog shows you the result.
4. Click **Close** to close the status dialog.

To modify an existing filter:

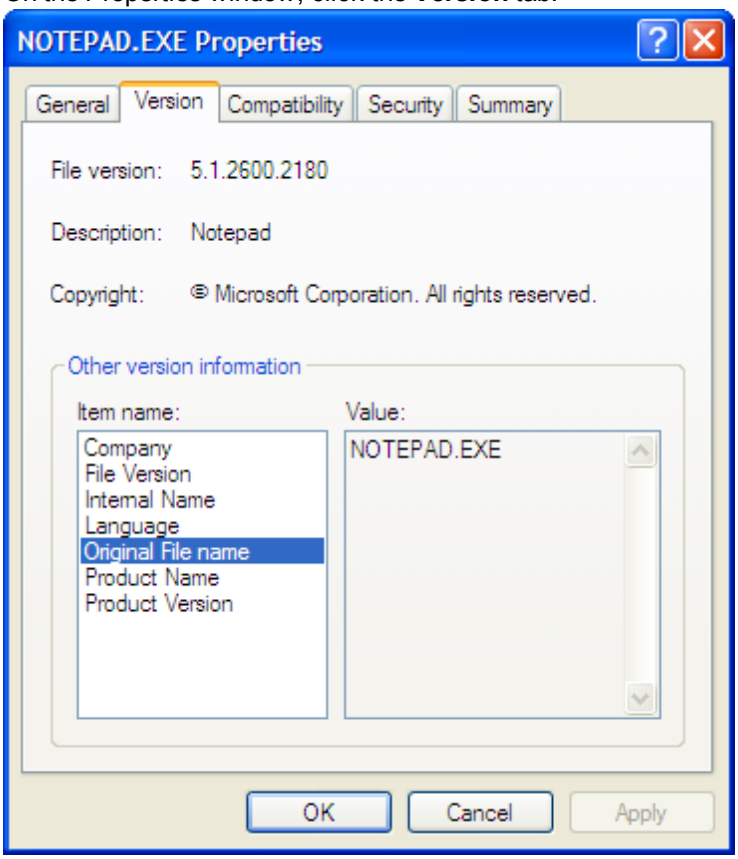
1. In the Filter list, click the filter description link to open the Filter Details window.
2. In the Filter Criteria area, type the specific filter criteria to use when collecting usage data. See "Defining Usage Criteria" below for help in determining what criteria to select.
3. Click **Save**.

Defining Usage Criteria

The Usage Collection Agent uses the file header information within each local executable file to determine whether that application meets defined filter criteria. You can use the file header information to determine what criteria to use when defining a filter.

To determine file header information:

1. Right-click an executable file on your system.
2. Select **Properties** from the shortcut menu.
3. On the Properties window, click the **Version** tab.



The information contained in the **Item name** and **Value** boxes is used by the Usage Collection Agent to filter the available usage data (with the exception of the Language and Internal Name items, which are not currently supported).

Note: Be aware that not all executable files support or correctly populate values stored in the file header.

The following example describes how to create a filter to search for a specific application.

To filter usage data for notepad.exe:

1. Create a new Usage Filter by launching the "Usage Collection Filter Creation Wizard" on page 349.
2. At the Properties step, define the following filter criteria:
   - **Description**: `Notepad`
   - **Enabled**: `Yes`
   - **File/Application Name**: `notepad.exe`
3. Deploy the Usage Collection Agent to one or more managed devices. See "Deploying the Usage Collection Agent" on page 176 for instructions.
   Usage data will be sent to RCA weekly and will include all usage data for Notepad for all devices that have the Usage Collection Agent installed.

Settings Management

Use the Settings Management section to create, modify, and delete settings profiles. Settings profiles allow you to create groups of configuration settings for software installed on the managed devices in your environment. A 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 targeted products.

Once you create and/or modify settings profiles, they can be deployed to the targeted systems where the relevant software is installed. In RCA Enterprise, Settings Profiles are listed as services and can be deployed to targeted machines through policy entitlement, similar to the deployment of other services.

Once settings profiles have been created and deployed, it is possible to see summary reports about the software giving administrators visibility to the run-time data of this software. See "Settings Management Reports" on page 209.

This section covers the following topics:

Settings Templates

Settings templates are used to create instances of settings profiles. You can download the most current content for settings templates from the HP Live Network site. See "Accessing HP Live Network Content" on page 127.

You can select any of the provided settings templates to create additional profiles or to modify existing ones. The Operations tab in the RCA Console provides a **Settings Templates** area under

Settings Management that allows you to see the software on your system that has configurable profiles.

Creating New Profiles

You can create additional profiles for the software on your system with configurable profiles. Settings templates are provided for this purpose. The template is used to create a settings profile instance for the relevant software. You can start with a blank profile or you can clone an existing one if it is similar to the one you want to create, thus making the procedure easier to perform.

To create a new settings profile:

1. On the Operations tab, expand Settings Management in the left navigation pane and click the **Settings Templates** link. Software with configurable profiles will be displayed in the content area on the right.
2. In the **DisplayName** column, click the name of the software for which you want to create a new profile. A window opens that contains the following tabs:
   - **Profiles:** Displays the existing profiles for the selected software. On this tab, you can create, view, modify, and delete settings profiles. Profile names displayed with angle brackets (< >) surrounding them are HP-supplied profiles.

     Note: Be aware that if you modify these profiles, your changes can be lost the next time you update your settings content from the HP Live Network site.
   - **Details:** Displays information about what the template does and how to use it.
3. On the Profiles tab, click **Create a New Profile** on the toolbar in the Settings Profiles table. The Settings Profile Creation Wizard opens.
   Alternatively, you can check the box next to an existing profile that you want to copy and click **Copy the Selected Profile**. The Copy and Modify Settings Profile Wizard opens in this case. This wizard allows you to clone the selected existing profile. If you select to copy an existing profile, all fields, except for the profile Display Name, will be populated with the values contained in the selected existing profile.
4. In either wizard, specify the following information:
   - **Display Name**: Type a name for the profile
   - **Description**: Type a description for the profile
5. Click **Next**. The next page of the wizard opens which allows you to type properties specific to the particular software. In the case of copy, these fields will be pre-populated. Modify these fields as necessary.
6. See the documentation for the given software to better understand the relevant property settings.
7. Click **Create** or **Copy** depending on the wizard. The newly created profile is listed in the Settings Profiles table on the Profiles tab. The number of profiles in the Operations area is also updated to reflect the latest addition.

Modifying Existing Profiles

Property settings for software with configurable profiles can be viewed and modified.

To modify a settings profile:

1. On the Operations tab, expand Settings Management in the left navigation pane and click the **Settings Templates** link. Software with configurable profiles will be displayed in the content area on the right.
2. In the **Display Name** column, click the name of the software that has a profile that you want to modify. A window opens displaying the existing profiles for the selected software on the Profiles tab.
3. On the Profiles tab in the **Display Name** column, click the name of the profile that you want to modify. A window opens with Summary and Properties tabs displaying all of the properties for the selected profile.
4. Modify the property values on both tabs as necessary.
5. Click **Save** to save your changes.

Deleting Profiles

Settings profiles can be deleted for software when they are no longer needed.

To delete a settings profile:

1. On the Operations tab, expand Settings Management in the left navigation pane and click the **Settings Templates** link. Software with configurable profiles will be displayed in the content area on the right.
2. In the **Display Name** column, click the name of the software that has a profile that you want to delete. A window opens displaying the existing profiles for the selected software on the Profiles tab.
3. On the Profiles tab, check the box next to the profile name(s) that you want to delete.
4. Click **Delete Selected Profile(s)** on the toolbar. A pop-up confirmation window opens.
   If the selected profiles are entitled in any external policy directories, you must manually remove these entitlements before continuing. Otherwise, you may get an agent connection failure (reported as error code 650).
5. Click **Yes** if you want to continue. A window opens displaying the status of the operation.
6. Click **Close** to exit the status window. The deleted profiles are no longer listed in the Settings Profiles table for the given application. The number of profiles in the Operations area is updated to reflect the latest deletion.

Security Management

Use the Security Management section to create, modify, and delete security profiles. Security and compliance profiles allow you to deploy customized security scan settings to devices in your environment. A security profile consists of configuration settings for devices, which allow you to manage the settings used during a security scan. By creating or modifying a security profile, you can analyze and parameterize configuration control data for targeted devices.

Once you create and/or modify security profiles, they can be deployed to the targeted systems where a security scan is necessary. In RCA Enterprise, Security Profiles are listed as services and

can be deployed to target machines through policy entitlement, similar to the deployment of other services.

Once security profiles have been created and deployed, it is possible to see summary reports about security and compliance software giving administrators visibility to the run-time data of this software. See "Security Tools Management Reports" on page 212.

Security Templates

Security and compliance templates are used to create instances of deployable security profiles. You can download the most current content for security templates from the HP Live Network site. See "Accessing HP Live Network Content" on page 127.

You can select any of the provided security templates to create additional profiles or to modify existing ones. The Operations tab in the RCA Console provides a **Security Templates** area under Security Management that allows you to see the security templates on your system that have configurable profiles.

Creating New Profiles

You can create additional profiles for the devices on your system. Security templates are provided for this purpose. The template is used to create a security profile instance. You can start with a blank profile or you can clone an existing one if it is similar to the one you want to create, thus making the procedure easier to perform.

To create a new security profile:

1. On the Operations tab, expand Security Management in the left navigation pane and click the **Security Templates** link. The security templates on your system will be displayed in the content area on the right.
   The first template displayed is a general security tool template that can be used to manage the scanning of all security software on your system. The following ones are specific to a particular software product and allow you to provide more options as relevant to that product.

   In our example, we are using the general template to illustrate how to create profiles.

2. In the **DisplayName** column, click the name of the template for which you want to create a new profile. As indicated, we are using the generic template. A window opens that contains the following tabs:
   - Profiles: Displays the existing profiles for the selected template. On this tab, you can create, view, modify, and delete security profiles. Profile names displayed with angle brackets (< >) surrounding them are HP-supplied profiles.

     Note: Be aware that if you modify these profiles, your changes can be lost the next time you update your security content from the HP Live Network site.

   - Details: Displays information about what the template does and how to use it.

3. On the Profiles tab, click **Create a New Profile** on the toolbar in the Security Profiles table. The Security Profile Creation Wizard opens.
   Alternatively, you can check the box next to an existing profile that you want to copy and click **Copy the Selected Profile**. The Copy and Modify Security Profile Wizard opens in this

case. This wizard allows you to clone the selected existing profile. If you select to copy an existing profile, all fields, except for the profile Display Name, will be populated with the values contained in the selected existing profile.

4. In either wizard, specify the following information:
   - **Display Name**: Type a name for the profile
   - **Description**: Type a description for the profile
5. Click **Next**. The next page of the wizard opens which allows you to type properties specific to the particular template. In the case of copy, these fields will be pre-populated and you will have to modify them as necessary. In the generic template, you must specify the following:
   - Scan Options: You can choose **Scan Only** or **Scan and Remediate**.
   - Remediation Enable Options: You must fill in the fields in this section only if you have chosen **Scan and Remediate** as your scan option. However, help is available next to each option field indicating the value expected.
   - Remediation Disable Options: You must fill in the fields in this section only if you have chosen **Scan Only** as your scan options. However, help is available next to each option field indicating the value expected.
6. Click **Create** or **Copy** depending on the wizard. The newly created profile is listed in the Security Profiles table on the Profiles tab. The number of profiles in the Operations area is also updated to reflect the latest addition.

Modifying Existing Profiles

Property settings for security profiles can be viewed and modified.

To modify a security profile:

1. On the Operations tab, expand Security Management in the left navigation pane and click the **Security Templates** link. The security templates on your system will be displayed in the content area on the right.
2. In the **Display Name** column, click the name of the template that has a profile that you want to modify. A window opens displaying the existing profiles for the selected template on the Profiles tab.
3. On the Profiles tab in the **Display Name** column, click the name of the profile that you want to modify. A window opens with Summary and Properties tabs displaying all of the properties for the selected profile.
4. Modify the property values on both tabs as necessary.
5. Click **Save** to save your changes.

Deleting Profiles

Security profiles can be deleted when they are no longer needed.

To delete a security profile:

1. On the Operations tab, expand Security Management in the left navigation pane and click the **Security Templates** link. The security templates on your system will be displayed in the

content area on the right.

2. In the **Display Name** column, click the name of the template that has a profile that you want to delete. A window opens displaying the existing profiles for the selected template on the Profiles tab.
3. On the Profiles tab, check the box next to the profile name(s) that you want to delete.
4. Click **Delete Selected Profile(s)** on the toolbar. A pop-up confirmation window opens.
   If the selected profiles are entitled in any external policy directories, you must manually remove these entitlements before continuing. Otherwise, you may get an agent connection failure (reported as error code 650).
5. Click **Yes** if you want to continue. A window opens displaying the status of the operation.
6. Click **Close** to exit the status window. The deleted profiles are no longer listed in the Security Profiles table for the given template. The number of profiles in the Operations area is updated to reflect the latest deletion.

Chapter 9

Configuration

The Configuration area allows you to manage user access to the Console, define and configure infrastructure servers, manage patch acquisition schedules and settings, manage hardware, and configure ODBC settings.

Use the links in the navigation area on the left side of the Configuration tab to access the various configuration options. These options are described in the following sections:

Core Configuration Options

- "Licensing" on next page
- "Core Console Access Control" on next page
- "Infrastructure Management" on page 273
- "Device Management" on page 307
- "Patch Management" on page 311
- "Out of Band Management" on page 335
- "OS Management" on page 338
- "Dashboards" on page 340
- "Usage Management" on page 338

Satellite Configuration Options

- "Licensing" on next page
- "Upstream Server" on next page
- "SSL" on page 274
- "Satellite Console Access Control" on page 269
- "Configuration" on page 271
- "Data Cache" on page 271
- "Satellite Console Patch Management" on page 334
- "Security and Compliance Management" on page 335
- "Policy" on page 277
- "OS Management" on page 338
- "Thin Clients" on page 310
- "Multicast" on page 305

Licensing

A functional RCA environment requires a valid Persistent-issued license. You can use this section to review your RCA license.

To apply a new license:

1. Copy and paste the license information from your new `license.nvd` file into the **License Data** text box.

   Note: When copying the license information from your license file, do not include the text that precedes the line `[MGR_LICENSE]` because this will result in the license information not being “readable” to the Console.

2. Click **Save**. Updated license information is displayed after **Current License**.

Upstream Server

On a Satellite console, use the Configuration tab **Upstream Server** area to edit the upstream host server information. The upstream server is the server this Satellite will synchronize with, as well as fetch information for requests if a service is disabled or a resource is unavailable. You may use SSL for this inter-server communication; the upstream server must be capable of receiving SSL requests.

Access Control

This panel offers different administrative controls depending on whether you are in the Core or Satellite Console.

- Access Control on the Core Console allows RCA administrators to configure and manage user access to the Console. For more information, see "Core Console Access Control" below.
- Access Control on the Satellite Console allows RCA administrators to select and configure an authentication method. For more information, see "Satellite Console Access Control" on page 269.

Core Console Access Control

Use the Access Control section to create instances of internal **users** and **groups** with unique custom IDs and passwords. Then, assign **roles** (see "Roles Panel" on page 258) to the users and groups to manage the areas of Console that the users can access, as well as the administrative tasks for which they are authorized.

Users & Groups Panel

In the Users & Groups panel, create user and group instances and assign a role to each. The role determines which areas of the Console each user can access.

Management jobs contain a **Creator** field that displays the user ID under which a job is created. It is the user IDs that are created in this area that will be displayed.

- During installation, a default user, `admin`, exists with the default password of `secret`. This "failsafe" user account has full access to the Console and cannot be deleted.
- RCA users and groups in Console can be either **internal** or **external**, as described below.
  - **Internal**
    All users and groups that you create in the Users & Groups panel are "internal". You can delete and update these users and groups from the Core Console. You can add internal users to internal groups only. You cannot add a group to an existing group.
  - **External**
    In the Enterprise edition, RCA administrators have the option of leveraging external directories (such as LDAP and Active Directory) to add users and groups and configure their access permissions and credentials. You cannot create, delete, or update these "external" users and groups from the Core Console; an administrator must use the LDAP/AD tools to do so. An RCA administrator can, however, configure a directory source for authentication. This source appears in the **Users & Groups** panel and the **Source** column references the directory from which the user and group originated.

The Users & Groups panel enables you to perform the following administrative tasks. All administrative tasks can be performed on internal users and groups at the core console. For external users and groups, only roles can be assigned and modified at the Core Console.

- "Directory Services Filters" below
- "Managing a User" below
- "Managing a Group" on page 257
- "Assigning Roles" on page 259

Directory Services Filters

The Users & Groups panel displays all the users and groups that are currently available in the internal directory or configured in the external Active Directory. To limit the amount of data displayed in the Users & Groups panel, you can use filters:

1. In the RCA Console, click **Configuration** tab.
2. In the left pane, click **Access Control** > **Users& Groups** Panel.
3. In the Information area, select one of the available options in the **Directory Services** list.
4. Create a **Filter** expression by selecting an attribute, an operator, and typing in the criteria to match.
5. Click **submit**. The users and groups that match the criteria you specified are listed in the Users & Groups panel.

Managing a User

You can perform the following tasks to manage a user:

- Create an internal user
- View and change an internal user's properties
- Delete an internal user
- Assign a role to a user (as described in the section, "Roles Panel" on page 258). You can assign more than one role to a user.
- Remove a role from a user (as described in the section, "Roles Panel" on page 258).
- View capabilities assigned to a user based on the user roles under the Capabilities tab in the User Properties panel.
- View targets assigned to a user based on the user roles by clicking a capability under the Capabilities tab in the User Properties panel.
- View groups that the user is assigned to. You can select a group's ID to access the Group Properties window and manage groups as described in "Managing a Group" on next page.

To create an internal user:

1. Click **Create a New User**  to launch the User Creation Wizard.
2. Specify values for the following fields:
   - ID: Specify the unique identifier for the internal user. Use alphanumeric characters (A-Z, a-z, and 0-9). You can also use underscore (_).
   - Display Name: Specify display name for the user.
   - Description: Specify a description for the user. This is an optional field.
   - Password: Specify a password for the user. Use only ASCII characters when creating passwords.

     Note: If you change the password for the *current user*, you will be logged out automatically. Log in as the user with the new password.

   - Confirm Password: Type the password again.
3. Click **Create**.
   An entry for the new user is created in the Users & Groups area. The Type column indicates if the entry in the ID column is a user.

To View and Modify User Properties:

1. Click an internal user's ID to view its properties.
2. In the User Properties window, modify the user's properties, such as the display name and description, and access the Change Password window.
3. Click **Save** to confirm and preserve any changes.

To Delete an Internal User:

Select the internal user's ID from the list and click **Delete the Selected User(s)/Group(s)**  .

Note: The *current user* cannot be deleted.

In order to delete this ID, you must log out and then log in as a different Administrator to execute the deletion.

Managing a Group

You can perform the following tasks to manage a group:

- Create an internal group (as described in "Creating an Internal Group" below).
- View and change an internal group's properties (as described in the next section).
- Delete an internal group (as described in "Deleting an Internal Group" on next page).
- Assign a role to a group (as described in the section, "Roles Panel" on next page). You can assign more than one role to a group.
- Remove a role from a group (as described in the section, "Roles Panel" on next page).
- View capabilities assigned to a group based on the roles.
- Assign one or more users to the group (as described in "Assigning a User to a Group" on next page).
- Remove one or more users from a group (as described in "Removing a User from a Group" on next page).

Creating an Internal Group

1. Click the **Create a New Group** to launch the Group Creation Wizard.
2. Type values for the following fields:
   - ID: Specify the unique identifier for the internal group. Use alphanumeric characters (A-Z, a-z, and 0-9). You can also use underscore (_).
   - Display Name: Specify display name for the group.
   - Description: Specify a description for the group. This is an optional field.
3. Click **Create**.

An entry for the new group is created in the Users & Groups area. The Type column indicates if the entry in the ID column is a group.

Viewing and Modifying Group Properties

1. Click an internal group's ID to view its properties.
2. In the Group Properties window, modify the group's properties, such as the display name and description.
3. Click **Save** to confirm and preserve any changes.

Assigning a User to a Group

1. Click an internal group's ID to launch Group Properties window.
2. Select **Users& Groups** tab.
3. Click the **Add Users to this Group**  . The User Selection window opens.
4. Select the users to assign to the group.
5. Click **Assign**. The refreshed ID column displays the remaining users available to be added to the group.
6. Click **Close** to return to Group Properties window. The **Users & Groups** tab displays all the users currently assigned to the group.

Removing a User from a Group

1. Click an internal group's ID to launch Group Properties window.
2. Select **Users & Groups** tab.
3. Select an ID from the list and click **Remove Selected User(s) from this Group**  .

Deleting an Internal Group

Select an internal group's ID from the list and click **Delete Selected User(s)/Group(s)**  .

Roles Panel

There are various levels of administrative authority (**roles**) that can be assigned to users and groups. Assign a role to a user or group based on the access and management-permissions that you want available to the user. In the Roles panel, you can create a role, assign capabilities to the role and assign the role to a user or a group. "Capabilities" on page 261 determine the areas of the Console a user can access and tasks the user can perform. You can delete roles and modify the properties. The default user roles in Console are:

- **Administrators**: These users have unlimited access to the Core Console, as well as the ability to perform all administrative functions. This is a "superset" role; it encompasses all of the functionality and authority of the Operator and Reporter roles.
- **Operators**: These users can perform management, operational, and reporting-related tasks in the Core Console. They cannot access the Configurations tab. This role encompasses the functionality and authority of the Reporter role.
- **Reporters**: These users' can view, compile, and print reporting data in the Core Console. Their access is limited to the Reporting and Dashboards tabs.

Note: You can assign more than one role to a user or group. You cannot delete or modify the default roles.

The Roles panel enables you to perform the following tasks:

- "Managing a Role" below
- "Assigning Roles" below
- "Capabilities" on page 261
- "Managing Targets" on page 268

Managing a Role

- You can perform the following tasks to manage a role:
- Create a Role (as described in "Creating a Role" below).
- View and change the role's properties (as described in "Viewing and Modifying Role Properties" below).
- Delete a Role (as described in "Deleting a Role" below).
- Assign a role to a user or group (see "Assigning Roles" below).
- Remove a user or group from a role (see "Removing a Role from a User or Group" on next page).
- Assign capabilities to a role (see "Managing Capabilities" on page 266).

Creating a Role

1. Click **Create a New Role** to launch the Role Creation Wizard.
2. Specify values for the following fields:
   - Role Name: Specify the unique identifier for the role. Use alphanumeric characters (A-Z, a-z, and 0-9). You can also use underscore (_).
   - Display Name: Specify display name for the role.
   - Description: Specify a description for the role. This is an optional field.
3. Click **Create**.

Viewing and Modifying Role Properties

1. Click a role to view its properties. The Role Properties window opens.
2. In the Role Properties window, modify the role's properties, such as the display name and description.
3. Click **Save** to confirm and preserve any changes.

Deleting a Role

To delete a role, select the role from the list and click **Delete the Selected Role(s)** .

Assigning Roles

You can assign a role to a user or group in either of two ways in the Console:

- Using the Roles panel:
  a. Click a role in the table to invoke the Role Properties window.
  b. Click **Users & Groups** tab; this tab displays a list of the users and groups that have been assigned this role.
  c. To assign user or group to the role, click **Add User(s)/Group(s) to this Role**. The User Selection window opens.
  d. Select user or group and click **Assign**. The refreshed ID column displays the remaining users or groups that can be assigned this role.
  e. Click **Close** to return to the Role Properties window. The **Users & Groups** tab displays refreshed list of the users and groups that have been assigned this role.
- Using the Users & Groups panel:
  a. Click an ID in the table to invoke the User Properties or Group Properties window.
  b. Select the **Roles** tab; this tab displays the roles currently assigned to the user or group.
  c. Click **Add Role(s) to this User** or **Add Role(s) to this Group** to launch the Role Selection window.
  d. Select a role to assign to the user or group and click **Assign**. The refreshed Role column displays the remaining roles available to be assigned to a user or a group.
  e. Click **Close** to return to the User Properties or Group Properties window. The Roles tab displays all the roles currently assigned to the user or group.

Removing a Role from a User or Group

You can remove roles from a user or group in either of two ways in the Console:

- Using the Roles panel:
  a. Click a role in the table to invoke the Role Properties window.
  b. Select **Users & Groups** tab; this tab displays a list of the users and groups that have been assigned this role.
  c. To delete user or group from the role, select user or group and click **Remove the Selected User(s)/Group(s) from this Role**. The refreshed ID column displays the remaining users or groups that have been assigned this role.
- Using the Users & Groups panel:
  a. Click an ID in the table to invoke the User Properties or Group Properties window.
  b. Select the **Roles** tab; this tab displays the roles currently assigned to the user or group.
  c. To delete role from the user or group, select role and click **Remove Selected Role(s) from this User** or **Remove Selected Role(s) from this Group**. The refreshed Role column displays the roles currently assigned to the user or group.

Capabilities

The capabilities determine which tasks the user can perform. You can use the Capability Management Wizard to view and manage the capabilities assigned to a role. You cannot create new capabilities. Capabilities cannot be assigned to the default roles. You can perform the following tasks to manage the capabilities:

- "To Assign Capabilities to Roles:" on page 266
- "Removing a Capability from a Role" on page 267

You can also add support for custom software domains and improve the user logon time. For more information, see the following sections:

- "Support for Custom Software Domains" on page 267
- "Improving External User Logon Time" on page 267

The following is the list of capabilities available in the Capability Management Wizard to associate with a role:

Available Capabilities

Capability Name	Description	Capability group(s) this capability belongs to
config.accesscontrol	Enables you to perform all Access Control based tasks under configuration tab.	Configuration
config.all	Enables you to perform all tasks under configuration tab.	Configuration
custom.report	Enables you to view all customized reports.	Report
dashboard.all	Enables you to view all dashboards under dashboard tab.	Dashboard
dashboard.Compliance Management.executive	Enables you to view Compliance Management executive dashboard and reports in the Dashboard and Reporting tabs.	Dashboard, Report
dashboard.Compliance Management.operational	Enables you to view Compliance Management operational dashboard and reports in the Dashboard and Reporting tabs.	Dashboard, Report
dashboard.HPCAManagement.executive	Enables you to view HPCA Management executive dashboard and reports in the Dashboard and	Dashboard, Report

Capability Name	Description	Capability group(s) this capability belongs to
	Reporting tabs.	
dashboard.HPCAManagement.operational	Enables you to view HPCA Management operational dashboard and reports in the Dashboard and Reporting tabs.	Dashboard, Report
dashboard.PatchManagement.executive	Enables you to view Patch Management executive dashboard and reports in the Dashboard and Reporting tabs.	Dashboard, Report
dashboard.PatchManagement.operational	Enables you to view Patch Management operational dashboard and reports in the Dashboard and Reporting tabs.	Dashboard, Report
dashboard.SecurityTools Management.executive	Enables you to view Security Tools Management executive dashboard and reports in the Dashboard and Reporting tabs.	Dashboard, Report
dashboard.SecurityTools Management.operational	Enables you to view Security Tools Management operational dashboard and reports in the Dashboard and Reporting tabs.	Dashboard, Report
dashboard.Vulnerability Management.executive	Enables you to view Vulnerability Management executive dashboard and reports in the Dashboard and Reporting tabs.	Dashboard, Report
dashboard.Vulnerability Management.operational	Enables you to view Vulnerability Management operational dashboard and reports in the Dashboard and Reporting tabs.	Dashboard, Report
management.all	Enables you to perform all tasks under management tab.	Management
mobile.config	Enables you to perform mobile management tasks under the Configuration tab.	Mobile
mobile.dashboard	Enables you to view mobile management dashboards for smart phones and tablets.	Mobile

Capability Name	Description	Capability group(s) this capability belongs to
mobile.notify	Enables you to notify all mobile devices in your enterprise.	Mobile
mobile.operation.management	Enables you to perform all mobile management tasks under the Operations tab.	Mobile
mobile.policy.entitle	Enables you to entitle mobile policies.	Mobile
mobile.policy.read	Enables you to view mobile policies.	Mobile
mobile.policy.unentitle	Enables you to unentitle mobile policies.	Mobile
mobile.read	Enables you to view the mobile services from the Mobile library.	Mobile
mobile.report	Enables you to view mobile management reports.	Mobile
operation.all	Enables you to perform all tasks under the Operations tab.	Operation
operation.infraMgmt	Enables you to perform all infrastructure management tasks under the Operations tab.	Operation
os.config.all	Enables you to perform OS related tasks under configuration tab.	OS, Configuration
os.deploy	Enables you to view and deploy OS to the managed devices.	OS, Management
os.export	Enables you to view and export the published OS to the `ServiceDecks` directory on your RCA server.	OS, Operation
os.import	Enables you to view and import OS into the OS Library.	OS, Operation
os.read	Enables you to view OS from the OS Library.	OS, Operation
patch.config.all	Enables you to perform patch related tasks under configuration	Patch, Configuration

Capability Name	Description	Capability group(s) this capability belongs to
	tab.	
patch.delete	Enables you to delete the patch device under the Operations tab. The patch device is deleted from the reporting database.	Patch, Operation
patch.dtm	Enables you to manage dtm job for patch.	Patch, Management
patch.export	Enables you to view and export the published patches to the `ServiceDecks` directory on your RCA Server.	Patch, Operation
patch.generalops	Enables you to perform all patch operations except patch delete device under the Operations tab.	Patch, Operation
patch.import	Enables you to view and import the patches into the Patch Library.	Patch, Operation
patch.notify	Enables you to manage notify job for patch.	Patch, Management
patch.policy.entitle	Enables you to view and entitle patch services.	Patch, Management
patch.policy.read	Enables you to view patch services.	Patch, Policy, Management
patch.policy.unentitle	Enables you to view and remove the entitled patch services.	Patch, Policy, Management
patch.read	Enables you to view patches from the Patch Library.	Patch, Operation
report.all	Enables you to view all reports under reporting tab.	Report
report.ApplicationManagementProfiles.all	Enables you to view Application Management Profiles reports under Reporting Views in the Reporting tab.	Report
report.ComplianceManagement.all	Enables you to view Compliance Management reports in the	Report

Capability Name	Description	Capability group(s) this capability belongs to
	Reporting tab.	
report.HPCAManagement.all	Enables you to view HPCA Management reports under Reporting Views in the Reporting tab.	Report
report.InventoryManagement.all	Enables you to view Inventory Management reports in the Reporting tab.	Report
report.PatchManagement.all	Enables you to view Patch Management reports in the Reporting tab.	Report
report.SecurityToolsManagement.all	Enables you to view Security Tools Management reports in the Reporting tab.	Report
report.SettingsManagement.all	Enables you to view Settings Management reports under Reporting Views in the Reporting tab.	Report
report.UsageManagement.all	Enables you to view Usage Management reports in the Reporting tab.	Report
report.VirtualizationManagement.all	Enables you to view Virtualization Management reports under Reporting Views in the Reporting tab.	Report
report.VulnerabilityManagement.all	Enables you to view Vulnerability Management reports in the Reporting tab.	Report
software.dtm	Enables you to manage dtm job for software.	Software, Management
software.export	Enables you to view and export software services to the `ServiceDecks` directory on your RCA server.	Software, Operation
software.import	Enables you to view and import software services into the Software Library.	Software, Operation

Capability Name	Description	Capability group(s) this capability belongs to
software.notify	Enables you to manage notify job for software.	Software, Management
software.policy.entitle	Enables you to view and entitle software services.	Software, Policy, Management
software.policy.read	Enables you to view available software services.	Software, Policy, Management
software.policy.unentitle	Enables you to view and remove the entitled software services.	Software, Management
software.read	Enables you to view software in the Software Library.	Software, Operation

Managing Capabilities

To Assign Capabilities to Roles:

1. Click a role in the Role column to assign capabilities. The Role Properties window opens.
2. Select the **Capabilities** tab.
3. Click **Launch Capability Management Wizard** to assign capabilities to the role. The Capability Management Wizard opens.
4. Select Capability Types from the list. All the capabilities available under the selected Capability Type are listed under capabilities column.
5. Select capabilities from the Capabilities column.
6. Click **Add to Selection**. The refreshed Capabilities column displays the remaining capabilities available to be assigned to the role. The Selected Capabilities tree located to the right displays the list of capabilities currently assigned to this role. To discard the changes, click **Reset**.
7. To assign more capabilities, repeat step 4 to step 6.
8. Click **Next** to review the capabilities selected. The status column indicates if a capability was recently assigned or existed earlier.
9. Click **Commit** to save the selected capabilities.
10. If you want to change a capability, click **Previous**. When you are ready to proceed, click **Commit**.
11. The capabilities assigned to the role are listed in Role Properties window.

Removing a Capability from a Role

1. Click a role in the Role column. The Role Properties window opens.
2. Select the **capabilities** tab.
3. Click **Launch Capability Management Wizard** to remove capabilities from the role. The Capability Management Wizard opens.
   The Selected Capabilities tree located to the right displays the list of capabilities currently assigned to this role.
4. Expand the Selected Capabilities list and select the capabilities to remove from this role.
5. Click **Remove Selected**. The refreshed Selected Capabilities tree displays the capabilities currently assigned to this role.
   To discard the changes, click **Reset**.
6. Click **Next** to review the capabilities removed. The status column indicates if a capability was recently removed.
7. If you want to change a capability, click **Previous**. When you are ready to proceed, click **Commit**.
8. The capabilities assigned to the role are listed in Role Properties window.

Support for Custom Software Domains

You can provide access control for custom software domains also. A user can perform tasks, in the default software domain as well as custom software domains, based on the capabilities assigned to the role associated with the user.

To enable access control for the custom software domains:

1. Add a comma separated list of custom domains to the parameter `custom_sw_domains` in the *<InstallDir>*`\tomcat\webapps\em\WEB-INF\console.properties` file.

   For example, a user with `software.read` capability can view the softwares in the custom domains, *software_custom1* and *software_custom2also* if the parameter `custom_sw_domains` is set in the `console.property` file as follows:

   `custom_sw_domains=`*software_custom1*,*software_custom2*
2. Restart the HPCA Tomcat service.

Improving External User Logon Time

Access Control dynamically verifies the cumulative capabilities for external users at each logon by fetching the data from the external directories. To assign capabilities to external users, you can assign roles to these users or add external users to groups with roles. The external users might take a long time to logon if they are part of multiple groups. You can reduce the user logon time by caching the group membership data for the external users for the hours you specify in the `group.cache.duration` parameter. Any external directory changes during this duration are reflected at next logon after the specified hours end.

To improve the user logon time:

1. Set the following parameters in the *<InstallDir>*`\tomcat\webapps\securitymanager\WEB-INF\securitymanager.properties` file:
   - `refresh.groups.at.logon=false`
   - `group.cache.duration=`*n*

   where *n* is the number of hours until the group membership data is cached.

   Note: When `refresh.groups.at.logon=true`, the dynamic refresh at logon is enabled and the `group.cache.duration` parameter is disregarded. By default `refresh.groups.at.logon` is set to true.
2. Restart the HPCA Tomcat service.

Managing Targets

Targets determine an OU or a group of managed devices on which users can perform the capabilities assigned to them based on their roles. Individual managed devices cannot be called targets and assigned to a role. When you assign a target to a role, all child OUs or groups under that target are automatically assigned to the role. Targets cannot be assigned to the default roles.

For a user, dashboards will display the targets assigned to roles with dashboard capabilities as well as targets assigned to roles with reporting capabilities. Similarly, reports will display targets assigned to roles with reporting capabilities as well as targets assigned to roles with dashboard capabilities.

Note: If you assign a group of target devices or users to a role for reporting and dashboard capabilities, the devices are not displayed in the reports.

Assigning Targets to a Role

To assign targets to a Role:

1. Click a role in the Role column to assign targets. The Role Properties window opens.
2. Select the **Targets** tab.
3. Click **Launch Target Management Wizard** to assign targets to the role. The Target Management Wizard opens.
4. Select your directory service from the Directory Services list. By default, the list of internal groups of managed devices is displayed in the Available Targets list in the Target Management Wizard.
5. Use Filters to limit the list of targets displayed in the Available Targets list.
6. Click **Submit**. The list of targets is displayed.

7. Select targets from the Target Name column. Click **Back** to navigate to the previous list of targets.
8. Click **Add to Selection**. The Selected Target list in the right pane displays the newly added targets in addition to the list of targets previously assigned to this role.
9. Click **Reset** to discard the targets you have selected and select the targets again.
10. To assign more targets, repeat step 4 to step 7.
11. Click **Commit** to assign the targets to the role.

Removing Targets from a Role

To remove targets from a role:

1. Click a role you want to remove targets from in the Role column. The Target Properties window opens.
2. Select the **Targets** tab.
3. Click **Launch Target Management Wizard** to remove targets from the role. The Target Management Wizard opens.
   The Selected Targets list in the right pane displays the list of targets currently assigned to this role.
4. Select the targets to remove from the role.
5. Click **Remove Selected**. The refreshed Selected Targets list displays the targets currently assigned to this role.
6. Click **Commit** to remove the targets from the role.

Satellite Console Access Control

The Access Control section of the Satellite Console allows an RCA administrator to select a Console-access authentication method (**Local Accounts** or **Directory Service Accounts**) and to configure its settings.

The Summary area of the Access Control section displays the Authentication Method that is currently enabled. The default (Local Accounts) is displayed.

Selecting and configuring an authentication method

1. Click **Configure Authentication**. The Authentication Wizard opens.
2. In the Set Server Authentication Method area, use the Authentication Method drop-down to select either:
   - **Local Accounts** – This method allows an administrator to set *administrator* and *operator* log-on credentials for the Satellite Console; these credentials restrict access to various parts of the Console. This is the default.
   - **Directory Service Accounts** – This method allows administrator authentication using Directory Service Accounts (such as Active Directory) that are in place in the environment.
3. Click **Next** to proceed to the Configuration area and specify the settings for the access method you have chosen.

Using Local Accounts

If you are using Local Accounts to secure access to the Satellite Console, change the password immediately after installing the Satellite server.

Note: Password Considerations

- Use only ASCII characters when creating passwords.
- If you change the password for the *current user*, you will be automatically logged out. Log in as the user, but with the new password.

1. Configure Console access for administrators and operators in the appropriate areas.
   - **Administrator** permissions allow the user to access all areas of the Console.
   - **Operator** permissions restrict the user's access to only the Operations area of the Console.
2. Click **Next**.
3. When the configuration is complete, click **Close**.

The next time you log in to the Satellite Console using a Local Account, use the new password.

Using Directory Service Accounts

An external Directory Service Account can be used to authenticate a user's access to the Satellite Console.

1. In the Directory Service Settings area, specify the configuration parameters as described below.
   - **Directory Host**: The hostname or IP address of the external directory server that will be used for authentication. If you enable SSL, you must specify the Fully-Qualified Domain Name (FQDN) of the external directory server.
   - **Use SSL**: Enable or disable SSL.
   - **Directory Port**: The port that will be used to access the external directory server. The default is 389. If you enable SSL, the default port used by Microsoft Active Directory for secure connections is 636.
   - **Base DN**: The base object in your directory at which to start searching when querying for the users.
     For example, `dc=europe,dc=acme,dc=com`.
   - **Access Group DN**: The Group DN that contains all members who are entitled to access the Core Console with administrative rights.
   - **Directory User ID**: A valid user ID that can access the directory server to verify that a person logging on to the Core is a member of the above-named Group DN. The default is administrator.
   - **Directory Password**: The password that is associated with the above-listed user ID.
2. In the Test LDAP Group User area, supply the credentials of a "test user".

   Note: The test user must be a member of the Access Group DN that was specified above. The Directory User ID and Test User ID must not be the same user account.

This test will ensure that you can access this server after the Directory Service Account configuration is complete.

- **Username**: The user name of an existing Access Group DN user.
- **Password**: The password that is associated with the above-listed user name.

3. Click **Next**.
4. When the configuration is complete, click **Close**.
   Administrators can now sign in to the Satellite Console using their Directory Service Account credentials.

Note: If you enable SSL and an internal or enterprise Certificate Authority is used on your directory server:
- The Certificate Authority certificate from the directory server must be exported in the Base-64 encoded x.509 format and appended to the ca-bundle.crt file located at <InstallDir>\ApacheServer\conf\ssl.crt on the RCA Satellite server.
- The Certificate Authority certificate from directory server must be imported into the RCA Satellite machine's "Local Computer" account's trusted root CA folder.

Configuration

The Configuration option in the left navigation pane on the Configuration tab is available on Satellite Consoles, only.

Configuration services supply "model" and service information to the RCA agents, based on their entitlements. The agents connect to the server to obtain this information and to satisfy changes. When this service is disabled on the Satellite server, RCA agents will have to use a different server to obtain the requested information. This "fallback server" designation should be built in to your infrastructure model (as configured in the CLIENT.SAP Instances of the Configuration Server Database).

To enable the configuration services, select the **Enable** check box and click **Save**.

Data Cache

The Data Cache area is available on Satellite Console only.

Apache Server cache and Proxy Server services control the underlying RCA cache-management service that is used to download data (such as software, patch, security and compliance, operating system, security, and audit) from an upstream host with which the Satellite is synchronized. This page enables you to:

- Enable and disable Apache Server cache services on this Satellite.
- Set Apache Server cache limit, in megabytes.

Note: You *must* configure Satellites before you cache and synchronize data on a Satellite

server. See the *Radia Client Automation Enterprise Installation and Upgrade Guide*, for details.

- Enable and disable Proxy Server preload (static cache) and Proxy Server dynamic cache.
- Enable and disable Patch Manager gateway preload on this Satellite.
- Enable and disable Security and Compliance Management gateway preload.

Configuring Data Cache

1. On the Configuration tab, click **Data Cache**.
2. Set the following options:
   - Select the **Enable Apache Server cache** check box to enable data services for a Satellite. This is the default setting and enables RCA agents that are connecting to the Satellite to receive their Patch Manager Gateway binaries and Security and Compliance Gateway binaries from the Satellite data cache.
   - Clear the **Enable Apache Server cache** check box to disable data services for a Satellite.
     - A synchronization with the upstream host does not download the Patch Manager Gateway binaries and Security and Compliance Gateway binaries to this Satellite.
     - Requests for Patch Manager Gateway binaries and Security and Compliance Gateway binaries from the RCA agents that connect to the Satellite are passed to the upstream host.
   - Select the **Enable Proxy Server preload (static cache)** check box to preload data services for a Satellite. This is the default setting and enables RCA agents that are connecting to the Satellite to receive their resources from the Proxy Server static cache.
   - Clear the **Enable Proxy Server preload(static cache)** check box to disable preloading the data services for a Satellite.
     - A synchronization with the upstream host does not download the resources to the Satellite.
     - Resource requests from the RCA agents that connect to a Satellite fail if the option **Enable Proxy Server dynamic cache** is *also* disabled.
   - Select **Enable Proxy Server dynamic cache** check box to enable data services from the Proxy Server dynamic cache for a Satellite. This option enables RCA agents that are connecting to the Satellite to receive their resources from the Proxy Server dynamic cache.
   - Clear the **Enable Proxy Server dynamic cache** check box to disable the data services from the Proxy Server Dynamic cache for a Satellite.
     Resource requests from theRCA agents that connect to the Satellite fail if the option **Enable Proxy Server preload(static cache)** is *also* disabled.
   - Select **Enable Patch Manager gateway preload** check box to enable Patch Manager Gateway Preload services for a Satellite. This ensures all the patch binaries available on the Core Patch Manager Gateway cache are preloaded to the Satellite Apache server data cache.
     Satellite data cache clean up is independent of the Core Patch Manager Gateway cache clean up. The patch binaries will be available on a Satellite Apache server data cache even if

the patch binaries are deleted from the Core Patch Manager Gateway cache. Patch binaries from the upstream server will be replicated to Satellite Apache server data cache on the next synchronization with that upstream server.

- Clear the **EnablePatch Manager gateway preload** check box to disable Patch Manager Gateway Preload services for a Satellite. This is the default setting.
  - A synchronization with the upstream host does not download the patch binaries available on the Core Patch Manager Gateway cache to the Satellite Apache server data cache.
  - Any data requests from the RCA agents that connect to the Satellite are passed to the upstream host.
- Select **Enable Security and Compliance Management gateway preload** check box to enable Security and Compliance Gateway preload services for a Satellite. This ensures that all the patches that are available on the Core server Security and Compliance gateway cache are preloaded to the Satellite Apache server data cache.
- Clear the **Enable Security and Compliance Management gateway preload** check box to disable Security and Compliance Gateway preload services for a Satellite.
  - A synchronization with the upstream host does not download the patches that are available on the Core server Security and Compliance Gateway cache to the Satellite Apache server data cache.
  - Any data requests from the RCA agents that connect to the Satellite are passed to the upstream host.
- Set **Apache Server cache limit (MB)** to set a maximum size (in megabytes) of the resource cache. The default is 40000 MB.

3. Click **Save** to implement your changes.

When the Operations tab is refreshed, the status of this service is shown under Summary.

Note: You must set the Satellite Cache Account instance to `AUDIT.ZSERVICE.*` for all Satellite servers under Policy->Users in the CSDB Editor to enable the Audit preload services for a Satellite. You must synchronize the Satellite server with the Core server after updating the Satellite Cache Account instance.

Note: The `HTCACHECLEAN` Windows Service runs automatically once a day to clean the Satellite Server cache of files that are no longer necessary. This time interval provides good performance for the vast majority of systems.

Infrastructure Management

The Infrastructure Management section allows you to configure various settings of your RCA infrastructure. See the following sections for details.

- "Proxy Settings" on next page
- "SSL" on next page
- "Policy" on page 277
- "Database Settings" on page 279

- "Satellite Management" on page 279
- "Directory Services" on page 295
- "Job Action Templates" on page 301
- "Multicast" on page 305
- "Live Network" on page 305

Proxy Settings

The Proxy Settings configuration page is used to specify the settings for proxy servers that will be used for internet based communication between the RCA Core Server and external data sources or recipients.

You can establish separate proxy settings for HTTP and FTP communication. The HTTP proxy server is used for Patch Manager Acquisitions, HP Live Network content updates, and Real Simple Syndication (RSS) feeds used by certain dashboard panes. Without these HTTP proxy settings, for example, Patch Manager acquisitions will fail and you will not be able to download bulletins, patches, and related items, such as Windows Update Agent (WUA) files.

The FTP proxy server is used by the Patch Manager to perform HP Softpaq acquisitions.

To configure your proxy settings:

1. On the **Configuration** tab, expand the **Infrastructure Management** area, and click **Proxy Settings**.
2. Select the tab for the proxy server that you want to configure: **HTTP** Proxy or **FTP Proxy**
3. Select the **Enable** box.
4. Provide the following information for the proxy server.
   - **Host**: network addressable name of the proxy server
   - **Port**: port on which the proxy server listens
   - **User ID**: user ID if the proxy server requires authentication
   - **Password**: password for the proxy user if the proxy server requires authentication
5. Click **Save** to implement your changes.

SSL

Enabling SSL protects access to the Core console. With SSL enabled, transactions made while connected to the console are encrypted. RCA supports up to five levels of CA certificates. This means up to five CAs can be used in RCA environment.

Caution: Make sure that you enable SSL and use HTTPS for communication in your RCA. environment. Using HTTPS ensures secure communication in your environment.

Use the SSL section to enable SSL, and define server and client certificates.

- "SSL Server" on next page
- "SSL Client" on next page

SSL Server

The SSL Server certificate is based on the host name of the RCA server. It allows your server to accept SSL connections. It should be signed by a well known certificate authority, such as VeriSign.

To enable and configure SSL for the RCA Server:

1. In the RCA Console, click **Configuration** tab.
2. In the left pane, click **Infrastructure Management** > **SSL**.
3. In the SSL Server area, select the **Enable SSL** check box.
4. Select whether to **Use existing certificates** or **Upload new certificates**.
   If Upload new certificates is selected, click **Browse** to navigate to and select Private Key File and Server Certificate File.
5. Click **Save**.

SSL Client

The Certificate Authority file contains the signing certificates from trusted Certificate Authorities. They allow the RCA server to act as an SSL client when connecting to other SSL-enabled servers. Your server installation comes with a default set of trusted authorities that should be sufficient for most organizations.

To define a CA Certificates File:

1. In the RCA Console, click **Configuration** tab.
2. In the left pane, click **Infrastructure Management** > **SSL**.
3. In the SSL Client area, click **Browse** to navigate to and select the CA Certificates File.
4. Select whether to append this certificates file to existing certificates, or to replace the existing certificate with this new file.
5. Click **Save**

Smart Card Authentication

Enterprise editions of Client Automation support two-way authentication using smart cards. SSL must be enabled for smart card authentication.

As part of the smart card login process, the user must select a certificate that matches a trusted certificate in the Core Server truststore. The process of validating this certificate against the user in the directory consists of the following checks:

- **subjectdn**
  The domain name (subjectdn) value of the certificate is obtained. A check is performed to determine if the subjectdn matches the equivalent userdn in one of the mounted directories where authentication is enabled. If so, the user is eligible to login. If not, the altsubjectname check is performed.

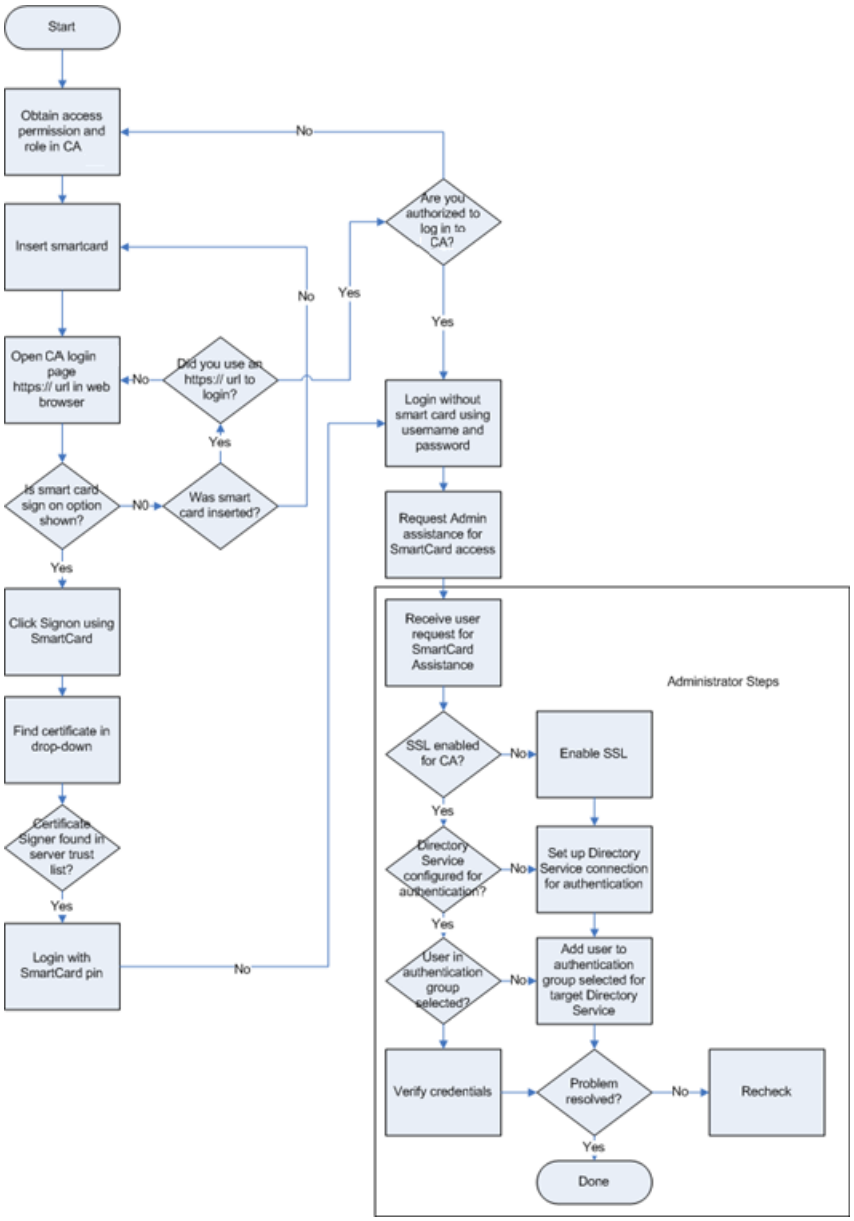
- **altsubjectname**
  The alternate subject name (altsubjectname) value of the certificate is obtained. A check is performed to determine if the altsubjectname matches the AD userprincipal name in one of the mounted directories where authentication is enabled. If so, the user is eligible to login. If not, the email address check is performed.
- **email address**
  It is determined if the certificate has an emailaddress value in the subjectdn. If available, a check is performed to determine if it matches the mail attribute in one of the mounted directories where authentication is enabled. If so, the user is eligible to login. If not, the usercertificate match is performed.
- **usercertificate match**
  A check is performed to determine if the usercertificate matches the usercertificate attribute in one of the mounted directories where authentication is enabled. If so, the user is eligible to login. If not, login fails.

For additional instructions on SSL, policy, and directory services, see the *Radia Client Automation Enterprise SSL Implementation Guide*.

Smart Card Login Process

The following diagram depicts the steps involved in the Smart Card login process. It provides alternative actions and questions to consider if a step in the normal process fails.

Smard Card Login Process



Policy

When configuring policy management to use external directory services, you must consider the following:

- "Policy Server Service Enablement on the Core Server" on next page
- "Policy Server Service Enablement on the Satellite Server" on next page
- "Making the Directory Service Schema Ready for Policy Management" on next page

Policy Server Service Enablement on the Core Server

The Policy Server service is always enabled on the Core Server so that the Core Server can connect to a directory service that contains entitlement information. To configure additional external directories for policy resolution, see "Directory Services" on page 295. Any directory service created with the **Used for Policy** option enabled will automatically be used for policy resolution.

Policy Server Service Enablement on the Satellite Server

On a Satellite Server, you can enable or disable the Policy Server service option. Leave this service disabled if one of the following conditions is true:

- an external policy store is not being used
- the Policy Server service will not be running
- the Satellite Server is configured in the streamlined mode

When this option is disabled and the Agent makes a request for policy resolution from the Satellite, the requested policy is obtained from an upstream server.

Full-Service Satellites should have this service enabled. When this option is enabled, policy resolution takes place on the Satellite server itself.

Making the Directory Service Schema Ready for Policy Management

Policy Server automatically generates LDIF (LDAP Data Interchange Format) schema configuration files for the Active Directory (AD) directory services configured on the Core Server. They are customized for each AD directory service and can be used to update the directory schema to allow for RCA policy management.

If you have schema update rights, you can import LDIF data from the configuration file into an AD directory service by executing the `ldifde` command which is available at the command prompt on the machine where AD is installed. The LDIF schema configuration files, which are input to this command, are stored in the *<InstallDir>*`\PolicyServer\etc\ldif` directory on the Core Server and on full-service Satellites Servers. You must copy the `ldif` file for the AD directory service whose schema you want to update to the machine where that AD directory service is installed. If you copy the file to the `C:\Temp` directory on the AD machine, and the file name is `companyABC.ldif`, the command line would be the following:

```
ldifde -i -f C:\Temp\companyABC.ldif
```

This command updates the AD schema with the schema changes present in the `ldif` file making the directory service ready for RCA policy management.

If your external directory service is not AD, you must manually configure the necessary attributes and objects classes in the directory service schema to enable RCA Policy Management. See the *Radia Client Automation Enterprise Policy Server Reference Guide* for detailed information.

Database Settings

Use Database Settings to configure the ODBC connections to your SQL and Oracle databases for the Core server objects.

Prerequisites

The Core database must be created and an ODBC connection defined for it. See the *Radia Client Automation Enterprise Installation and Upgrade Guide* for more details.

To configure Messaging:

1. On the Configuration tab, click **Infrastructure Management** then **Database Settings**.
2. Set the following options.
   - **DSN**: Select the DSN for the Core database.
   - **User ID**: Specify the user ID for the DSN.
   - **Password**: Specify the password that is associated with the ODBC user ID.
   - **Server Host**: Specify the name of the server hosting the database.
   - **Server Port**: Specify the server port (default is 1433)
3. Click **Save**.

Satellite Management

The Infrastructure Management, Satellite Management area on the Configuration tab enables you to deploy and manage Satellite servers from the RCA Console. Satellite servers are used to optimize bandwidth and increase network performance by providing remote services, including data caching, for managed devices.

For RCA Enterprise Edition, you can choose one of three deployment modes:

- **Streamlined** (Standard) mode offers only data caching services to the Client Automation agents that the Satellite serves.
- **Full** service mode offers configuration services as well as data caching and OS configuration services to the Client Automation agents that the Satellite serves.
- **Custom** mode allows you to select specific services to enable on the Satellite.

For more information about deployment modes, see “Radia Client Automation Satellite Server” in the *Radia Client Automation Enterprise Installation and Upgrade Guide*.

To define and configure Satellite servers, complete the following tasks:

1. Import the device into the RCA device repository. See "Importing Devices" on page 145 for more information.
2. Add devices to the Servers group. See "Servers" on next page.
3. Deploy the Satellite Server component to these devices. This enables remote services, including data caching, on these devices. See "Install the Satellite Server Component" on page 283.

4. Optionally, create Server Pools and assign Servers to these pools. See "Server Pools" on page 288
5. Create Locations and assign Servers or Server Pools to these Locations. See "Locations" on page 290.
6. Create Subnets and assign them to Locations. See "Subnets" on page 293.

Managed devices connect to Satellite servers based on the subnet that is assigned to Server or Server Pool Locations. For example, if a device is on subnet 208.77.1.0 and you have assigned that subnet to a specific Location, your device contacts the assigned Servers or Server Pools for this Location in priority order as defined within the Location.

If the Proxy Server dynamic caching is enabled on the Satellite server, the data requested by agents is automatically cached on the Satellite server. The Satellite servers can also be pre-populated with all data on the RCA Core server using the synchronize feature. See "Delete a Server from Server Pools" on page 286 for details.

Note: You can define and configure Satellite servers from the RCA Core server only. You cannot do this from another Satellite server.

The Satellite Management area contains the following tabs:

- "Servers" below
- "Server Pools" on page 288
- "Locations" on page 290
- "Subnets" on page 293

Servers

The Satellite Management **Servers** tab displays all Core and Satellite servers that currently belong to the Servers group. You can select one of three possible views on this tab, namely:

- Core Server: Displays the Core server only
- Satellite Servers: Displays Satellite servers only
- All Servers: Displays both the Core and Satellite servers, as well as devices manually added to the Servers group and Legacy Proxy Servers from a previous version of the product.

You can open the Server property page for each server to view or edit server properties, to view assigned "Locations" on page 290, and to view or edit "Server Pools" on page 288 assignments.

You can use the toolbar buttons on the Servers tab to define additional Satellite servers by adding devices to the Servers group and then installing the Satellite server component to those devices. Satellite servers are devices added to the Servers group, with the Satellite server component installed.

Servers Toolbar Buttons

Button	Description
	**Refresh Data** – Refresh the list of servers.
	**Show/Hide Filter Input** – Show or Hide the Filter input area to restrict the display of Servers to only those matching user specified criteria.
	**Add device(s) to Servers group** – Add devices to the RCA Satellite Servers group.
	**Remove device(s) from Servers group** – Remove devices from the RCA Satellite Servers group.
	**Install the Satellite Server** – Launch the Satellite Server Deployment Wizard to install the Satellite server on the selected devices.
	**Uninstall the Satellite Server** – Launch the Satellite Server Removal Wizard to uninstall the Satellite server from the selected devices.
	**Synchronize the selected Satellite Servers service cache** – Synchronize the selected Satellite server's service cache with the RCA Core server.
	**Delete the Selected Device(s)** – Remove the device from the RCA device repository.

Note: Removing the Satellite server using the **Remove device(s) from Servers group** button, **Uninstall the Satellite Server** button, or **Delete the Selected Device(s)** button does not delete the device details from the DMASTATS table. If you want to delete the Satellite server details from the RDBMS database, you must manually remove the corresponding Satellite server entry from the DMASTATS table. For more information on DMASTATS, see *Radia Client Automation Enterprise Distributed Configuration Server Reference Guide*.

After you add servers, you can optionally assign them to "Server Pools" on page 288. You must assign Servers or Server Pools to "Locations" on page 290 to enable client devices to contact these Servers.

The following sections detail what you can do using the Server property sheet and the toolbar buttons on the Servers tab:

- "Add a Satellite Server" on next page
- "Remove a Satellite Server" on next page
- "Install the Satellite Server Component" on page 283
- "Uninstall the Satellite Server component" on page 284
- "Server Details Window" on page 285
- "Synchronize Satellite Servers Service Cache" on page 286
- "Delete a Server" on page 288

Add a Satellite Server

Before you install the Satellite server component, add the device to the Servers group. When selecting devices to add as Satellite servers, consider the following:

- The devices should have adequate space to store published services.
- The devices should have a capable, high-speed network card (100 MB or 1 GB data transfer rates).
- The devices should be located on a subnet where you want to localize download traffic to that network.

Note: The following ports must be excluded if a firewall is enabled on any of the Satellite Servers that you will be using:

- TCP 139, 445, 3463, 3464, 3465, and 3466

Note that 3466 is the default RCA port. If you customized this port when you installed RCA, be sure that the port you are using is also open.

- UDP 137 and 138

Windows Firewall users can select File and Printer sharing to exclude TCP ports 139 and 445 and UDP ports 137 and 138.

To add an infrastructure server to the Servers group:

1. On the Servers toolbar in the **All Servers View**, click the **Add device(s) to Servers group** toolbar button.
   The Device Selection window opens and shows a list of all devices imported into RCA that do not belong to the Servers group.
2. Select one or more devices from the list, and click **Add Devices**.
3. Click **Close** to close the device selection window.

The added devices now appear in the **Servers** list in the **All Servers** view on the **Servers** tab.

Remove a Satellite Server

If you do not want a device to be managed as a Satellite server, you can remove that server from the Servers group.

Note: You must explicitly uninstall the Satellite server component from the device *before* removing the device from the Servers group. If you remove the device without uninstalling the RCA Satellite server component, the device will automatically re-appear after a period of time since it is still an active Satellite server, and will also remain a member of the Servers group. See "Installing the Satellite server component" on page 284.

To remove a server from the Servers group:

1. On the Servers tab, select the devices that you want to remove from the Servers group.
2. Click the **Remove device(s) from Servers group**  toolbar button. A confirmation pop-up window opens.
3. Click **Yes** to confirm.
   The devices that you selected are removed from the group.

Install the Satellite Server Component

After you add a device to the RCA Satellite Servers group, you can deploy the Satellite server component to that device. This is required to enable remote services, including data caching, on that server.

When you deploy the Satellite server component to a device from the RCA Console, the Core completes the following background processing:

- Using the credentials that you provide, the RCA Core server establishes a connection with the device. These credentials must provide Administrator access to the `IPC$` share on the remote system. If this access level is not available in your environment, perform a manual installation of the Satellite Server component instead of deploying through the RCA Console.
- If the RCA Management Agent is not installed on the device, the Core installs the Management Agent on the device.
- The Management Agent downloads the Satellite server component from the Core server and installs it on the device. The Satellite server deployment process also handles the upgrade and migration scenarios. If a previous version of the Satellite server component is already installed on the device, it is automatically detected and the component is upgraded to the current release and the cache is migrated. Additionally, if the device has an Integration Server-based Proxy Server components installed, the proxy service is stopped, the Integration Server-based Proxy Server is removed, the Satellite server component is installed, and then the cache is migrated.
- The Management Agent automatically runs the First Time Setup Wizard on the device and populates the Host Device field with the name of the Core server.
- The Satellite Server registers with the Core Server.

Note: You can also install the Satellite Server component manually using your HPCA installation media. To register the manually installed Satellite servers, you must first synchronize these Satellites with the Core server.

The Satellite servers that are deployed from the RCA Core Console register with the RCA Core server automatically.

The pertinent CLIENT.SAP and POLICY.USER instances are automatically managed by this Satellite registration process. If Satellite data changes such that a SAP/USER change is required, RCA automatically makes this change.

The RCA administrator can disable this auto-management process by setting the `rmp.cfg` option ENABLE_SAP_MANAGEMENT to 0. By default, this option is ON and is not present in `rmp.cfg`. If you disable this option, the Satellite Management user interface (UI) is rendered inoperable and should no longer be used.

Caution: The manual configurations in the `rmp.cfg` are for Advanced Implementations ONLY. Do not change settings in `rmp.cfg` unless you are a highly experienced RCA administrator.

Installing the Satellite server component

1. Select one or more devices from the Satellite Servers list using the check boxes in the left column.
2. Click **Install the Satellite Server** toolbar button to launch the "Satellite Server Deployment Wizard" on page 350.
3. Follow the steps in the wizard to deploy the Satellite Server component to the selected devices. The Satellite Server is installed to :
   `SystemDrive:\Program Files\Hewlett-Packard\HPCA`

Note: You can also install the Satellite server manually on each device. You might choose to do this, for example, to reduce network traffic.

See the *Radia Client Automation Enterprise Installation and Upgrade Guide* for installation instructions.

If you install the Satellite Server manually, it will appear in the Satellite Servers list. The Satellite server will not serve client devices, until you assign a Location to it to enable client devices to contact the Server.

Services can be preloaded to Satellite Servers using the Synchronize feature. You can also schedule a DTM job using one of the Satellite Servers job action templates. See "Delete a Server from Server Pools" on page 286 for details.

After you have created Satellite Servers, you must define Locations and then assign the Satellite Servers to these Locations. See "Locations" on page 290 for details.

Uninstall the Satellite Server component

If you do not want a device to function as an RCA Satellite Server, you must remove the Satellite server component from that device.

To uninstall the Satellite server component:

1. Select devices from the Satellite Servers list using the check boxes in the left column.
2. Click **Uninstall the Satellite Server** toolbar button to launch the "Satellite Server Removal Wizard" on page 351.
3. Follow the steps in the wizard to remove the Satellite server component from the selected devices.

You can follow the progress of your Satellite Server Removal job under the Jobs area on the Management tab. After this job completes, the Satellite Servers list will show that the Satellite server component is not installed on this device.

Server Details Window

To access the Server Details window, click any server name link in the Servers list on the Servers tab.

From the Server Details window, you can view detailed information about a Satellite server and perform various server management tasks. The following tabs are available on the Server Details window:

- **Summary**: The Summary tab displays the server details, such as Vendor, IP Address, Operating System, HPCA Build ID, and Service Pack.
- **Properties**: The Properties tab displays the server properties, including the server status. By default, the server is enabled, and the client devices can contact this server for resolution. You can disable the Satellite server during the maintenance phase to avoid device connects to this server.
- **Cache**: The Settings area in the Cache tab display the cache preloading options for a Satellite server. You can preload a Satellite server for Software, Patch, and Operating System service cache. The **Preload Enabled** option ensures that the files available on the upstream server cache are preloaded to the Satellite server. If Proxy Server dynamic caching is enabled, the files are cached on the Satellite server as they are requested by the agents.
  The Synchronization area displays the last time the server's service cache was synchronized with the upstream server. Click **Synchronize** to synchronize the Satellite server content with the upstream host. For more information, see the "Delete a Server from Server Pools" on next page.
- **Server Pools**: The Server Pools tab displays the Server Pool assignments for this Server. You can use the toolbar buttons on this tab to add a server to or remove it from the available Server Pools. For more information, see "Server Pools" on page 288.
- **Locations**: The Locations tab displays the Location assignments for this Server. For details on adding and assigning Locations, see "Locations" on page 290.
- **Reporting**: The Reporting tab displays the preload summary for the services that are preloaded or removed from a Satellite server. Only preloaded services are displayed.
- **Operations**: The Operations tab shows the status and state of the configurable Satellite services ("Satellite Configuration Options" on page 253). It also lists the basic properties of the server, including the upstream host. From this tab, you can synchronize a Satellite or flush a cache. You must provide valid RCA Console login credentials to the Satellite server to access this tab.
- **Configuration**: The Configuration tab enables you to configure the "Satellite Configuration Options" on page 253 listed on "Satellite Configuration Options" on page 253. You must provide valid RCA Console login credentials to the Satellite server to access this tab.

Add a Server to Server Pools

You can assign the selected server to an existing Server Pool. To add a server to Server Pools, complete the following steps:

1. Click the **Add Server to existing Server Pool** button on the toolbar. The Server Pool Selection window opens displaying the available Server Pools.
2. Select one or more Server Pools to which you want to add a Server.
3. Click **Add Server to Server Pools**.
4. Click **Close**.

Delete a Server from Server Pools

You can remove the selected server from Server Pool(s). To remove a Server from Server Pools, complete the following steps:

1. Select the Server Pool(s) from which you want to remove the Server.
2. Click the **Remove Server from the selected Server Pool(s)** button on the toolbar. A confirmation pop-up window opens.
3. Click **Yes** to remove the Server.

Synchronize Satellite Servers Service Cache

Each time devices request resources that are not available on the Satellite Server's local cache, the data is retrieved from the RCA Core server. If the Proxy Server dynamic caching is enabled on the Satellite server, the requested data is stored in the cache of the Satellite server, and provided to the client devices.

A Satellite server's service cache can be preloaded with the data required by managed devices. A Satellite server automatically caches data when it is requested by a client device. Using the Synchronize feature, you can preload a Satellite server's cache with all available data on the upstream server.

You can select which data to preload using the Cache tab in the Server Details window (after the Satellite server has been deployed).

Note: Preloading consists of downloading large binary files and therefore may affect overall network performance. When possible, perform synchronizations during off-hours when optimal network performance is not a priority.

To view the current synchronization status of each server, see the **Last Synchronized** column on the Satellite Servers list, or see the Synchronization section on the Cache tab in the Server Details window. **Last Synchronized** area records the last time the synchronize feature was *initiated* on a server.

Note: After a Satellite Server is first synchronized, a new entry is added to the Managed Devices report with an RCA Agent ID of RPS_<DEVICENAME>. This entry exists specifically to display the preload status of the Satellite Server services and does not contain detailed hardware information for the associated device.

Selecting which data to preload

1. After the Satellite Server is deployed, click the Server link in the Satellite Servers list to open the **Server Details** window .
2. Click the **Cache** tab.
3. Use the drop-down lists to enable or disable the services that you want to make available for preloading from the upstream server. By default, preloading is disabled for all services.
4. Click **Save** to commit your changes.
5. Click **Synchronize** to preload the Satellite Server with available data.

Synchronizing Satellite Servers

1. On the Configuration tab, go to the Satellite Management area under Infrastructure Management.
2. On the Servers tab, select the servers that you want to synchronize.
3. Click the **Synchronize the selected Satellite Servers service cache**  toolbar button to update all selected server's with the latest data from the RCA Server. The specific services preloaded to each server depend on the settings configured on the **Cache** tab in each server's Server Details window.

Note: You can also synchronize a Satellite server from the "Server Details Window" on page 285. Alternatively, you can schedule a DTM job using one of the Satellite Synchronization job action templates. See "Create a New DTM or Notify Job" on page 154 for more information.

Viewing a summary of preloaded services in a Satellite server's cache

Open the Server Details window, and click the **Reporting** tab.

The Reporting tab displays the pre-loaded services available in the cache and the status of each.

The **Event** column describes the current status:

- **Update (Preload)** – the service was updated during the last cache synchronization.
- **Install (Preload)** – the service was preloaded successfully (initial preload).
- **Uninstall (Preload)** – the service was removed from the preload cache.
- **Repair (Preload)** – the cache for the service was either missing files or contained invalid files and was repaired during the last synchronization.

Only preloaded services are displayed in the report. Services stored on a Satellite Server through the default method (cached automatically when requested by a managed device) are not displayed.

Delete a Server

If you no longer want a device to be in the RCA device repository, you can delete the device. You may want to perform this operation when a device is no longer part of your environment. When a Server is deleted, it is automatically removed from any Locations or Server Pools to which it may be assigned.

Deleting a device is the reverse of importing devices. See "Importing Devices" on page 145 for more information.

Note: You must explicitly uninstall the Satellite server component from the device *before* removing the device from the RCA device repository. If you delete the device without uninstalling the RCA Satellite Server component, the device will automatically re-appear after a period of time since it is still an active Satellite Server, and will remain a member of the Servers group. See "Installing the Satellite server component" on page 284.

To delete a Server:

1. On the Servers tab, select the devices that you want to remove from the RCA repository.
2. Click the **Delete the Selected Device(s)** toolbar button A confirmation pop-up window opens.
3. Click **Yes** to confirm.
   The devices that you selected are removed from the RCA repository.

Server Pools

The Satellite Management Server Pools tab displays all RCA Server Pools that have been created in your environment. Server Pools are groupings of Servers (Core or Satellites) that will be contacted by devices to resolve policy and retrieve data. Servers can be assigned to Server Pools (a maximum of 30 Servers), and Servers and Server Pools are assigned to "Locations" on page 290 to enable client devices to contact them.

A Server Pool is used to perform software load balancing of client connections. If a grouping of Servers have equal priority to handle client connections, these Servers can be grouped into a Server Pool, which can then be assigned to a Location. Clients randomly contact Servers in the Server Pool, thus distributing the load across the Servers in the pool. For example, if your environment contains three Satellite servers in the US that should be contacted with equal priority by client devices in a particular Location, these Servers can be grouped into a US Server Pool and then assigned to the Location.

By default, the RCA Core Server Server Pool containing the RCA Core server is installed on your system. You cannot delete this Server Pool.

You can use the Server Pools property sheet to view or edit Server Pool properties.

You can use the toolbar buttons on the Server Pools tab to add and remove Server Pools.

Server Pools Toolbar Buttons

Button	Description
	**Refresh Data** – To refresh the list of Server Pools.
	**Show/Hide Filter Input** – To show or hide the Filter input area to restrict the display of Server Pools to only those matching user specified criteria.
	**Create a New Server Pool** – To launch the Server Pool Creation Wizard.
	**Delete the selected Server Pool(s)** – To delete selected Server Pools.

The following sections detail what you can do using the Server Pool property sheet and the toolbar buttons on the Server Pools tab:

- "Create a New Server Pool" below
- "Delete a Server Pool" below
- "Server Details Window" on page 285

Create a New Server Pool

You can create Server Pools and add Core and Satellite Servers to them to create a grouping of Servers that an agent can contact for data and policy resolution.

To create a new Server Pool:

1. Click **Create a New Server Pool**  toolbar button to launch the "Server Pool Creation Wizard" on page 351.
2. Follow the steps in the wizard to create the new Server Pool.
   The Server Pool is added to the Server Pool list on the Server Pools tab.

Delete a Server Pool

You can delete Server Pools when they are no longer needed.

To delete a Server Pool:

1. Select the Server Pools that you want to delete from the Server Pool list using the checkbox in the left column.
2. Click **Delete the selected Server Pool(s)**  toolbar button. A confirmation pop-up window opens.
3. Click **Yes** to confirm.
   The selected Server Pools are removed from the Server Pool list on the Server Pools tab.

Server Pool Details Window

To access the Server Pool Details window, click any Server Pool name link in the Server Pools list on the Server Pools tab.

From the tabs on the Server Pool Details window, you can view detailed information about a Server Pool and perform various server management tasks. The following tabs are available on the Server Pool Details window:

- **Properties**: The Properties tab displays the properties information that you specified in the "Server Pool Creation Wizard" on page 351 when you created this Server Pool. You can edit the properties on this tab.
- **Servers**: The Servers tab displays the Servers that are currently assigned to this Server Pool. You can use the toolbar buttons on this tab to add or remove Servers in this Server Pool.

Add Servers to a Server Pool

To add servers to a Server Pool, complete the following steps:

1. Click the **Add Servers to Server Pool** button on the toolbar. The Server Selection window opens displaying the available Servers.
2. Select one or more Servers to add to this Server Pool. You can add a maximum of 30 servers to a Server Pool.
3. Click **Add Servers**.
4. Click **Close**.
   The selected Servers are assigned to the Server Pool as displayed on the Servers tab.

Remove Servers from a Server Pool

To remove servers from a Server Pool, complete the following steps:

1. Select the Server(s) that you want to remove from this Server Pool.
2. Click the **Remove the Selected Server(s) from this Server Pool** button on the toolbar. A confirmation pop-up window opens.
3. Click **Yes** to remove the Servers.
   The selected Server(s) are removed from the Server Pool as displayed on the Servers tab.

Locations

Use the Locations tab to view existing Locations or to add new Locations in your RCA infrastructure. When you add a new Location, you define the Subnets that form this Location and then assign this Location to an ordered set of Servers or Server Pools. To resolve policies and to retrieve data resources, managed devices connect to Satellite servers based on Subnet assignment to Locations and the priority order of the Servers or Server Pools.

You can use the toolbar buttons on the Locations tab to add or remove Locations.

Locations Toolbar Buttons

Button	Description
	**Refresh Data** – Refresh the list of Locations.
	**Show/Hide Filter Input** – Show or Hide the Filter input area to restrict the display of Locations to only those matching user specified criteria.
	**Create a New Location** – Launch the Location Creation Wizard.
	**Delete the selected Location(s)** – Delete selected Locations.

The Locations list includes information about each Location in your RCA infrastructure, including the description and the geographic information.

The following sections detail the tasks you can complete using the Locations property sheet and the toolbar buttons on the Locations tab:

- "Create a New Location" below
- "Delete a Location" below
- "Location Details Window" on next page

Create a New Location

To create Locations, define Subnets and an ordered set of Servers and Server Pools for each Location.

To create a new location:

1. Click **Create a New Location**  toolbar button to launch the "Location Creation Wizard" on page 352.
2. Follow the steps in the wizard to create the new Location.
   The Location is added to the Location list on the Location tab.

Delete a Location

You can delete Locations from your RCA infrastructure if they are not required.

To delete a location:

1. Select the Locations that you want to delete from the Location list using the checkbox in the left column. You cannot delete the Default Location. Additionally, when you delete a Location, any Subnets assigned to that Location will be reassigned to the Default Location.
2. Click the **Delete the selected Location(s)** toolbar button. A confirmation pop-up window opens.
3. Click **Yes** to confirm.
   The selected Locations are removed from the Location list on the Locations tab.

Location Details Window

To access the Location Details window, click any Location name link in the Locations list on the Locations tab.

From the tabs on the Location Details window, you can view detailed information about a Location and perform various server management tasks.

- **Properties**: The Properties tab displays the properties information that you specified in the "Location Creation Wizard" on page 352 when you created this Location. You can edit the properties on this tab.
- **Connections**: The Connections tab displays the current Server or Server Pool connections for this Location. It enables you to add, import, and remove connections. The devices that are part of Subnets assigned to this Location contact the Servers or Server Pools listed in the priority specified to resolve policy and retrieve resources. The Order column indicates the priority in which the Server or Server Pool will be contacted. The Reorder column arrows enable you to reorder the connections.
- **Subnets**: The Subnets tab displays the Subnets that are currently assigned to this Location. You can use the toolbar buttons on this tab to assign additional Subnets to this Location or remove Subnets from it by reassigning them to a different Location.
- **Devices**: The Devices tab displays the devices that are in this Location. This tab is view only.

Add connections to a Location

You can add new connections to a Location. The agent connections use the resources from the Server or Server Pool you define a connection to. To add connections to a Location, complete the following steps:

1. Click **Add Connection** link. The Location Connection Selection window opens.
2. Select a resource from the available types to assign to this location.
3. Click **Add Connection**.
4. Click **Save**.
   The new connections are added to the Location as displayed on the Connections tab.

Import connections to a Location

You can import connections from an existing Location. The existing connections that are defined for this Location are removed when you import connections. To import connections to a Location, complete the following steps:

1. Click Connections tab.
2. Click **Import Connections**. The Location Selection window opens.
3. Select the Location with the connections you want to import.
4. Click **Import Connections**.

5. Click **Save**.
   The imported connections are added to the Location as displayed on the Connections tab.

Assign additional Subnets to a Location

To assign additional Subnets to a Location, complete the following steps:

1. Click the Subnets tab.
2. Click the **Assign additional Subnets to this Location** button on the toolbar. The Subnet Selection window opens displaying the Subnets that are not already assigned to this Location.
3. Select one or more Subnets to assign to this Location.
4. Click **Assign Subnets to Location**.
5. Click **Close**.
   The selected Subnets are assigned to the current Location as displayed on the Subnets tab.

Reassign Subnets to a different Location

You can reassign the Subnets for the selected Location to a different Location. To reassign Subnets to a different Location, complete the following steps:

1. Click the Subnets tab.
2. Select the Subnet(s) that you want to assign to a different Location.
3. Click the **Assign the selected Subnet(s) to a different Location** button on the toolbar. The Location Selection window opens displaying the other Locations that exist in your environment.
4. Select a Location to which you want to reassign the selected Subnets.
5. Click **Assign Subnets to Location**.
   The selected Subnets are now reassigned to the Location you selected.

Subnets

The Subnets that are known to RCA are displayed on the Subnets tab. RCA Agents communicate their subnet configuration during client connections, enabling the Subnets in your environment to be automatically detected and displayed on the Subnets tab. Subnets can also be manually created, as described in "Create a New Subnet" on next page.

Subnets are subdivisions of the IP network space and contain a network address and subnet mask. Subnets can be created using IPv4 or IPv6. In RCA, Subnets are often represented in Classless Inter-Domain Routing (CIDR) notation. In CIDR notation, the previous example would be displayed as 192.168.1.0/24. Every HPCA Subnet is assigned to a single Location; typically a Location will serve multiple Subnets. For example, you might group together many Colorado Subnets into a Colorado Location. Devices that belong to a particular Subnet will contact the Servers and Server Pools associated with the Subnet's assigned Location to resolve policy and retrieve data.

The Subnets tab displays details such as name and description of the subnet, assigned location, number of devices available on the subnet, and total number of usable hosts. For an IPv6 subnet,

the total number of usable hosts is shown zero. The Subnets tab also allows you to view and edit Subnet properties, create and delete Subnets, and assign Subnets to Locations.

You can use the toolbar buttons on the Subnets tab to add and remove Subnets.

Subnets Toolbar Buttons

Button	Description
	**Refresh Data** – Refresh the list of Subnets.
	**Show/Hide Filter Input** – Show or Hide the Filter input area to restrict the display of Subnets to only those matching user specified criteria.
	**Create a New Subnet** – Launch the Subnet Creation Wizard.
	**Delete the selected Subnet(s)** – Delete selected Subnets.

The following sections detail the tasks that you can complete using the Subnet property sheet and the toolbar buttons on the Subnets tab:

- "Create a New Subnet" below
- "Delete a Subnet" below
- "Subnet Details Window" on next page

Create a New Subnet

Subnets are automatically detected based on device connections, but they can also be manually created. You may want to manually create Subnets to prepare that Subnet for management with RCA. Creating a Subnet manually enables you to assign that Subnet to the appropriate Location before Agents being installed on that Subnet. When Agents are later installed on that Subnet, they will already be associated with the appropriate Location.

As part of Subnet creation, you assign a Subnet to a regional Location. Devices that belong to a particular Location because of Subnet assignment will contact the Servers and Server Pools associated with that Location to resolve policy and retrieve data.

The following procedure explains how to manually create a Subnet.

To create a new Subnet:

1. Click **Create a New Subnet** toolbar button to launch the "Subnet Creation Wizard" on page 353.
2. Follow the steps in the wizard to create the new Subnet.
   The Subnet is added to the Subnet list on the Subnets tab.

Delete a Subnet

You can remove Subnets when they are no longer needed based on changing network configurations within your environment.

Note: You cannot delete a Subnet that contains active devices, as the Subnet will be immediately detected again based on device connections. If you attempt to delete such a Subnet, the Subnet will still appear in the list but will be reassigned to the Default Location. Additionally, the CSDB instance for the Subnet (under PRIMARY.CLIENT.SUBNET) will be deleted.

To delete a Subnet:

1. Select the Subnets that you want to delete from the Subnet list using the checkbox in the left column.
2. Click **Delete the selected Subnet(s)** toolbar button. A confirmation pop-up window opens.
3. Click **Yes** to confirm.
   The selected Subnets are removed from the Subnet list on the Subnets tab.

Subnet Details Window

To access the Subnet Details window, click the link for the Subnet in the Subnet column of the Subnet list.

From the tabs on the Subnet Details window, you can view detailed information about a Subnet.

- **Properties**: The Properties tab displays the properties information that you specified in the "Subnet Creation Wizard" on page 353 when you created this Subnet or that was automatically determined based on Agent connections. You can edit the properties on this tab.
- **Devices**: The Devices tab displays all devices that are located on the selected Subnet. This tab is view only.

Directory Services

Directory Services are used for many things, including the following:

- Running reports based on Active Directory (AD) / Lightweight Directory Access Protocol (LDAP) containers & groups
- Enabling external AD/LDAP sources for authentication to the RCA Console
- Policy assignment – a policy is a designation of the services to which a user, an agent computer, or a managed device is entitled
- OS Management operations
- Agent Notification based on AD/LDAP sources

Radia Client Automation supports two basic policy usage patterns:

- The **normal** pattern enables you to administer policy (for software and patches, for example) stored in an external LDAP directory—such as Active Directory—that you supply. This policy source is used by the Policy Server to drive resolution in the Configuration Server. Policies in the directory are administered by the RCA Console.

In order to perform policy management on an external directory service, you must first update the Schema. See the *Radia Client Automation Enterprise Policy Server Reference Guide* for additional information about configuring your environment to use external directories for policy.

Note: This type of policy is not supported in the internal directory of the Portal. See the *Radia Client Automation Enterprise Portal Reference Guide* for more information.

- The other policy usage pattern supported pertains to **operating system (OS) management**. OS management policies are stored internally in the RCA Portal. In this case, the Portal provides the operational interface to the Configuration Server to support OS resolutions. Policy administration is done using the OS Management features in the RCA Console. See the *Radia Client Automation Enterprise OS Management Reference Guide* for additional details.

Note: OS Management policy is now supported for external LDAP directories.

Navigate the Directory Services Page

Before you can use LDAP policy management, you must first define the LDAP environment to which you are connecting. To do this, you must create and configure a Directory Services object.

To access the Directory Service page, click the **Directory Services** link in the left navigation menu on the Configuration tab.

The following table describes the toolbar buttons available on the Directory Services page. Use these toolbar buttons to manage any existing Directory Services or create new Directory Services.

Directory Services Toolbar Buttons

Icon	Toolbar Button Name	Description
	Refresh Data	Refreshes the Directory Services list.
	Show/Hide Filter Input	Use to show or hide the filter toolbar. You can filter Directory Services data by using a text string and narrow the search by selecting individual Directory Services columns to include in the search.
	New Directory Services	Launches the Directory Services Creation Wizard.
	Start the Selected Directory Services	Use to start an existing Directory Service that is stopped.
	Stop the Selected Directory Services	Use to stop an existing Directory Service that was previously started.

Icon	Toolbar Button Name	Description
	Restart the Selected Directory Services	Use to restart an existing Directory Service.
	Delete the Selected Directory Services	Deletes a Directory Service from the list.

View Directory Service Details

You can view information about any Directory Services objects that have been defined.

To view Directory Service details:

1. From the Configuration tab, click **Directory Services** in the left pane.
2. Click the name of the directory service for which you want to view details or change options.
3. Click the **Summary** tab to see basic information about the directory service. You cannot modify these properties.
4. Click the **Properties** tab to see the **General Settings** and **Connection Settings**. You can modify any of these settings. All parameters marked with an asterisk (*) are required. Click **Save** after making modifications.

Modify Directory Service Property Settings

You can modify the property settings for any Directory Services objects that have been defined.

To modify Directory Service options:

1. From the Configuration tab, click **Directory Services** in the left pane.
2. Click the name of the directory service that you want to change.
3. Click the **Properties** tab to display the directory service options.
4. Click **General Settings** or **Connection Settings** to display the settings that you want to change. All parameters marked with an asterisk (*) are required.
5. Make changes to the settings. To see a list of these settings, see the following topics:
   - "Configure a Connection to the Configuration Server Directory Service" on next page
   - "Configure Connections to External Directory Services" on page 299
6. Click **Save**.
7. Click **Close** to acknowledge the Execution Status dialog. Click the **X** in the upper right corner to close the Property Settings window.

The options for the directory service have changed. Depending on which settings you modify, you may be required to log out of the RCA Console and log back in.

Configure a Connection to the Configuration Server Directory Service

Before you configure a connection to your external directory services, you must first create a connection to the internal Configuration Server Directory Service. This is known as the HPCA-CS connection.

Note: The HPCA-CS connection cannot be used for policy resolution.

The Configuration Server Directory Service connection (HPCA-CS) is a prerequisite for using the RCA Console to administer policy. Be sure to configure this connection first before configuring an LDAP or LDAPS (Secure) connection.

To configure the Configuration Server directory service:

1. From the Configuration tab, click **Directory Services** in the left pane.
2. From the Directory Services detail section, click the  (Create New Directory Service) button. The Directory Service Connection Wizard starts.
3. Specify a Display Name and Description. From the **Type** list, select **HPCA-CS**. Only one HPCA-CS directory service can be created.
4. Click **Next**.
5. Under Connection Settings, you have the following options. All parameters marked with an asterisk (*) are required.
   - For **Startup**, select **Automatic** to automatically start this directory service when the Portal starts.
   - For **Host**, type the host name or IP address of the Configuration Server.
   - For **Port**, type the port number for the Configuration Server. The default is 3464.
   - Use **Service Account ID** to set which account you will use to sign in to the Configuration Server. The Service Account is used for both read and write operations. It must have full read access to this directory source and it must have write access to the top of the tree to which it will be editing.
   - Use **Password** to specify the password for the Service Account ID. Retype the password in the **Confirm Password** text box.
   - Use **Timeout** to specify in seconds the timeout for your connection to your Configuration Server. Keep the default of 120 unless directed to by Persistent Support.
   - Use **Connection Attempts** to specify how many times the RCA Console should attempt to connect to your Configuration Server before failing.
   - Use **Connection Delay** to specify the amount of time in seconds to delay between connection attempts.
6. Click **Next**.

7. Review the Summary screen. If all properties are correct, click **Commit**.
8. Click **Close** to acknowledge the dialog.
   The directory source is added to the Directory Services list.

Configure Connections to External Directory Services

Note: Before you configure a connection to your external directory services, follow the instructions to "Configure a Connection to the Configuration Server Directory Service" on previous page.

You can administer LDAP policies through the RCA Console by assigning Services to Directory Service objects.

Before you can do this, however, you must configure connections to your external directory services. The following types of external directory services are supported:

- Lightweight Directory Authentication Protocol (LDAP)
- LDAP with Secure Sockets Layer (SSL) support (LDAPS (Secure))

If you are using SSL on your LDAP server, then you should use the LDAPS (Secure) type of connection.

Each external LDAP directory service may be used for any combination of:

- Authentication
- Reporting
- Policy Entitlement

For example, suppose that you have two directories. One contains all user accounts, and the other is specifically for policy. You want to authenticate against the user account directory. In this case, you should create two directory services with their connections defined differently:

- Create one directory service for authentication with a connections where:
  - **Used for Authentication** is selected
  - **Used for Policy** is not selected
  - **Use Service Account** is not selected

  Selecting **Used for Authentication** enables users to log in to the RCA Console using their external LDAP directory account for this directory service.
- Create another for policy where:
  - **Used for Authentication** is not selected
  - **Used for Policy** is selected
  - **Use Service Account** is selected

This configuration will enable you to sign in using the first directory service, and configure policy using the second directory service.

Note: Note that if a directory source is configured with **Used for Authentication**, but **Use Service Account** is not selected, users must sign in using their external LDAP directory credentials. If **Use Service Account** is selected, users can sign in using their local RCA Console user name and password.

Configuring LDAP or LDAPS (Secure) Directory Services

1. From the Configuration tab, click **Directory Services**.
2. From the Directory Services detail section, click the  (New Directory Service) button. The Directory Service Creation Wizard starts.
3. Specify a **Display Name** and **Description**.
4. From the **Type** list, select one of the following options:
   - Select **LDAP** if your LDAP server does not use SSL.
   - Select **LDAP (Secure)** if your LDAP server uses SSL.
5. Click **Next**.
6. Enter the required connection parameters. You have the following options. All parameters marked with an asterisk (*) are required.
   - For **Startup**, select **Automatic** to automatically start this directory service, when the Portal starts.
   - **Host** is the fully qualified host name or IP address of the LDAP Server.
   - **Port** is the LDAP Port. For LDAP without SSL, the default value is 389. For LDAP(Secure), the default value is 636.
   - Use **Service Account ID**, to set which account that the RCA Console will use to sign in to the directory services server. The Service Account is used for both read and write operations. It must have full read and write access to this directory source.
   - Use **Password** to specify the password for the Service Account ID. Retype the password in Confirm Password.
   - **Base DN** is used as the root distinguished name (DN) when browsing the directory through the RCA Console.
   - For LDAP(Secure), also specify the following information:
     - Use **CA Certificate Directory** to specify the directory of the SSL certificate. The path is relative to the server where the Portal is located. For example: *<InstallDir>*`\HPCA\ManagementPortal\etc\CACertificates`
     - Use **CA Certificate File** to specify the location of the SSL certificate. The path is also relative to the server where the Portal is located. For example: *<InstallDir>*`\ManagementPortal\etc\CACertificates\`*<LDAP Certificate File Name>*
7. Click **Next**.

8. Enter the required user interface parameters. You have the following options.
   - **Used for Reporting**: When enabled, this directory service becomes enabled in the Reporting tab of the RCA Console as a filter source. The Reporting Server must be configured to use the Portal as its directory source for this feature to work. You can also configure LDAP using the `rrs.cfg` file. For more information, see the *LDAP Configuration* section in the *Radia Client Automation Enterprise Reporting Server Reference Guide*.
   - **Used for Policy**: When enabled, this directory service can be used in the RCA Console for policy management.
   - **Used for Authentication**: When enabled, this directory service becomes enabled as a sign-in option on the RCA Console login screen to allow user authentication based on your existing directory users. The following two parameters will become available.
     - **Authentication Group DN**: This is used as the source for authorized users into the RCA Console. Any user that is a member of this group will be enabled to sign in to the RCA Console. For faster user authentication, you can configure the `AUTH_LEVEL` parameter in the `rmp.cfg` file. For more information on `AUTH_LEVEL`, see *Client Automation Enterprise Portal Reference Guide*.
     - **Use Service Account**: When enabled, all read and write requests for this directory service will use the **Service Account ID** specified in the **Connection Settings**. When disabled, all read and write requests for this directory service will use the signed-on user's credentials.
   - **Leaf Node Filter**: Enter an LDAP-style filter value to filter out nodes with large numbers of data types so that they will not be displayed in the tree navigation view. Objects such as computers and users should be filtered for better usability. Refer to your directory-specific schema to determine the suitable way to filter each node. The following example filters out computers and users:
     ```
     (!(|(objectclass=user)(objectclass=computer)))
     ```
     You can also configure Leaf Node Filtering using the `rrs.cfg` file. For more information, see the *Leaf Node Filtering* section in the *Radia Client Automation Enterprise Reporting Server Reference Guide*.
9. Click **Next**.
10. Review the Summary information. If all properties are correct, click **Commit**.
11. Click **Close** to acknowledge the dialog.

Job Action Templates

Job Action Templates enable you to pre-define parameters used when creating new jobs.

Job Action Templates are managed in the Infrastructure Management area on the Configuration tab. To view the list of available Job Action Templates, click the **Job Action Templates** link in the left navigation menu.

In the Job Action Templates window, the Enabled column indicates whether or not the template is available when you create a new job using the HPCA Job Creation Wizard. Click any template name to edit its parameters, or click the **New Job Action Template** button to create a new template. See "Create a New Template" on next page for detailed instructions.

The following Job Action Templates are provided when you install the RCA Core:

- Audit Connect
- HPCA Nightly Summary
- Patch Connect
- Refresh DTM Schedules
- Satellite Synchronization (All)
- Satellite Synchronization (Configuration)
- Satellite Synchronization (Data)
- Security Connect
- Software Connect
- Usage Connect
- VMware ThinApp Sync

Each of these templates instructs the agent on a target device to connect to the pertinent domain in the CSDB. For example, the Security Connect template causes the agent to connect to the SECURITY domain. This, in turn, forces all services in the SECURITY domain to which the device is entitled to be executed.

Note: Before you can successfully run a Satellite Synchronization or Refresh DTM Schedules job on a client device, the RCA agent on that client must have performed a prior connect operation to the RCA Core.

Create a New Template

Use the following procedure to create a new Job Action Template. To modify an existing template, simply click its name in the Job Action Templates list.

To create a new Job Action Template:

1. From the **Configuration** tab, click and expand **InfrastructureManagement**.
2. Click **Job Action Templates.**
3. Click the **New Job Action Template** button  . The Job Action Template Creation Wizard opens.
4. Select a starting point for your new template. You can select from:
   - Blank Template – enables you to define all of the parameters available.
   - Sample Templates – contain pre-defined parameters depending on the connect type or options selected when the template was created. See "Sample Templates" on page 304.
   - User-Defined Template – contains the settings specified in another template.
5. Click **Next**.
6. Define the parameters for the template. All parameters marked with an asterisk (*) are required.

The **UI Setting** drop-down box associated with some parameters determines whether the parameter is displayed when you create a job with the HPCA Job Creation Wizard.

- **Hidden** will not display the parameter.
- **View Only** will show the parameter in the wizard.
- **View & Edit** will show the job and allow you to modify the parameter.

Display Name: Type a name for the template. This name is displayed on the Job Action Templates page.

Description: Type a detailed description for the template. The description is also displayed on the Job Action Templates page.

Enable Template: Select to enable the template. Enabled templates are available for use when you create a job.

Connection Parameters

These items pertain to the managed client system:

Notify Port: Type the Notify port. The default port is 3465.

Job User ID: Type the Job User ID. This is required if job security is enabled on the client device.

Password: Type the password. This is also required if job security is enabled on the client device. Only asterisks will appear when you type the password.

Action Parameters

These items to pertain to both Notify and DTM jobs:

Service Selection: Select to display a service selection list in the HPCA Job Creation. Only entitled services are included in the list.

Command: Type the command to run on the remote system when the job is executed. This executable is limited to those available in the RCA Agent root folder.

Parameters: Type the parameters for the command.

Additional Parameters: Include any additional parameters for the command. Note that any **Additional Parameters** are combined with the **Parameters** specified.

Job Parameters

Concurrent Process Limit: Type the maximum number of processes allowed for the job. This is the number of “threads” used to process a job—in other words, how many notifies that you want to perform at the same time. The default is 25.

- Use a smaller number for a small network or a risky job
- Use a larger number for a large network

New Process Delay: Type the time (in seconds) to wait between activating new processes for this job. The default value is based on the connect type. Change this value based on the estimated time it will take for the job to complete on a single target system. The valid range is 60-65,535.

You can use this parameter to manage network traffic and avoid over-running (flooding) the network. Allow at least 20 minutes for OS connects and 5 minutes for Software connects.

7. Click **Submit**.

The new template is displayed in the Job Action Templates window. If **Enable Template** was selected, the template will be available when creating a new jobs with the HPCA Job Creation Wizard. See "Managing Jobs" on page 148 for details on using the wizard to create a Notify job.

Sample Templates

Sampletemplates enable you to create a Job Action Template based on pre-defined parameters normally used for particular connect types. The Sample Templates are defined below:

Audit Connect

This template instructs managed clients to connect to the RCA server for the purpose of gathering data used to create the RCA Management Reports.

HPCA Nightly Summary

This template is used to periodically “roll-up” data for a specified group of devices. See "Device Groups for Data Roll-Up" on page 218.

Patch Connect

Patch Connects are used to update the patches entitled to devices.

Refresh DTM Schedules

DTM job schedules can be refreshed by creating a Notify or DTM job and using the Refresh DTM Schedules job action template. See "Refresh DTM Schedules on Targets" on page 155.

Satellite Synchronization (All, Configuration, and Data)

The Satellite Synchronization templates are used to synchronize Satellite servers with the Core server to make the latest data available to the Satellites. See "Creating Satellite Synchronization Jobs" on page 157.

Security Connect

A Security Connect will resolve any security entitlements from the SECURITY Domain.

Software Connect

A Software Connect is used to update the list of software entitled to the group or device.

Usage Connect

Usage connect is used to install the usage agent on the device and begin collecting usage data.

VMware ThinApp Sync

This template instructs a managed device to check with the Core or Satellite server to see if there are any updates to the ThinApp services to which it is entitled.

Multicast

Multicast is the delivery of information to a group of destinations simultaneously using the most efficient strategy, it is used for Operating System image and application delivery.

- To enable Multicast, click the checkbox and then click **Save**.

Live Network

Live Network settings required to communicate with the HP Live Network content server are configured in the Infrastructure Management area on the Configuration tab. See "Configure the Connection to the HP Live Network Server" below.

Live Network updates are configured in the Infrastructure Management area on the Operations tab. See "Live Network" on page 223.

Configure the Connection to the HP Live Network Server

Use the Live Network settings to configure the connection used to automatically download the latest content from HP Live Network and to establish the RSS feed for the "HP Live Network Announcements" on page 98 and the "HP Live Network Patch Manager Announcements" on page 122 dashboard panes. This includes the following items:

- URL for the HP Live Network content server used to download the most recent scanners and data.
- Your HP Passport login credentials.

Note: For your security and convenience, the HP Live Network content server uses HP Passport authentication. HP Passport is a single sign-in service that enables you register with all HP Passport-enabled web sites using a single user ID and password. To set up your HP Passport profile, go to:

http://h20229.www2.hp.com/passport-registration.html

Make sure that your HP Passport profile includes the 12-digit service agreement identifier (SAID) associated with your HPCA support contract. This SAID must include entitlement to HP BSA Essentials so that you can access the HP Live Network content server. For assistance, contact your HP Software sales representative.

Note: Passwords entered on this page are encrypted.

You can test your configuration information before you save it. When you request a test, the RCA Console attempts to connect to the HP Live Network content server. If the connection succeeds, you know that your configuration information is valid. See "Test Your Live Network Settings" on next page for details.

Specifying the HP Live Network connection settings

1. On the Configuration tab, expand the Infrastructure Management area, and click **Live Network**.
2. Specify the following information. All parameters marked with an asterisk (*) are required.
   - **HP Live Network User ID**—your HP Passport user ID.
   - **HP Live Network Password**—your HP Passport password.
   - **HP Live Network Content URL**—the location of the HP Live Network content server for vulnerability definitions and scanners (URL filled in by default).
   - **HP Live Network Connector**—the path to the Live Network Connector executable on the system hosting the RCA Core (path filled in by default).
     For more information, see "Run the HP Live Network Connector Manually" on page 439 and "Download the HP Live Network Connector" on page 129.
3. To test the settings that you have specified, click **Test**. See "Test Your Live Network Settings" below for more information.
4. Click **Save** to implement your changes.

Note: The RCA Console does not automatically save your configuration settings after a successful test. You must click the **Save** button if you want to save your settings.

Note: If you leave this page, any information that you entered in the text boxes before clicking **Save** will be lost. Be sure to click **Save** if you want to keep this information.

Note: You can use the **Reset** button to restore the most recently saved settings.

Test Your Live Network Settings

When you are configuring your Live Network settings, you can test your settings to make sure that they work before you save them.

To run a test, click the **Test** button in the lower right corner of the page. The RCA Console first confirms that all required settings are specified and that all settings have the proper format. It then takes the following actions:

The RCA Console attempts to connect to the HP Live Network content server and log in using the user name and password specified. Any proxy information that appears on the Proxy Settings page in the Infrastructure Management configuration area is used.

Depending on network traffic and other parameters, this test can take up to three minutes. A dialog box asks you whether you want to continue with the test. If you want to continue, click **Yes**.

After the test is completed, the Test Results dialog box shows you the outcome of the test. The following table summarizes the possible outcomes and implications of each.

Live Network Settings Test Results

Icon	Outcome	Explanation and Suggested Action
	Test was successful.	All settings are valid. Save your configuration.
	Test failed.	Here are some of the more common reasons that a test can fail: • A required setting is missing. • A setting is specified using an invalid format (for example, an invalid URL or path). • A setting is spelled incorrectly. • The login credentials for the HP Live Network content server are not valid (for example, if your subscription has expired).
	Unknown	This outcome does not necessarily mean that your configuration information is invalid. It simply means that the test could not be completed. For example, if the RCA Console is unable to connect to the HP Live Network content server within three minutes, the test times out. This can occur for the following reasons: • The server is unavailable. • Network traffic impedes the connection. • A firewall blocks the connection. This outcome can also occur if the connection goes through a proxy server, and either the proxy information specified is not correct or the proxy server blocks the connection.

To troubleshoot a failed or inconclusive test result, check the spelling and format of all the settings on the tab. Also check the `vms-server.log` file for errors.

Note: You must click the **Save** button to save your settings—even if the test is successful. The RCA Console does not automatically save your settings.

Device Management

Use the Device Management section to configure alert options and Thin Client and Remote Control settings.

The following sections describe the available device management options:

- "Alerting" on next page
- "Thin Clients" on page 310
- "Configure Remote Control" on page 310

Alerting

Use the Alerting section to configure CMI and S.M.A.R.T. alerts and reporting options.

- "CMI" below
- "S.M.A.R.T." on page 310

CMI

The CMI Softpaq is installed to each HP targeted device as part of the RCA Agent Deployment. The HP Client Management Interface (CMI) provides enterprise managers and information technology professionals with an increased level of management instrumentation for HP business-class desktops, notebooks, and workstations.

CMI hardware-specific information is captured and available for reporting. Use the **HP Specific Reports** Reporting View in the Display Options section of the Reporting tab to create CMI hardware-related reports. (Select **Inventory Management Reports,Hardware Reports,** then **HP Specific Reports** to view CMI-related reporting options).

The following hardware related alerts are reported using the HP CMI and S.M.A.R.T. Drive Alert Monitoring:

HP CMI and S.M.A.R.T. Runtime alerts

Runtime alerts	Desktop	Workstation	Notebook
BIOS configuration change	x	x	x
BIOS configuration security	x	x	x
Chassis intrusion	x	x	
Fan stall	x	x	
Fan normal*	x	x	
Thermal caution	x	x	
Thermal critical	x	x	
Thermal normal*	x	x	

* Can be indirectly detected by a management console through the absence of a Fan Stall or Thermal Caution/Critical alert.

HP CMI and S.M.A.R.T. Post error alerts

POST error alerts	Desktop	Workstation	Notebook
101-Option ROM Checksum Error	x	x	
163-Time & Date Not Set	x	x	
164-Memory Size Error	x	x	

POST error alerts	Desktop	Workstation	Notebook
214-DIMM Configuration Warning	x	x	
511-CPU fan not detected	x	x	
512-Rear Chassis fan not detected	x	x	
513-Front Chassis fan not detected	x	x	
515-Power Supply fan not detected	x	x	
912-The computer cover has been removed	x	x	
917-Front Audio not connected	x	x	
918-Front USB not connected	x	x	
1720-S.M.A.R.T. Hard Drive detects imminent failure	x	x	
1801-Microcode Update Error	x	x	

For additional CMI information see:

http://h20331.www2.hp.com/Hpsub/cache/284014-0-0-225-121.html

Use the CMI tab to modify HP CMI settings. Modified settings take effect the next time a managed client connects to the RCA infrastructure.

Note: CMI is compatible with only specific HP device models. See your device description for compatibility information.

Configuring CMI

1. In the RCA console click the **Configuration** tab, then select **Device Management**.
2. Click the **Alerting** -> **CMI** option.
3. To report on captured client alerts from managed HP devices, select **Enabled** from the **Report Client Alerts** drop-down list. Alert reporting is disabled by default. The Minimum Severity to Report drop-down list will become available after you select Enabled.
4. Select the minimum alert severity to report.
5. To turn on client alerts for managed HP devices, select **Enabled** from the **Show Client Alerts** drop-down list. Alerts are disabled by default. The Minimum Severity to Display and Alert Window Timeout dialogs will become available after you select Enabled.
6. Select the minimum alert severity to display on the client device.
7. Type the number of seconds an alert should appear on the client device. By default, an alert is displayed for five seconds.
8. Click **Save**.

S.M.A.R.T.

Self-Monitoring, Analysis, and Reporting Technology (S.M.A.R.T.), is a monitoring system for computer hard disks that detects and reports on various indicators of reliability, acting as an early warning system for drive problems. This feature provides information on predictable failures on HP devices caused because of overheating or other wear and tear issues. You can view **S.M.A.R.T. Alerts** reports on Core Console under **Reporting** tab - **Inventory Management Reports** - **Detail Reports**.

As part of the RCA agent, you can enable detection of these events for both display and reporting purposes. S.M.A.R.T. monitoring is disabled by default. Use the RCA Administrator CSDB Editor to enable and configure the S.M.A.R.T. monitoring settings.

To enable and configure S.M.A.R.T. monitoring:

1. Click **Start**>**Programs**>**Radia Client Automation Administrator**>**Radia Client Automation Administrator CSDB Editor**. The logon dialog box opens.
2. Type your User ID and Password. By default, the user name is `ADMIN` and the password is `secret`.
3. Click **OK**. The RCA Admin CSDB Editor window opens.
4. Navigate to PRIMARY.CLIENT.Network Locations (LOCATION).Default.DEFAULT_RADALERT.
5. Set the following parameters to `Y`:
   - `SMRTMON` - Enables you to monitor events
   - `SMRTDISP` - Enables you to display events
   - `SMRTREP` - Enables you to report events

You can now display and report the events generated on the agent computer.

Thin Clients

Thin Client Management service provides Windows CE devices with configuration data. When this service is disabled on a Core, this information will not be available for Satellites or Agents requesting this information.

To enable Thin Client Management, select the check box and then click **Save**.

Configure Remote Control

The RCA Console provides the capability to remotely access devices in either the internal or external repository using Windows Remote Desktop Connection, Virtual Network Computing (VNC), or Windows Remote Assistance.

As the RCA administrator, you can configure the RCA Console to enable any or all of these connection types. You can also disable remote control altogether.

For each type of connection, you must specify the port on which the remote target devices will be listening for the remote connection. See "Requirements for Remote Connections" on page 164 for additional requirements associated with each connection type.

To configure remote control:

1. On the Configuration tab, click **Remote Control** in the left navigation tree.
2. Select the type of connection (or connections) that you want to enable:
   - **Enable VNC (Virtual Network Computing)**
   - **Enable Windows Remote Desktop**
   - **Enable Windows Remote Assistance**
3. For VNC and Windows Remote Desktop, specify the **Port** on which the remote devices will be listening for the remote connection.
   It is not necessary to specify a port for Windows Remote Assistance, because Windows Remote Assistance always uses a Distributed Component Object Model (DCOM) interface on port 135.
4. Click **Save**.
5. Click **Close** to close the Execution Status dialog box.

For information about using the remote control function, see "Controlling Devices Remotely" on page 163.

Patch Management

Use the Patch Management link to enable patch management and define ODBC parameters for your patch database.

Note: This link provides different administrative options depending on whether you are in the Core or Satellite Console.

The current section describes the Patch Management options available from the Core Console Patch Management link. See "Satellite Console Patch Management" on page 334 for a description of the options available on the Satellite Console.

Patch Management options are explained in the following:

Patch Distribution Settings allow you to choose a new, lightweight model for applying Microsoft patches. For details, see the chapter "Patch Management Using Metadata" on page 355.

Database Settings

Patch must be enabled in order for the Patch Management areas of the Console and patch-acquisition facilities to be available.

Use the Database Settings area to enable this feature which will start the Patch Manager service (`HPCA Patch Manager`) and synchronize the Patch database with the Core authoritative CSDB information stored in the Patch Library with the patch information in the SQL database.

Prerequisite

The Patch database must be created and an ODBC connection defined for it. For details, see the *Radia Client Automation Enterprise Installation and Upgrade Guide*.

To enable and configure Patch:

1. Select **Enable** (this will start the **HPCA Patch Manager** service).
2. In the Patch ODBC Settings area, set the following options.
   - **ODBC DSN**: Select the DSN for the Patch SQL database.
   - **ODBC User ID**: Specify the user ID for the DSN.
   - **ODBC Password**: Specify the password that is associated with the ODBC user ID.
3. In the Patch ODBC Settings area, set the following options:
   - **ODBC DSN**: Select the DSN for the Patch SQL database.
   - **ODBC User ID**: Specify the user ID for the DSN.
   - **ODBC Password**: Specify the password that is associated with the ODBC user ID.
4. Click **Save**.

If you modified Patch ODBC Settings, follow the prompts to restart the Patch Manager Service.

Distribution Settings

Use the Distribution Settings area to enable and configure the **Patch Metadata Download** option.

When this option is enabled, the page also displays the related options for **Patch Gateway Operations** settings

These options allow you to patch Microsoft devices using Microsoft Update Catalog with the lightweight acquisition and distribution model. It offers several advantages as discussed in the chapter "Patch Management Using Metadata" on page 355.

Caution: The use of Patch Management using Metadata also *requires* you to **Enable the Download Manager**. To do this, go to the **Configuration > Patch Management > Agent Options** page.

- **Enable Download of Patch Metadata only** Check this box to manage patches using the lightweight, Metadata mechanism.

With this option, only metadata is downloaded and published to the Configuration Server Database, and the patch binary files are downloaded and cached to the Patch Manager Gateway when an Agent requests them or when the Gateway is preloaded.

Caution: If you Enable Patch Metadata downloads, you must also enable and configure the following before running an acquisition:

- Patch Gateway Operations on Core or on Satellite(Required)

- Agent Options: Enable Download Manager (Required)

- Java Patches: Download JDK and JRE patches manually (Required)

Note: When **Enable Patch Metadata downloads** is checked, the Vendor value to acquire patches switches from MICROSOFT to MSFT.

Note: For additional details on configuring your environment and acquiring patches using Metadata download and gateway operations, see "Patch Management Using Metadata" on page 355. Make sure to configure Offline Scanning and set the Download Manager Preload option.

Patch Gateway Operations

The Patch Gateway Operations settings are available if the Patch Metadata Download option is enabled from the Patch Distribution page.

Note: The Patch Gateway Operations discussed in this section are applicable for the Patch Gateway on the Core server only. See "Satellite Console Patch Management" on page 334 for the Patch Gateway Operations available on the Satellite server.

Use these settings to enable the gateway.

Once enabled, additional entries allow you to configure it for caching and managing the patch binaries.

The Patch Gateway is required to use the Patch Metadata Download option for the lightweight patching of Microsoft Agents with one of the Microsoft Update Catalog data feeds.

The role of the Patch Gateway is to download, cache and deliver the actual patch binary data to the Agents when **Enable Download of Patch Metadata only** is turned on. There is an optional Gateway preload option that allows patch binaries to be cached into the gateway on acquisition, as opposed to when they are requested from the agents.

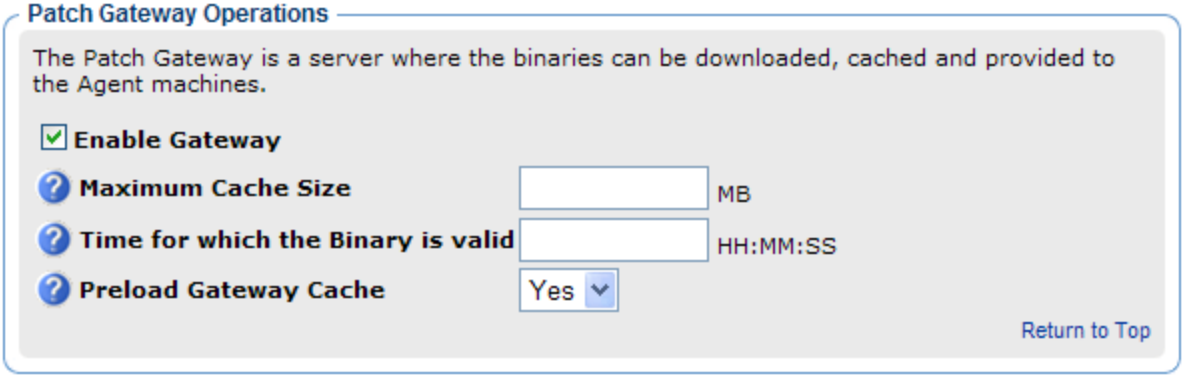
- **Enable Gateway** Check this box to make the Gateway available for on-demand downloading and caching of Microsoft patch binary data.

When Enable Gateway is checked, the following fields are available:

- **Maximum Cache Size** Specifies the maximum size of the Gateway cache in megabytes. Blank or zero means “do not limit the cache”.

Default: 1000 MB

- **Time for which the Binary is valid** Specifies the maximum time, in hours:minutes:seconds format, that the gateway will keep a cached binary file without re-validating it from the upstream server. A value of -1 or blank means the binary will not be refreshed. A value of 10:00:00 means the binary will be downloaded again after 10 hours of being in the cache.
  Default: Blank (no refresh)
- **Preload Gateway Cache** Specify **Yes** (default) to have the patch binaries cached on the Gateway when you run an acquisition. HP cautions you before setting the preload option. The advantage of preloading is that the first agent that requests the patch binary can obtain it without having to first wait for the gateway to download it. However, the disadvantage of preloading is that it results in downloads of all the patch binaries for an acquisition—regardless of whether the agents will need them or not.
  Specify **No** if you want the gateway to download and cache the patch binary data only when it receives Agent requests for the patches. The default setting is Yes.



Agent Options

These Agent Options apply to patching Microsoft devices only.

Use the **Agent Options** available from the **Configuration** tab > **Patch Management** area to enable and configure these Patch Manager Agent options for patching Microsoft Devices.

The next time the Patch Agents connect to the RCA servers they will receive any configuration changes that you set on these panels.

- "Download Manager Options" below
- "Agent Options" on page 316

Download Manager Options

- **Enable Download Manager**: Select this box to download the required patch files onto the Agent machines using a background, asynchronous process. The Download Manager operates outside of the normal RCA Agent Connect process. During a Patch Agent Connect, the following process runs in the background:
  a. Patch Agent Connect verifies if the patch is applicable and entitled to devices.
  b. Patch Agent Connect triggers the Download Manager and queues its download request to Download Manager if the patch is applicable and entitled to devices.

c. Download Manager runs independently and downloads the binaries. If the user turns off the machine or is disconnected from the network during the download, on reboot, the timer ensures that the Download Manager resumes downloading the binary from the point where it stopped. If **Apply patches after download completion** is set to Yes, Download Manager automatically triggers a new Patch Agent Connect.

d. After the binaries are downloaded from the Download Manager, they are installed in the next Patch Agent Connect.

Caution: Download Manager must be enabled to use Patch Distribution using Metadata.

When selected, several Download Manager options are displayed.

Complete the Download Manager Options using the following table:

Download Manager Options for Patch Agents

Option and Valid Values	Description
Network Utilization Values = 0 to 100 % 0 is default	Specifies the maximum percentage of available network bandwidth to download the patch files when the device is active. A value of 0 means the download will use the available network bandwidth. Example: 25 specifies no more than 25% of the available bandwidth should be used for the patch download process.
Network Utilization in Screensaver Mode Values = 0 to 100 % 0 is default	This is a Screen Saver network utilization option. Network Utilization in Screensaver Mode specifies the maximum percentage of available network bandwidth to download the patch files when Screen Saver is on. This is typically a larger percent than when Screen Saver is off. A value of 0 means the download will use the available network bandwidth when Screen Saver is on. Example: 80 increases the bandwidth used to download the patch files by 80% when screen saver is on.
Delay initialization Values = 0 to 999 seconds 0 is default	After initialization, specifies the number of seconds to delay before starting or resuming the download of patches. This allows other processes to startup first, and then resume the patch download. Example: Set to 15 to delay initialization by 15 seconds. A value of 0 means there is no delay.
Apply patches after download completion Values = Yes (default) or No	After download completion, set to 'Yes' to trigger a Patch Agent Connect to apply the patches. It recommends setting the value to Yes. Set to 'No' to have the patches applied when the next Patch Agent Connect is triggered.

Click **Save** to set these configuration options. The Patch Agents will receive the new configuration the next time they connect to the RCA servers.

Agent Options

The following Agent Options are available for patching Microsoft devices.

- **Disable Automatic Updates**: Select Yes or No from the drop-down box. Use this option to address issues whereby the Patch Agent scan or deployment is getting interrupted because Automatic Updates is set to ON.
  - **Yes**: The Patch Agent will disable Microsoft Automatic Updates before each scan or deployment. Once Patch scan/deployment is done, it reverts the Automatic Updates to its original state.
  - **No**: (The default) The Patch Agent will not disable Automatic Updates before each scan or deployment.
- **Delete Software Distribution Folder**: Select Yes, Backup, or No from the drop-down box.
  - Yes: The Patch Agent deletes the contents of the SoftwareDistribution folder before every patch scan. Read the Caution (above) on service restarts.
  - Backup: The Patch Agent first backs up and then deletes the contents of the SoftwareDistribution folder before every patch scan. Read the Caution (above) on service restarts.
  - No: (Default) The Patch Agent will not do anything to the SoftwareDistribution folder.

  This option is available to address the following issues:
  - Drastic growth in the size of the `SoftwareDistribution` folder
  - `SoftwareDistribution` folder corruption
  - Increased load on the Configuration Server during Patch connects

  Caution: Setting **Delete Software Distribution** folder to Yes or Backup automatically restarts the services for Microsoft Automatic Updates and BITS. It warns against setting this option if the service restarts will cause issues in your environment, especially for those customers who are using both RCA Patch Management and Automatic Updates as co-located patch solutions.
- **Manage Installed Bulletins (-mib)**: Select None, No, or Yes from the drop-down box. This option controls how bulletins already installed on the target devices are handled.

Caution: If you do not supply a **-mib** option, the patch agent will behave as if you selected the **-mib Yes** option, which is resource intensive.

- **None: (Recommended)** Manage all installed bulletins except for those that are detected as “no risk” bulletins. This is the recommended behavior since there is no effect on the client agent in terms of vulnerability or re-patching, and it offers greater performance.
- **No:** Manage Patch Manager-installed bulletins only; do not manage bulletins installed by an external source.
- **Yes**: Manage all installed bulletins, whether installed by Patch Manager or an external source. This option is resource intensive.

Click **Save** to set the configuration options. The Patch Agents will receive the new configuration the next time they connect to the RCA servers.

Agent Updates

Use Agent Updates to configure agent updates for Patch Management.

Radia Client Automation Patch Agent Updates

Radia Client Automation Patch Agent Updates are used to acquire and apply maintenance for Radia Client Automation (RCA) Patch Manager agent files. For more information on this, see "Agent Updates" on page 235. The following settings are configured in the Radia Client Automation Patch Agent Updates section.

- **Updates**: If you select Publish, the updates will be published to the PATCHMGR Domain, but will not be connected for distribution (deployment) to Patch Manager target devices. You will need to create these connections. If you select Publish and Distribute, the updates will be published to the PATCHMGR Domain and connected to the DISCOVER_PATCH instance. This option will distribute the updates to your Patch Manager target devices.
- **OS**: Specify the vendor operating system types for which you wish to acquire and manage Patch Manager agent updates.
- **Version**: Select the Patch Manager Version for which you would like to acquire agent updates. You can only publish one version to one Configuration Server. The default is the current installed version.

> **Caution:** If you are installing Patch Manager for the first time, do not modify the Version parameter from the installation default.

Preferences

Under Preferences, configure vendors and acquisition settings. These settings will be reflected in the Vendor Settings and Acquisition Jobs.

- **Enable Patch Management for Vendor(s)**: Specify the OS vendors you will be acquiring patches for. These vendors will be represented in Vendor Settings and Acquisition Settings. If you decide at a later date to acquire patches for additional vendors, they must be enabled here, first.
- **Save Acquisition Summary**: Specify how long in days to keep the Patch Auth Store (PASTORE) instances. This class contains one instance for each patch acquisition session. If this value is smaller than the Save History Detail value, then Save History Detail will be set to the value for Save Acquisition Summary. The value 0 means never delete any history of Patch Acquisition.
- **Save History Detail**: Specify how long in days to keep the Publisher Error (PUBERROR) instances. This class contains one instance for each patch acquisition error.
- **Patch Data Repository Path**: The directory where patches are downloaded to before they are published to the Configuration Server. If you choose to perform an acquisition using a directory that is pre-populated with data from a previous acquisition, specify the pre-populated directory path in this parameter.

- **Retired Bulletins**: Shows the bulletins to retire separated by commas. This parameter works on the bulletin level, not at the product or release level.
  - The Retired Bulletins option performs the following functions:
  - Deletes specified bulletins if they exist in the Configuration Server DB during the current publishing session.
  - Does not publish the bulletins specified in the retire parameter to the Configuration Server DB during the current publishing session. The use of the Retire option supersedes the Bulletins option.
  - Deletes the binaries for the specified bulletins from the Patch Manager Gateway server, if metadata model is used to manage patches.
- **Excluded Products**: Precede any products you want excluded with an exclamation point (!) in the format of *vendor*::*product* in a comma separated list. If an include filter is not set, all products are assumed. If you provide any included filters, then the excluded filters will be a subset of the included products. Be sure to conform to the vendor's naming standards. For example, Microsoft refers to Internet Explorer using its full name, rather than a common abbreviation such as IE. For example, to include all Windows products except Windows 95, type `{Microsoft::Windows*,Microsoft::!Windows 95}`.
  For new Patch Manager installations, the acquisition and management of patches for the following products are *excluded, by default*:

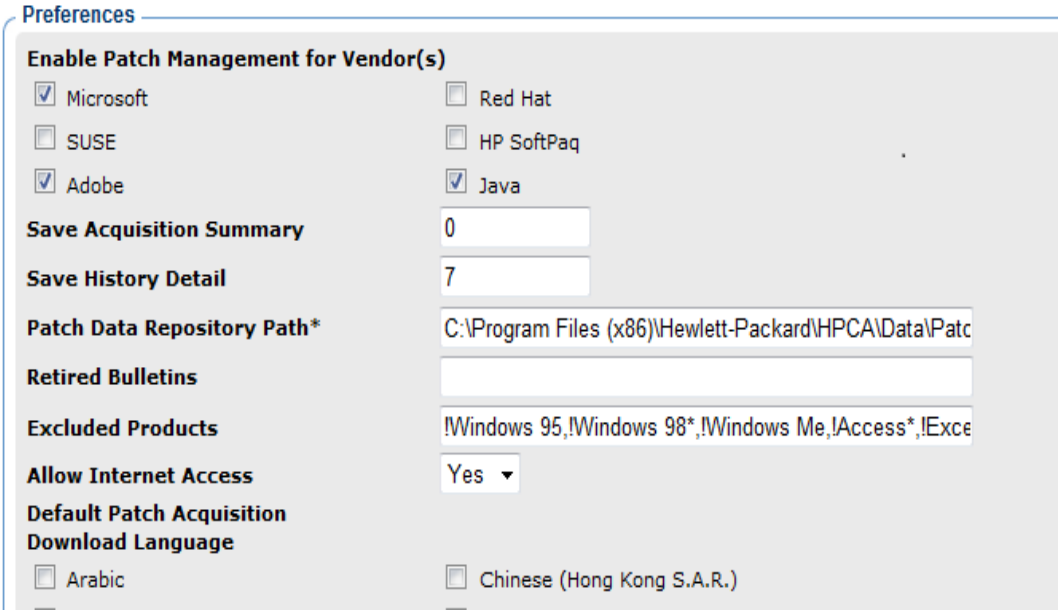
  Security and non-security patches for Microsoft Office, Windows 95, Windows 98, Window Me, and Microsoft Office products.

  Security patches for SuSE specific products *-yast2, *-yast2-*, and *-liby2. The automated management of SuSE OS yast specific products are not supported by Patch Manager.

  Note: If you are migrating from a previous version of Patch Manager and did not remove your `patch.cfg` before migration, if you wish to exclude all Microsoft Office products or their standalone versions from Patch Manager acquisition and management, append the following text to your product exclusion list:

  ```
  ",!Access*,!Excel*,!FrontPage 200[023],!FrontPage
  9[78],!InfoPath*,!Office*,!OneNote*,!Outlook*,
  !PowerPoint*,!Project 200[023],!Project
  98,!Publisher*,!Visio*,!Word*,!Works*"
  ```

  Note the text shown above is all one line and the quotes displayed above are *not* to be included in the user interface Excluded Product text box.



- **Allow Internet Access:** Select Yes or No from the drop-down box. Use this option to specify whether the Patch Manager Server is to be allowed access to the internet.
  - **Yes:** (Default) Patch Manager will access the internet during acquisitions.
  - **No:** Patch Manager will not access the internet during acquisitions. In this case, only the bulletins (metadata and binaries) that already exist in the data folders are published.
- **Default Patch Acquisition Download Language**: Specify the languages for which you want to acquire and manage security and non-security patches. Note that only Microsoft non-security patches are supported. The default is en (English).

Vendor Settings

Vendor Settings displays vendor-specific URLs and other options required for patch acquisition and management activities on the agents in your enterprise.

Before entering Vendor Settings, first use the Preferences page to enable the appropriate vendor(s) and OS selections.

Caution: If you change vendor settings from one acquisition session to the next so that you exclude one or more products or operating systems that were previously selected, all patches specific to the excluded products or operating systems will be removed from the Configuration Server Database. This also means the excluded products or operating systems are no longer eligible for vulnerability assessment and management. This applies to all vendors.

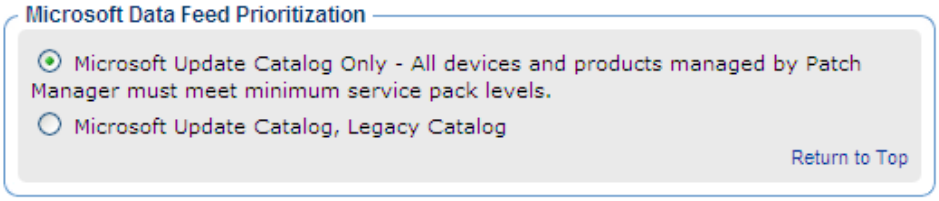
Vendor Settings

- "Microsoft Data Feed Prioritization" on next page
- "Red Hat Feed Settings" on page 321
- "SuSE Feed Settings" on page 323

- "HP SoftPaq Feed Settings" on page 326
- "Adobe Settings" on page 333
- "Java Settings" on page 333

Microsoft Data Feed Prioritization

The following Microsoft Data Feed Prioritization settings are configured in the Vendor Settings section to support and prioritize the available Microsoft update repositories and methods for acquisition and download.



Note: For more information on Microsoft patch management activities, see the Patch Acquisition chapter in the *Radia Client Automation Enterprise Patch Management Reference Guide*.

- **Microsoft Update Catalog Only**: (Default option) All patches are acquired from the Microsoft Update Catalog. To use this option, all devices in the enterprise must meet minimum operating system and product levels as set by Microsoft. Devices not meeting these minimum requirements will not be patched.
  If you change to this option, a warning message will open indicating the following:

  "The Microsoft Update Catalog Only feed was selected. Only select this option if ALL managed devices in your enterprise meet minimum operating system and service pack levels supported by Microsoft Update Catalog."

  Click **Yes** to acknowledge the warning and Click **Save** to confirm.
- **Microsoft Update Catalog, Legacy Catalog**: Patches are acquired from the Microsoft Update Catalog and an HP repository containing current HP-corrected metadata, referred to as the Legacy Catalog. If a patch exists in both the Microsoft Update Catalog and the Legacy repository, then:
  - If the target device meets the minimum OS requirements supported by Microsoft Update Catalog, the device will be patched by leveraging Microsoft Update Catalog and Windows Update Agent technologies.
  - If the target device does not meet the minimum OS requirements supported by Microsoft Update Catalog, the device will be patched using metadata hosted in the Legacy Catalog.

Note: Patches hosted in the HP Legacy Catalog may require HP metadata correction. If you choose to enable the **Microsoft Update Catalog, Legacy Catalog** option Microsoft security bulletins deemed applicable to legacy Microsoft Operating systems (including Service Pack variants) and Microsoft products will have a "_L" appended to the Microsoft bulletin name for identification purposes within the Configuration Server PATCHMGR Domain as well as

Patch Manager reports as viewed through the Reporting Server.

Caution: Office patches that are acquired and managed using Microsoft Update Catalog technologies will not detect if Office Applications are managed by Radia Client Automation Application Self-service Manager or an Administrative Control Point. In either case, if a bulletin affecting an Office application is entitled to a device, Patch Manager will manage the Office patch and install it locally on the devices that are vulnerable.

Microsoft Feed Settings

The following settings are configured in the Vendor Feeds section:

Basic and Advanced Fields

- **Architecture**: Select the architectures for the acquisition of Microsoft patches. The supported architectures include:
  - **x86** for 32-bit Intel architectures
  - **x64** for AMD64 or Intel EM64T.

Red Hat Feed Settings

The following settings are configured in the Red Hat Feed section:

Advanced-only Fields

- **Red Hat**: Specifies the URL for the Red Hat Network data feed. The default is http://xmlrpc.rhn.redhat.com/XMLRPC.

Basic and Advanced Fields

- **Publish Package Dependencies**: Specify **yes** if you want to publish additional Red Hat packages that downloaded security advisories may depend on. The default is No. Prerequisite, or dependent, Red Hat packages required to install Red Hat Security Advisories can be acquired from two places. They can either be downloaded from the Red Hat Network during acquisition or they can be found locally if previously copied from the Red Hat Linux installation media. During an acquisition, Patch Manager will first look for the .rpm packages in the appropriate directory. For example:

  For Red Hat Enterprise Linux 4ES on x86, place the baseline operating system rpm files supplied on Red Hat installation media in `Data\PatchManager\Patch\redhat\4es`.

  For Red Hat Enterprise Linux 4ES on x86-64, place the baseline operating system rpm files supplied on Red Hat installation media in `Data\PatchManager\Patch\redhat\4es-x86_64`.

  When naming the `Data\PatchManager\Patch\redhat\packages` subdirectories, refer to the list of **OS Filter Architecture** values. Use the applicable folder name based on the value following `REDHAT::` as the subdirectory name.

If a patch's prerequisite software is not found locally, then the package will be downloaded from the Red Hat Network. To decrease the time needed for acquisition, it recommends copying the dependency packages to the appropriate packages directory from your Linux installation media. The Red Hat RPM packages can be found on the Linux installation media under the `RedHat/RPMS` directory.

- **OS Filter**: Support is provided for x86 (32-bit Intel) and x86-64 (Opteron/EMT64) architectures for: all combinations of Red Hat Version 4 and Releases AS, ES and WS, all combinations of Red Hat Version 5 Releases for Servers and Clients, and all combinations of Red Hat Version 6 Releases for Servers and Clients. For a given architecture, select the operating system and release combination for the acquisition of Red Hat patches.
  - **x86** Architectures: Possible values for Red Hat x86 architectures in the `patch.cfg` file are:
    `REDHAT::4as, REDHAT::4es, REDHAT::4ws,`

    `REDHAT::5server, REDHAT::5client,`

    `REDHAT::6server, REDHAT::6client`
  - **x86-64** Architectures: Possible values for Red Hat x86-64 architectures in the `patch.cfg` file are:
    `REDHAT::4as-x86_64, REDHAT::5server-x86_64,`

    `REDHAT::4es-x86_64, REDHAT::5client-x86_64,`

    `REDHAT::4ws-x86_64, REDHAT::6server-x86_64,`

    `REDHAT::6client-x86_64`

Adobe Feed Settings

The following settings are configured in the Adobe Feed section:

Basic and Advanced Fields

- **Adobe Products**: Select the Adobe products for which you want to acquire the patches. Currently, Adobe Acrobat (versions 8, 9, and 10), Adobe Reader (versions 8, 9, and 10), and Adobe Flash Player (versions 8 and 9) are supported.
- **Architecture**: Select the architectures for the acquisition of Adobe patches.
  - **x86** for 32-bit Intel architectures
  - **x64** for AMD64 or Intel EM64T

x86 and x64 are applicable for Adobe Flash Player only. For Adobe Acrobat and Adobe Reader, same patches can be installed on x86 and x64 platforms.

Java Feed Settings

You must download the Java patches manually. To download the Java patches:

1. Create a folder on the RCA Core server for storing the Java patch files. For example, `C:\JavaPatches`. You can choose to have this location on your network, an ftp server, or an

http server.

2. Create sub-folders, `JDK` and `JRE` under `C:\JavaPatches` to download the respective JDK and JRE patches.

The following settings are configured in the Java Feed section:

Basic and Advanced Fields

- **Java Products**: Select the Java products for which you want to acquire the patches. Currently, Java Runtime Environment (versions 1.6 and 1.7) and Java Development Kit (versions 1.6 and 1.7) are supported.
- **Architecture**: Select the architectures for the acquisition of Java patches.
  - **x86** for 32-bit Intel architectures
  - **x64** for AMD64 or Intel EM64T
- **Java Patch Location**: Specify the location where you have already downloaded the JDK and JRE patches. For example: `C:\JavaPatches`. You can also specify a network file system path, an http location, or an ftp location.

If you have not downloaded Java patches earlier. Perform the following steps to download the patches.

1. Click the **Click here to download Java patches manually** link. A list of available Java patches appears.
2. Click the JDK and JRE bulletin you want to download. It opens the Oracle site for Java downloads.
3. Save the bulletins at respective locations. For example, `C:\JavaPatches\JDK` or `C:\JavaPatches\JRE`.

After completing the download process, specify the location where you have downloaded the patches in the **Java Patch Location** text box. The location in this example is `C:\JavaPatches`.

SuSE Feed Settings

To configure settings for patching SuSE Linux, choose the SuSE Feed Setting for the Version Levels and OS platforms that are in your environment. SuSE 9 feed settings are entered separately from SuSE 10 and 11 feed settings. SuSE 10 and 11 feed settings also include a Product Type selection for Enterprise Desktop and Enterprise Server.

Switch from the Basic to Advanced settings if you also need to set or fix the URLs for the SuSE meta data feeds.

SuSE 9 Feed Settings

Click **Advanced** to view or modify the default URLs for SuSE 9 feed settings that are listed below.

Advanced-only Fields

- **SuSE 9**: Specifies the secure URL to acquire security advisory metadata for SuSE 9. The defaults are:
  https://you.novell.com/update/i386/update/SUSE-CORE/9/
  https://you.novell.com/update/i386/update/SUSE-SLES/9/
- **SuSE 9-x86_64**: Specifies the secure URL for acquiring updates for SuSE 9 on AMD64 or Intel EM64T architectures. The defaults are:
  https://you.novell.com/update/x86_64/update/SUSE-CORE/9/
  https://you.novell.com/update/x86_64/update/SUSE-SLES/9/

Basic and Advanced Fields

Use the Basic or Advanced page to type the required settings for getting SuSE 9 Data Feeds.

- **UserID**: Specifies your SuSE user ID. Obtain a user id from the vendor.
- **Password**: Specify the password for the SuSE UserID.
- **OS Filter**: Select the operating system version and architecture combinations for the acquisition of SuSE Linux Enterprise Server patches. Support is provided for SuSE Versions 9 on x86 (32-bit) architecture as well as x86-64 (AMD64 and Intel EM64T) architectures.
  The valid OS Filter value for x86 architectures in `patch.cfg` is `suse::9`.

  The valid OS Filter values for x86-64 architectures in `patch.cfg` is `suse::9-x86_64`.

SuSE 10 and 11 Feed Settings

Use the field on the **Basic** view to type the required feed settings to acquire security advisory patches for SuSE 10 and 11 devices.

Click **Advanced** to view or modify the default URLs for SuSE 10 and 11 feed settings that are listed below.

Advanced-only Fields

- **SUSE 10**: Specifies the secure URL to acquire security advisory meta data for SUSE 10 (SLES10 and SLED10) on x86 architectures.
  Defaults:
  https://nu.novell.com/repo/\$RCE/SLES10-Updates/sles-10-i586/
  https://nu.novell.com/repo/\$RCE/SLED10-Updates/sled-10-i586/
- **SUSE 10SP1:** Specifies the secure URL for acquiring updates for SUSE 10 (SLES10 and SLED10) Service Pack 1 on x86 architectures.
  Defaults:
  https://nu.novell.com/repo/\$RCE/SLES10-SP1-Updates/sles-10-i586/
  https://nu.novell.com/repo/\$RCE/SLED10-SP1-Updates/sled-10-i586/
- **SUSE 10SP2**: Specifies the secure URL for acquiring updates for SUSE 10 (SLES10 and SLED10) Service Pack 2 on x86 architectures.
  Defaults:
  https://nu.novell.com/repo/\$RCE/SLES10-SP2-Updates/sles-10-i586/
  https://nu.novell.com/repo/\$RCE/SLED10-SP2-Updates/sled-10-i586/

- **SUSE 10-x86_64**: Specifies the secure URL to acquire security advisory meta data for SUSE 10 (SLES10 and SLED10) on x86-64 architectures.
  Defaults:
  https://nu.novell.com/repo/\$RCE/SLES10-Updates/sles-10-x86_64/
  https://nu.novell.com/repo/\$RCE/SLED10-Updates/sled-10-x86_64/
- **SUSE 10SP1-x86_64:** Specifies the secure URL for acquiring updates for SUSE 10 (SLES 10 and SLED 10) Service Pack 1 on x86-64 architectures.
  Defaults:
  https://nu.novell.com/repo/\$RCE/SLES10-SP1-Updates/sles-10-x86_64
  https://nu.novell.com/repo/\$RCE/SLED10-SP1-Updates/sled-10-x86_64/
- **SUSE 10SP2-x86_64**: Specifies the secure URL for acquiring updates for SUSE 10 (SLES 10 and SLED 10) Service Pack 2 on x86-64 architectures.
  Defaults:
  https://nu.novell.com/repo/\$RCE/SLES10-SP2-Updates/sles-10-x86_64/
  https://nu.novell.com/repo/\$RCE/SLED10-SP2-Updates/sled-10-x86_64/
- **SUSE 10SP3:** Specifies the secure URL for acquiring updates for SUSE 10 (SLES10 and SLED10) Service Pack 3 on x86 architectures.

  https://nu.novell.com/repo/\$RCE/SLES10-SP3-Updates/ sles-10-i586/
  https://nu.novell.com/repo/\$RCE/SLED10-SP3-Updates/ sled-10-i586/
- **SUSE 10SP3-x86_64:** Specifies the secure URL for acquiring updates for SUSE 10 (SLES 10 and SLED 10) Service Pack 3 on x86-64 architectures.
  Defaults:
  https://nu.novell.com/repo/\$RCE/SLES10-SP3-Updates/ sles-10-x86_64/
  https://nu.novell.com/repo/\$RCE/SLED10-SP3-Updates/ sled-10-x86_64/
- **SUSE 11**: Specifies the secure URL to acquire security advisory meta data for SUSE 11 (SLES11 and SLED11) on x86 architectures.
  Defaults:
  https://nu.novell.com/repo/\$RCE/SLES11-Updates/sle-11-i586/
  https://nu.novell.com/repo/\$RCE/SLED11-Updates/sle-11-i586/
- **SUSE 11SP1**: Specifies the secure URL for acquiring updates for SUSE 11 (SLES11 and SLED11) Service Pack 1 on x86 architectures.
  Defaults:
  https://nu.novell.com/repo/\$RCE/SLES11-SP1-Updates/ sles-11-i586/
  https://nu.novell.com/repo/\$RCE/SLED11-SP1-Updates/ sled-11-i586/
- **SUSE 11-x86_64**: Specifies the secure URL to acquire security advisory meta data for SUSE 11 (SLES11 and SLED11) on x86-64 architectures.
  Defaults:
  https://nu.novell.com/repo/\$RCE/SLES11-Updates/sle-11-x86_64/
  https://nu.novell.com/repo/\$RCE/SLED11-Updates/sle-11-x86_64/
- **SUSE 11SP1-x86_64**: Specifies the secure URL for acquiring updates for SUSE 11 (SLES 11 and SLED 11) Service Pack 1 on x86-64 architectures.
  Defaults:
  https://nu.novell.com/repo/\$RCE/SLES11-SP1-Updates/ sles-11-x86_64/
  https://nu.novell.com/repo/\$RCE/SLED11-SP1-Updates/ sled-11-x86_64/

Basic and Advanced Fields

Use the Basic or Advanced page to type these required settings for getting SuSE 10 and 11 Data Feeds. SuSE Versions 10 and 11 support includes two product types: Enterprise Server and Enterprise Desktop.

Note: All combinations of Product Type and OS Filters selected on this page will be available for SuSE acquisitions. Before running an acquisition, you can use the Exclusion option to omit any combinations that you do not want to acquire.

- **Product Type**: For SUSE 10 or 11, select the SUSE Linux product types installed on the devices in your environment.
  - **Enterprise Server:** Specifies the SUSE Linux Enterprise Server (SLES) product type. To obtain SLES 10 or SLES 11 security advisories, check the Product Type of Enterprise Server.
  - **Enterprise Desktop:** Specifies the SUSE Linux Enterprise Desktop (SLED) product type. To obtain SLED 10 or SLED 11 security advisories, check the Product Type of Enterprise Desktop.
- **UserID**: Specifies your SUSE 10 or SUSE 11 user ID. Obtain a user id from the vendor. For details, see "SuSE Requirements for Patch Management" on page 328.
- **Password**: Specify the password for the SUSE UserID.
- **OS Filter**: Select the operating system *version*, *service pack* and *architecture* combinations for the acquisition of SUSE Version 10 and 11 patches. Support is provided for:
  - SUSE Version 10 base and Service Packs 1, 2, and 3 on x86 (32-bit) architectures, as well as SUSE Version 10 base and Service Packs 1, 2, and 3 on x86-64 (AMD64 and Intel EM64T) architectures.
  - SUSE Version 11 base and Service Packs 1 on x86 (32-bit) architectures as well as SUSE Version 11 base and Service Packs 1 on x86_64 (AMD64 and Intel EM64T) architectures.

Valid SUSE 10 OS Filter values for x86 architectures in patch.cfg are:
`suse::10, suse::10SP1, suse::10SP2,` and `suse::10SP3.`

Valid SUSE 10 OS Filter values for x86-64 architectures in patch.cfg are:
`suse::10-x86_64`, `suse::10SP1-x86_64, suse::10SP2-x86_64,` and `suse::10SP3-x86_64.`

Valid SUSE 11 OS Filter values x86 architectures in patch.cfg are:
`suse::11`, `suse::11SP1.`

Valid SUSE 11 OS Filter values for x86-64 architectures in patch.cfg are:
`suse::11-x86_64, suse::11SP1-x86_64.`

HP SoftPaq Feed Settings

The following settings are configured in the HP SoftPaq Feed section. Click **Advanced** to see all fields, including the HP SoftPaq URL field, click **Basic** to return to the Basic page.

Use the predefined job named `hpsoftpaq` to acquire the HP Softpaqs for the SysIDs and Bulletins specified here. The `hpsoftpaq` job is listed with the available jobs on the **Start Acquisition** operation.

Advanced field

- **HP SoftPaq URL**: Specifies the URL for the HP SoftPaq data feed. Default: http://h50203.www2.hp.com/hpapps/onlineDiag/ActiveCheck.
- **HP SoftPaq ActiveCheck URL**: Specifies the URL for the HP SoftPaq ActiveCheck data feed. Default: http://h50203.www2.hp.com/hpapps/onlineDiag.

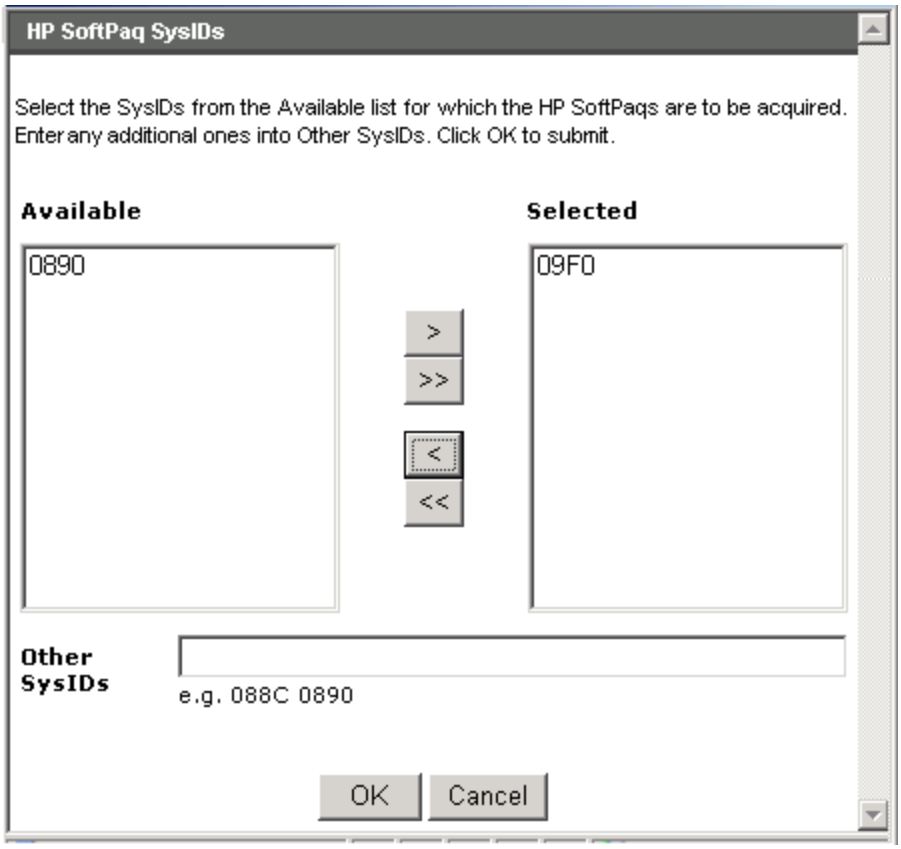
Basic and Advanced fields

- **HP SoftPaq Types**: Check the types of HP SoftPaqs to acquire and manage.
  - Application
  - Bios
  - Driver
  - Firmware
- **SysIDs:** Specifies the SysIDs that will be acquired for HP SoftPaqs.
  If your HP devices have reported inventory information to the RCA database, SysIDs can be selected from a list using the Get SysIDs button:
  Click **Get SysIDs** button. This opens the HP SoftPaq SysIDs dialog box. The Available column lists any HP SoftPaq SysIDs reported from your HPCA-inventoried HP devices.

  Use the arrow buttons to move individual SysIDs from the **Available** column to the **Selected** column. SysIDs in the Selected column will be acquired.

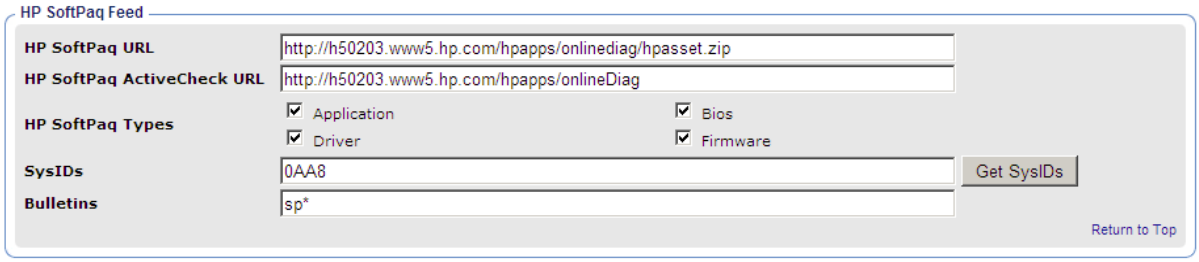
  Optionally, use the **Other SysIDs** text area to type space-separated SysIDs not already listed in the Selected column. For example, enter:
  ```
  0890 8844 30A4 300F
  ```

  Click **OK** to return to the Vendor page for HP SoftPaq.



The **SysIDs** list will show the 'Selected' plus 'Other SysIDs' entries from the HP SoftPaq SysIDs dialog box.

- **Bulletins:** HP SoftPaqs are acquired using the pre-defined acquisition job, named hpsoftpaq. Use the Bulletins area to type the bulletins to be acquired when the hpsoftpaq job is run. To acquire all bulletins for the SysIDs, enter:
  SP*.



Click **Save** to save your Vendor settings.

A job to acquire HP Softpaqs is predefined. To run it, select **hpsoftpaq** from those listed within the **Start Acquisition** operation.

SuSE Requirements for Patch Management

SuSE feed settings require a secure (SSL) connection and a Vendor-supplied User ID and password, as discussed in this topics.

Note: SuSE 10 and SuSE 11 devices have additional requirements; see "SuSE 10 and SuSE 11 Registration Requirements" below.

- **SSL:** The Novell website requires a secure (SSL) connection for patch acquisition. The need for a secure connection within Patch Management is only required on the server that is used to perform secure patch downloads from the Novell website. At the time of this writing, the Novell website does not require or perform certificate validation.
- **SuSE Linux Vendor User ID and password:** The requirements for getting a Vendor User ID and password vary by SuSE Version number.
- **SuSE 9:** For SuSE 9 security patch acquisition, you must establish a User ID and password through your SuSE Linux vendor to access SuSE Internet resources. Specify these credentials when you configure SuSE devices for Patch Management using the Console's **Configuration tab > Patch Management > Vendor Settings** page.
- **SuSE 10 and SuSE 11:** For SuSE 10 and SuSE 11 security patch acquisition of SLES10, SLED10, SLES11 or SLED11 patches, you must establish mirror credentials through your SuSE 10 or SuSE 11 Linux vendor to access SuSE 10 or SuSE 11 Channels. Specify these credentials when you configure SuSE for Patch Management using the Console's **Configuration tab > Patch Management > Vendor Settings** page.

Obtaining SuSE 10 or SuSE 11 mirror credentials

1. Establish the username and password for login to the Novell Customer Center (NCC) through your SuSE Linux vendor when the SuSE 10 or SuSE 11 product is bought.
2. Login to the NCC using the login account information given by the vendor when the SuSE 10 or SuSE 11 product was bought.
3. Click on **Mirror Credentials** under the **Myproduct** link in the left panel.
   In the Credentials area of the Mirror Credentials page, you will see the Username and Password. In the Channels area, you will see the SuSE 10 or SuSE 11 Channel details.
4. Use the Username and Password obtained from the above steps when completing the User ID and password credentials for SuSE 10 or SuSE 11 Patch Acquisition. See the Vendor Settings topic for configuring "SuSE 10 and SuSE 11 Registration Requirements" below.

SuSE 10 and SuSE 11 Registration Requirements

Starting with SuSE 10 and onwards, Novell's explicit policy states that to receive security patches and updates, each SuSE agent Operating System must be registered with Novell and have their licenses managed and validated either directly through the Novell Customer Center (NCC) or Subscription Management Tool.

Note: RCA Patch Management does not validate that Novell's license or registration policy is met for SuSE 10 or above systems. It is the customer's responsibility to adhere to Novell's policy and have their SuSE10 and SuSE11 machines registered with validated licenses.

Registering your SuSE 10 or SuSE 11 systems with the Novell Customer Center

Go to the Novell website for details on registering your SuSE 10 and SuSE 11 systems with the Novell Customer Center.

As of this writing, the topic *Registering and Updating SUSE Linux Enterprise 10* is available at:

http://www.suse.com/products/register.html

On Reboot Requirement for Linux Patches

Reboot is not required when applying application patches to Linux machines. However, a reboot is required when you apply any kernel-related Linux patches. As of now, Radia Patch Management does not support the automatic rebooting of Linux machines when a kernel patch is installed. It is the user's responsibility to reboot manually whenever a kernel patch is installed.

Acquisition Jobs

Use the Acquisition Jobs section to configure patch acquisition schedules and settings.

To create and run Patch Management acquisition jobs, use these areas of the Console:

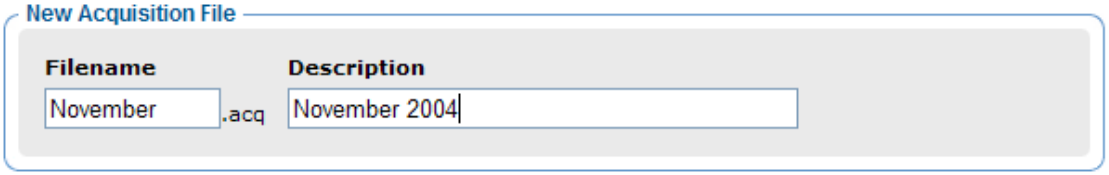
- Use the Configuration tab, Infrastructure Management area to type any necessary HTTP and FTP Proxy settings.
- Use the Configuration tab, Patch Management area, Acquisition Jobs task to define the Acquisition Jobs.
- Use the Operations tab, Patch Management area, Start Acquisition task to run the jobs.

Note: It recommends acquiring from only one vendor at a time. In addition, some SuSE Security Advisories and Microsoft Office Security Bulletins may take an extended period of time to download.

The acquisition job settings that are required depend on your environment.

Creating or Editing an Acquisition Profile using the Console

1. From Configuration, click **Patch Management,** then **Acquisition Jobs**.
2. Either select an existing file to edit, or click **New** to create a new file. Click the trashcan icon to delete an acquisition file. In this example, we click **New**.



3. If you are creating a new file, type a Filename and Description, then click **Next**.
4. You will be taken to Step 2, where you can complete Acquisition Settings for the new job.

- **Acquisition File Description**: Create a description for the acquisition file.
- **Bulletins**: Specify the bulletins for acquisition separated by commas. The asterisk (*) wildcard character is recognized. For Red Hat Security advisories, use a hyphen (-) in place of the colon (:) that appears in the Red Hat Security advisory number as issued by Red Hat.

  Note: If you do not want to download any bulletins, type `NONE` in the Bulletins field.

  - Microsoft Security bulletins use the naming convention `MS`*YY*-###, where *YY* is the last two digits of the year that the bulletin was issued and *CCYY*:###, where *CC* indicates the century and *YY* the last two digits of the year when the advisory was issued, and ### the Red Hat patch number. However, because the colon is a reserved character in products, you must use a hyphen (-) in place of the colon (:) that appears in the Red Hat-issued Security advisory number. Specify individual Red Hat Security advisories to Patch Management using the modified naming convention of **RHSA-***CCYY*-###.
  - Adobe Security bulletins use the naming convention `APSBYY-##`, where `YY` is the last two digits of the year that the bulletin was issued. You can see all Adobe bulletins at http://www.adobe.com/support/security/.
  - Adobe Flash Player uses a static bulletin name as `APSB-FLASH-PLAYER`. Use this name if you want to download security updates for Adobe Flash Player.
  - Java updates use the naming convention `<Java product>-#-#-UPD-##`, where Java product is JDK or JRE, `#-#` is the version of the Java product, and `##` is the serial number. Example, `JDK-1-7-UPD-33`. You can see all Java bulletins at http://www.oracle.com/technetwork/java/javase/downloads/index.html.
  - SuSE Security patches use version-specific naming conventions identified below.
    Use a comma to separate multiple SuSE patch entries (regardless of version). Do not use a space to delimit multiple entries; it will not be accepted.
    - For SuSE 9, use `SUSE-PATCH-####`, where the prefix `SUSE-` is followed by the SuSE 9 patch metadata filename. For example: `SUSE-PATCH-1234`
    - For SuSE 10, use `SUSE-PATCH-platformrel-package-####`, where the prefix `SUSE-` is followed by the SuSE 10 patch metadata filename. For example: `SUSE-PATCH-SLESP1-MOZILLAFIREFOX-1234`

> **Note:** As the instance field length in the CSDB is limited to 32 characters, all SuSE 10 bulletins will be published using HP-reformatted instance names that are shorter and easier to distinguish than the actual SuSE 10 bulletin names. The reformatting drops the SUSE-PATCH prefix and reorders the remaining content to move the unique numbering scheme earlier in the format.

- For SuSE 11, use `UPDATEINFO-platformrel-package-####`, where the entry reflects the entire `UPDATEINFO*.xml` filename for the Suse 11 patch without the `.xml` extension. For example: `UPDATEINFO-SLESSP0-MOZILLAFIREFOX-1234`.

> **Caution:** If the SuSE 11 filename contains a comma, you must replace it with a dash (-) when entering the bulletin name to be acquired. The comma is the reserved character to delimit multiple bulletins.

> **Note:** All SuSE 11 patch names are automatically reformatted into shorter, unique names when they are published to the PRIMARY.PATCHMGR domain of the CSDB.

- **Mode**: Specify BOTH to download the patches and the information about the patches. Specify MODEL to acquire only the metadata for patches. Only the Bulletins and Numbers for the patches are downloaded, but not the actual patch files. Use this mode so that you can use the reports to expose vulnerabilities on managed devices.
- **Force**: Use force in the following situations.
  - You previously ran an acquisition using the mode MODEL, and now you want to use BOTH.
  - You previously ran an acquisition filtering for one language (lang), and now, you need to acquire bulletins for another.
  - You previously ran an acquisition specifying one product, and, now, you need to acquire for another.

  For example, suppose that originally you had only Windows XP computers in your enterprise, so you used `-product {Windows XP*}`. A month later, you roll out Windows Vista. If you want to acquire the same bulletins, you will need to run the acquisition with `-product {Windows Vista*,Windows XP*}` and `-force y`.

  If replace is set to `Y`, the bulletins will be removed and reacquired, regardless of the value of force.
- **Replace**: Set replace to `Y` to delete old bulletins, specified in the bulletins parameter, and then re-acquire them. This will supersede the value for force. In other words, if you set replace to `Y`, then any bulletin specified for that acquisition will be deleted and reacquired, whether force is set to N or Y.
- **Command Line Overrides**: Use this parameter only when it is necessary to override your regular acquisition parameters. If used incorrectly, the acquisition will fail. Use the format of *-parameter value*.

Microsoft Settings

- **Acquire Microsoft Patches?**: Select **Yes** if you want to acquire Microsoft Patches. For additional settings, go to the Vendor Settings page.
  If you select **Yes**, the following options appear:
- **Acquire Microsoft Non Security Patches**: Select **Yes** to acquire Microsoft non-security patches. Select **No** to manage security patches only.
- **Mark Supersedence for all the bulletins**: Select **Yes** to run acquisition for a particular bulletin and update all of the existing bulletins in the Configuration Server Database. Select **No**, if you do not want to update the bulletins in the Configuration Server Database. Selecting **Yes** for this option enables you to update the bulletins in the Configuration Server Database without running acquisition for all of the bulletins each time.
  If you select **Yes** for the supersedence option and run an acquisition for any new bulletin using the Microsoft Update Catalog (MUC) or Optimized Patch Utility Service (OPUS) data feed, all existing MUC bulletins will be updated in the Configuration Server Database and the `bulletins.xml` file. At the same time, all existing OPUS bulletins will be updated in the `patch_data` file. As a result, the Configuration Server Database, the `bulletins.xml` file, and the `patch_data` file are all modified irrespective of the data feed selected for the new bulletin.

  Note: Bulletins can be marked for supersedence for the MUC and OPUS data feeds.
- **Language**: Select the language for which you want to download the Microsoft patches.

RedHat Settings

- **Acquire RedHat Patches?**: Select **Yes** if you want to acquire RedHat Patches. For additional settings, go to the Vendor Settings page in the Patch Management.

Adobe Settings

- **Acquire Adobe Patches?**: Select **Yes** if you want to acquire Adobe Patches. For additional settings, go to the Vendor Settings page in the Patch Management.
- Select the check box, **I have read and accepted the Adobe EULA at Adobe Software Licensing Agreement**. You can check the license agreement at http://www.adobe.com/products/eulas/.

Java Settings

- **Acquire Java Patches?**: Select **Yes** if you want to acquire Java Patches. For additional settings, go to the Vendor Settings page in the Patch Management.

SuSE Settings

- **Acquire SUSE Patches?**: Select **Yes** if you want to acquire SuSE Patches. For additional settings, go to the Vendor Settings page in the Patch Management.

5. Click **Next** to select products to exclude from an acquisition session.

   Caution: If you exclude one or more products or operating systems from one acquisition to the next, all patches specific to the products or operating systems that you excluded from acquisition will be removed from the Configuration Server Database. As a result, the removed products or operating systems are no longer eligible for vulnerability assessment and management. This applies to all vendors.

   Expand the appropriate vendor's products and check the products you want to exclude from the acquisition. Uncheck the products you want to include.

6. Click **Finish** to save the acquisition file you created.

Satellite Console Patch Management

When the Core server is configured to use the Metadata Based Patch Distribution model, the Agent on the managed device requests binaries from the Satellite server to patch vulnerabilities.

On the Satellite Console, you can use the Patch Management link to configure Satellite servers to either retrieve the requested binaries from the Internet through the Patch Gateway or to forward the request to the configured upstream server.

When you disable the Patch Gateway, the Satellite server will forward the request for the patch binaries to the upstream server. This is the default setting for this option. When you enable the Patch Gateway, the Satellite server will retrieve the patch binaries directly from the Internet. Enabling the gateway is recommended because it is a more efficient and direct way to acquire the binaries and allows you to fine tune how long you want to cache the binaries based on the needs of your enterprise.

If a proxy server is required to access the Internet, go to the **Proxy Settings** link on the Configuration tab in the Satellite console. The instructions are the same as those provided in "Proxy Settings" on page 274 for the Core Console except that the Proxy Settings link is not located under Infrastructure Management in the Satellite Console. It is a top-level link.

To configure the Patch Gateway on the Satellite server:

1. On the Configuration tab, click **Patch Management**. The Patch Management window opens.
2. If you want to forward the patch requests to the upstream server, select **Disable Gateway**. If you want the Satellite server to retrieve the patch binaries from the Internet, select **Enable Gateway**.
3. If you have selected the **Enable Gateway** option, you must configure the following options:
   - **Cache Lifetime (Days)**: Specify the number of days before the patch binary can be removed from the cache whether it has been used or not. Do not specify 0 as the number of days. The recommended number to specify is the number of days you have to apply the patch.
   - **Failover to Upstream Server**: Enable this option to failover to the upstream server if the gateway is unable to retrieve the Agent requested files from the Internet.
4. Click **Save** to save your configuration settings.

Security and Compliance Management

The Security and Compliance Management area is available on Satellite Console only.

The Security and Compliance Management link enables you to configure Satellite servers to ensure the requested patch binaries that are required to remediate vulnerabilities are retrieved from the Internet through the Security and Compliance Gateway or to forward the request to the configured upstream server.

When you disable the Security and Compliance Gateway, the Satellite server forwards the request for the binaries to the upstream server. This is the default setting for this option. When you enable the Security and Compliance Gateway, the Satellite server retrieves the binaries directly from the Internet.

If a proxy server is required to access the Internet, go to the Proxy Settings link on the **Configuration** tab in the Satellite console. The instructions are the same as those provided in "Proxy Settings" on page 274 for the Core Console except that the Proxy Settings link is not located under Infrastructure Management in the Satellite Console. It is a top-level link.

Configuring the Security and Compliance Gateway on the Satellite server

1. Log on to Satellite Console and click **Configuration** tab.
2. Click **Security and Compliance Management**. The Security and Compliance Management options appear in the details pane.
3. Select one of the options to retrieve the requested patch binaries:
   - Select **Disable Gateway** to forward the requests for patch binaries to the upstream server.
   - Select **Enable Gateway** to enable Satellite server to retrieve the patch binaries from Internet. The patch binaries are retrieved from the vendor and cached on the Security and Compliance Gateway server. If you have selected the **Enable Gateway** option, you must configure the following options:
     - **Cache Lifetime (Days)**: Specify the number of days before the patch binaries can be removed from the cache. The value for this field can vary from 1–*n*, where *n* can be any positive integer.
     - **Failover to Upstream Server**: Enable this option to ensure that request for binaries is forwarded to the upstream server if the Security and Compliance Gateway is unable to retrieve the agent requested binaries from the Internet.
4. Click **Save** to save your configuration settings.

Out of Band Management

Use the Configuration tab's Out of Band (OOB) Management area to configure OOB Management settings and preferences. For additional information on using Out of Band Management, see the *Radia Client Automation Enterprise Out of Band Management User Guide*. The following sections describe the available configuration options:

- "Enablement" on next page
- "Device Type Selection" on next page
- "vPro System Defense Settings" on page 337

Enablement

Use the Out of Band Management Enablement area to enable or disable the out of band management features supported by vPro or DASH devices.

Select the **Enable** checkbox to enable out of band management features.

Enabling Out of Band Management allows vPro or DASH devices to be contacted through the OOB Management remote operations capability in addition to the normal Wake on LAN capabilities of the RCA console.

For additional information on using Out of Band Management, see the *Radia Client Automation Enterprise Out of Band Management User Guide*.

Device Type Selection

After enabling OOB Management, use the Device Type Selection area to select the type of OOB device you want to manage.

It is possible to make one of three choices for device type. These are explained in the following sections:

- "DASH Devices" below
- "vPro Devices" below
- "Both vPro and DASH Devices" on next page

Depending on the device type that you chose, the RCA Console displays an interface relevant to that selection as explained in "Configuration and Operations Options Determined by Device Type Selection" on next page.

You can now go to the Operations tab and see the "Out of Band Management" on page 229 section to view the OOB Management options.

For additional information on using Out of Band Management, see the *Radia Client Automation Enterprise Out of Band Management User Guide*.

DASH Devices

If you select DASH, you can type the common credentials for the DASH devices if the DASH administrator has configured all of the devices to have the same username and password.

You can change the credentials the next time you visit this window if you have made a mistake entering them or if they have changed.

vPro Devices

If you select vPro devices, you must type the SCS login credentials and the URLs for the SCS Service and Remote Configuration to access vPro devices.

You can change the credentials the next time you visit this window if you have made a mistake entering them or if they have changed.

Both vPro and DASH Devices

If you select both types of devices, you can type the common credentials for the DASH devices and you must type the SCS login credentials and the URLs for the SCS Service and Remote Configuration needed to access vPro devices.

See Device Type Selection in the Administrative Tasks chapter of the *Radia Client Automation Enterprise Out of Band Management User Guide* for complete details.

Configuration and Operations Options Determined by Device Type Selection

After you make your device type selection, you will see options on the Configuration and Operations tab that reflect this selection. They are summarized in the following table.

Configuration and Operations options

	DASH	vPro
Configuration	No additional options	vPro System Defense Settings
Operations	Device Management	Provisioning vPro Devices Group Management Alert Notification

Note: You must log out and log in again to the RCA Console when you make or change your device type selection to see the device-type related options in the navigation panel on the Configuration and Operations tab.

vPro System Defense Settings

Before managing System Defense features on vPro devices and device groups you must define vPro System Defense Settings.

Note: This configuration option appears only if you have selected the vPro device type. System Defense settings do not apply to DASH devices.

- **Managing System Defense Filters**
  For vPro devices, you can create, modify, and delete System Defense filters. System Defense filters monitor the packet flow on the network and can drop or limit the rate of the packets depending if the filter condition is matched. Filters are assigned to System Defense Policies that can be enabled to protect the network.
- **Managing System Defense Policies**
  For vPro devices, you can create, modify, and delete System Defense policies and then deploy them to multiple vPro devices on the network. System Defense policies can selectively isolate the network to protect vPro devices from malware attacks.

- **Managing System Defense Heuristics Information**
  For vPro devices, you can create, modify, and delete heuristics specifications and then deploy them to multiple vPro devices on the network. These heuristics serve to protect the devices on the network by detecting conditions that indicate a worm infestation and then containing that device so that other devices are not contaminated.
- **Managing System Defense Watchdogs**
  For vPro devices, you can create, modify, and delete agent watchdogs and then deploy them to multiple vPro devices on the network. Agent watchdogs monitor the presence of local agents on the vPro device. You can specify the actions the agent watchdog must take if there is a change in state of the local agent.

For additional details, see vPro System Defense Settings in the Administrative Tasks chapter of the *Radia Client Automation Enterprise Out of Band Management User Guide* for complete details.

This is the last administrative task you have to perform on the Configuration tab to get the RCA Console ready for you to manage System Defense features on vPro devices. Now, in the role of Operator or Administrator, you can go to the Operations tab and start to manage the OOB devices in your network as explained in the "Operations" on page 221 chapter.

OS Management

Use the Operating System area to configure options pertaining to operating system deployment.

- "Settings" below

For additional information about OS Management, see the *Radia Client Automation Enterprise OS Management Reference Guide* in the RCA Reference Library.

Settings

The Operating Systems service allows Agents to connect to the RCA server and retrieve their OS entitlements and provisioning information. When this service is disabled on a Core, this information will not be available for Satellites or Agents requesting this information.

To enable the Operating Systems service, select the **Enable** box, and click **Save**.

During OS deployment, if you are planning to boot devices across the network, you must first enable the Boot Server (PXE/TFTP) installed with the Core. This will start two Windows services on the Core server: Boot Server (PXE) and Boot Server (TFTP).

- To enable the Boot Server (PXE/TFTP), select the **Enable Boot Server** box, and click **Save**.

You can host both the RCA Boot Server (PXE) and a DHCP server on the same machine.

For additional information about OS Management, see the *Radia Client Automation Enterprise OS Management Reference Guide* .

Usage Management

Use the Usage Management section to configure usage database connection settings and usage data collection settings.

- "Database Settings" below
- "Settings" below

See the *Radia Client Automation Enterprise Application Usage Manager Reference Guide* for more information about collecting and analyzing usage data using RCA.

Database Settings

You can configure the usage database connection settings or set up a new SQL/ORACLE database dedicated to Usage Manager by using the Database Settings page.

To configure the usage database connection settings:

1. On the Configuration tab, click **Usage Management** and then **Database Settings**.
2. Select the **Enable** box to enable usage data collection.
3. Specify the following Open Database Connection (ODBC) information:
   - **DSN** (data source name)
   - **User ID**
   - **Password**

   These settings must match the configured system ODBC DSNs on the Client Automation server. If the specified database has not yet been initialized, it will be initialized when these settings are saved.

   Note: To setup a new SQL/ORACLE database dedicated to Usage Manager, create a new DSN for the Usage database and provide the User ID and Password for that database.
4. Click **Save**.
   To disable usage data collection, clear the **Enable** box.

Settings

Usage data is collected when the Usage Collection Agent is deployed. Usage settings are applied to existing client devices during their collection schedule. If required, usage data can be obfuscated to ensure privacy.

Note: Obfuscation should be enabled before deploying the Usage Collection Agent. If it is enabled after this agent is deployed, some reporting data will appear in both obfuscated and non-obfuscated forms.

To obfuscate usage data:

1. Use the drop-down lists to select which usage data information should be hidden:
   - **Computer** – Hide computer-related information. The computer name is reported as a random set of alphanumeric values.
   - **User** – Hide user-specific information. The user name is reported as [AnyUser].

- **Domain** – Hide domain information. The domain name is reported as a random set of alphanumeric values.
- **Usage** – Hide usage counts and times. The executable file usage times and launch counts are all reported as zero values.

Select **Enabled** next to the usage information that you want to obfuscate within the usage reports.

2. Click **Save** to commit the changes.

See "Deploying the Usage Collection Agent" on page 176 to deploy the Usage Collection Agent and define a collection schedule.

Dashboards

Use the Dashboards area on the Configuration tab to configure the dashboards:

The "HPCA Operations" below dashboard provides information about the number of client connections and service events that have occurred over a given period of time.

The "Vulnerability Management" on next page dashboard provides data pertaining to security vulnerabilities on the client devices in your enterprise.

The "Compliance Management" on page 342 dashboard provides information about how well the managed client devices in your enterprise comply with regulatory standards, such as FDCC.

The "Security Tools Management" on page 343 dashboard shows you information about the anti-spyware, anti-virus, and software firewall products installed on the managed client devices in your enterprise.

The "Patch Management" on page 344 dashboard provides data pertaining to patch policy compliance on the client devices in your enterprise.

By default, a subset of the dashboard panes are enabled. Provided that you have administrator privileges, you can enable or disable any of the panes.

HPCA Operations

The HPCA Operations dashboard shows you the work that RCA is doing in your enterprise. The client connection and service event metrics are reported in two time frames. The Executive View shows the last 12 months. The Operational View shows the last 24 hours. Both views contain the following information panes:

- "Client Connections" on page 87
- "Service Events" on page 89

The Executive View also includes the following pane:

- "12 Month Service Events by Domain" on page 90

All of these panes are visible by default. You can use the configuration settings to specify which panes appear in the dashboard. For detailed information about these panes, see the "RCA Operations Dashboard" on page 87.

To configure the HPCA Operations dashboard:

1. From the Configuration tab, click **Dashboards**.
2. Under Dashboards, click **HPCA Operations**.
   This dashboard is enabled by default. To disable it, clear the **Enable HPCA Operations Dashboard** box, and click **Save**.
3. Under HPCA Operations, click either **Executive View** or **Operational View**.
4. Select the box for each pane that you want to show in the dashboard. Use the ? icon to display information about any related RCA configuration that is required for each pane.
5. Click **Save** to implement your changes

Vulnerability Management

The Vulnerability Management dashboard provides information about any publicly known security vulnerabilities that are detected on the managed client devices in your network.

The Vulnerability Management dashboard Executive View includes the following four information panes:

- "Vulnerability Impact by Severity (pie chart)" on page 92
- "Historical Vulnerability Assessment" on page 94
- "Vulnerability Impact by Severity (bar chart)" on page 99
- "Vulnerability Impact" on page 95

The Operational View includes the following four information panes:

- "HP Live Network Announcements" on page 98
- "Most Vulnerable Devices" on page 100
- "Most Vulnerable Subnets" on page 102
- "Top Vulnerabilities" on page 103

You can use the configuration settings to specify which panes appear in the dashboard. For detailed information about these panes, see "Vulnerability Management Dashboard" on page 91.

Note: HP Live Network provides a vulnerability scanner and updated vulnerability content to RCA. You must configure the Live Network settings before you can use the RCA vulnerability management features.

Configuring the Vulnerability Management dashboard

1. From the Configuration tab, click **Dashboards**.
2. Under Dashboards, click **Vulnerability Management**.
3. By default, this dashboard is enabled. To disable it, clear the **Enable Vulnerability Management Dashboard** box, and click **Save**.
4. Under Vulnerability Management, click either **Executive View** or **Operational View**.

5. Select the box for each pane that you want to show in the dashboard. Use the ? icon to display information about any related RCA configuration that is required for each pane.
   The following panes require additional information:

   - **Vulnerability Impact (Executive View)**
     Specify the default age of vulnerabilities to display in the chart. For example, if you type 90 days, only those vulnerabilities published during the last 90 days will be displayed in the chart. The default value is 45 days.
   - **HP Live Network Announcements (Operational View)**
     Enter the following information pertaining to your HP Live Network subscription:

   a. URL for the HP Live Network RSS notification feed

   b. Fully qualified host name for the HP Live Network authentication server

   Currently valid defaults are provided. You may also need to enable a proxy server using the **Console Settings** page.

6. Click **Save** to implement your changes.

Compliance Management

The "Compliance Management Dashboard" on page 104 provides information about how well the managed client devices in your network comply with various regulatory standards, such as the Federal Desktop Core Configuration (FDCC) standard.

The Compliance Management dashboard includes two views: the Executive View and the Operational View.

The Executive View includes the following information panes:

- "Compliance Summary by SCAP Benchmark" on page 106
- "Compliance Status" on page 105
- "Historical Compliance Assessment" on page 108

The Operational View includes the following information panes:

- "Top Failed SCAP Rules " on page 111
- "Top Devices by Failed SCAP Rules " on page 112

You can configure the dashboard to show or hide any of these panes. For detailed information about the panes, see the "Compliance Management Dashboard" on page 104.

You can also enable or disable the entire dashboard. If you disable the dashboard, the Compliance Management link will not appear in the left navigation menu on the Home tab.

Note: HP Live Network provides a compliance scanner and updated compliance content to RCA. You must configure the Live Network settings before you can use the RCA compliance management features.

Configuring the Compliance Management dashboard

1. From the Configuration tab, click **Dashboards**.
2. Under Dashboards, click **Compliance Management**. By default, this dashboard is enabled. To disable it, clear the **Enable Compliance Management** box, and click **Save**.
3. Under Compliance Management, click either **Executive View** or **Operational View**.
4. Select the box for each pane that you want to show in the dashboard. Use the [?] icon to display information about any related RCA configuration that is required for each pane.
5. Click **Save** to implement your changes.

Security Tools Management

The "Security Tools Management Dashboard" on page 113 shows you information about the anti-spyware, anti-virus, and software firewall products installed on the managed client devices in your enterprise.

The Security Tools Management dashboard has two views: the Executive View and the Operational View.

The Executive View includes the following information panes:

- "Security Product Status" on page 114
- "Security Product Summary" on page 115

The Operational View includes the following information panes:

- "Most Recent Definition Updates" on page 116
- "Most Recent Security Product Scans" on page 117

You can configure the dashboard to show or hide any of these panes. For detailed information about the panes, see the "Security Tools Management Dashboard" on page 113.

You can also enable or disable the entire dashboard. If you disable the dashboard, the Security Tools Management link will not appear in the left navigation menu on the Home tab.

Note: HP Live Network provides a security tools scanner and related content to RCA. You must configure the Live Network settings before you can use the RCA security management features.

Configuring the Security Tools Management dashboard

1. From the Configuration tab, click **Dashboards**.
2. Under Dashboards, click **Security Tools Management**.
   By default, this dashboard is enabled. To disable it, clear the **Enable Security Tools Management Dashboard** box, and click **Save**.
3. Under Security Tools Management, click **Executive View** or **Operational View**.

4. Select the box for each pane that you want to show in the dashboard. Use the ? icon to display information about any related RCA configuration that is required for each pane.
5. Click **Save** to implement your changes.

Patch Management

The Patch Management dashboard provides information about any patch vulnerabilities that are detected on managed devices in your network. By default, the Patch Management dashboard is disabled.

The Executive View of the Patch Management dashboard includes two information panes:

- "Device Compliance by Status (Executive View)" on page 119
- "Device Compliance by Bulletin" on page 120

The Operational View includes the following information panes:

- "HP Live Network Patch Manager Announcements" on page 122
- "Device Compliance by Status (Operational View)" on page 123
- "Microsoft Security Bulletins" on page 124
- "Most Vulnerable Products" on page 125

You can use the configuration settings to specify which panes appear in the dashboard. For detailed information about these panes, see the "Patch Management Dashboard" on page 119.

Configuring the Patch Management dashboard

1. From the Configuration tab, click **Dashboards**.
2. Under Dashboards, click **Patch Management**.
   By default, this dashboard is disabled. To enable it, select the **Enable Patch Dashboard** box, and click **Save**.
3. Under Patch Management, click either **Executive View** or **Operational View**.
4. Select the box for each pane that you want to show in the dashboard. Use the ? icon to display information about any related RCA configuration that is required for each pane.
   The following requires additional information:
   - **The Microsoft Security Bulletins (Operational View)**

     a. Specify the URL for the Microsoft Security Bulletins RSS feed
     Currently a valid default URL is provided. You may also need to enable a proxy server on the **Console Settings** page.
   - **HP Live Network Patch Manager Announcements (Operational View)**Enter the following information pertaining to your HP Live Network subscription:

     a. URL for the HP Live Network RSS notification feed

     b. Fully qualified host name for the HP Live Network authentication server
     Currently valid defaults are provided. You may also need to enable a proxy server using the **Console Settings** page.

5. Click **Save** to implement your changes.

Chapter 10

Wizards

While using the RCA console, you will use many different wizards to perform various management functions. This section contains an explanation of the individual steps you will encounter within each wizard.

Note: Some wizards can be launched from multiple areas of the control panel.

Note: The RCA console may open additional browser instances when running wizards or displaying alerts. To access these wizards and alerts, you must include the console as an Allowed Site in your browser's pop-up blocker settings.

Group Creation Wizard

Software or patches must be deployed to groups of managed devices in your database. Use the Group Creation Wizard to define device groups based on devices you specify, discovered devices, or on the devices returned as part of a reporting query.

The following procedure creates groups for internal directories. Groups that you create in the RCA Console are created in the internal zone under the Groups container.

To create an internal directory group:

1. On the Management tab tool bar, click **Create a New Group**. The RCA Group Creation Wizard opens.
2. Type a name and description for the group.
3. Click **Add Devices**. The Add Devices window opens.
4. Define Search Parameters and click **Search** to display a list of devices. (Clicking **Search** without defining parameters will return a list of all available devices).

5. Select the devices that you want to add, and click **Add**. When you are finished adding devices, close the Add Devices to a New Group window.
6. To remove devices, select the devices in the Members grid, and click **Remove Devices**.
7. Click **Submit**. The new group is added to the Groups container within the internal zone.

Service Import Wizard

Use the Service Import Wizard to import services from the `ServiceDecks` directory on the RCA server into the Software, Patch, or OS library. By default, this directory is located here:

<InstallDir>`\Data\ServiceDecks`

To import a service using the Service Import wizard:

1. On the **Operations** tab, click the **Import Service** toolbar button from any of the following pages:
   - **Software Management** > **Software Library**
   - **Patch Management** > **Patch Library**
   - **OS Management** > **OS Library**

   This launches the wizard.
2. Select the service to import. All service decks in the RCA server's `ServiceDecks` directory whose names contain the following words appear in the list of available services:

Library	Service Deck Name Must Contain	RCA Domain
Software	SOFTWARE	SOFTWARE
Patch	PATCH	PATCHMGR
OS	OS	OS

   By default, the `ServiceDecks` directory is located here:

   <InstallDir>`\Data\ServiceDecks`

   The fourth section of each service's file name contains a descriptive name for that software service, patch, or OS. For example, the service deck for the Orca software application is:

   PRIMARY.SOFTWARE.ZSERVICE.ORCA
3. Review the summary information, and click **Import**. The service is imported and will now be available in the pertinent (Software, Patch, or OS) HPCA library.
4. Click **Close** to exit the wizard.

Service Export Wizard

Use the Service Export Wizard to export services from the HPCA Software, Patch, or OS libraries to the `ServiceDecks` directory on the RCA server machine.

To export a service using the Service Export wizard:

1. On the **Operations** tab, click the **Export Service** toolbar button from any of the following pages:
   - **Software Management** > **Software Library**
   - **Patch Management** > **Patch Library**
   - **OS Management** > **OS Library**

   This launches the wizard.
2. Select the service to export.
3. Review the summary information and click **Export**. The service is exported to the RCA server's `ServiceDecks` directory. By default, this directory is: *<InstallDir>*`\Data\ServiceDecks`

   A service deck consists of several files, all of which have the same file name prefix. For example, the service deck name for the Orca software application is:

   PRIMARY.SOFTWARE.ZSERVICE.ORCA

   The fourth section of each file name in the service deck contains the descriptive name for the software, patch, or OS that was exported.
4. Click **Close** to exit the wizard.

Usage Collection Filter Creation Wizard

Use the Usage Collection Filter Creation wizard to create new usage collection filters.

To create a new collection filter:

1. On the Operations tab, click **Usage Management**, and then click **Collection Filters**.
2. Click the **Create New Filter** toolbar button. The wizard opens.
3. To configure the filter parameters, type the filter criteria into each text box.
   Only type values for those fields that you wish to filter usage data against. Empty text boxes are ignored and not used as part of the filter criteria.

   Note: To track all applications on agent computer, in the **File/Application Name** text box, type the value as `*`.

   The values that you type are compared to the file header in the software executable file to determine if the collected usage data meets the filter criteria.

   To determine how to filter for a specific piece of software, see "Dashboards" on page 340 .

   Note: Configuring filters to collect and report on more than 50 applications results in a large amount of data that can create severe reporting performance issues over time.
4. Click **Create.**
5. Click **Close** to exit the wizard.
   A new filter is added to the Collection Filters list.

Satellite Server Deployment Wizard

Use the Satellite Server Deployment Wizard to install the Satellite Server and enable remote services, such as data caching.

To deploy the Satellite Server:

1. On the **Configuration** tab, go to the **Infrastructure Management** > **Satellite Management** area.
2. Click the **Servers** tab.
3. Select one or more devices in the Satellite Servers list.
4. Any existing RCA Satellite Servers or Legacy Proxy Servers selected will be automatically upgraded to the latest RCA Satellite Server version.
5. Click the **Install the Satellite Server** toolbar button to launch the wizard.
6. Type the **User ID** and **Password** with administrator level access on the target device.
7. Click **Next**. The Properties window opens.
8. Select the **Installation Drive**, **Data Drive**, and **Deployment Mode**.

   Note: If you want to install the Satellite to a location other than the default location, you must follow these steps before the installation:

   a. Copy all of the RCA installation files for Satellite from the HPCA media to the target machine.

   b. Edit the parameters `INSTALLDIR` and `DATADIR` in the `setup.ini` file.

   c. Run the `setup.exe`

   For RCA Enterprise Edition, you can choose one of the following three modes:

   - **Streamlined** (Standard) mode offers only data caching services to the Client Automation agents that the Satellite serves.
   - **Full** service mode offers configuration services as well as data caching and OS configuration services to the Client Automation agents that the Satellite serves.
   - **Custom** mode allows you to select specific services to enable on the Satellite.

   For more information about deployment modes, see “Radia Client Automation Satellite Server” in the *Radia Client Automation Enterprise Installation and Upgrade Guide*.
9. Click **Next**. The Schedule window opens.
10. Specify the run schedule for the deployment job. Select **Run: Now** to deploy the Satellite Server right away, 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 Satellite Server download file is large. The deployment may take a long time if network traffic is heavy. You can check the status of the job in the Jobs area on the Management tab.
14. Click **Close** to exit the wizard.

Satellite Server Removal Wizard

Use the Satellite Server Removal Wizard to uninstall the Satellite Server from one or more devices in the RCA Satellite Servers group.

To uninstall the Satellite Server:

1. On the Configuration tab, go to the Infrastructure Management, Satellite Management area.
2. Click the **Servers** tab.
3. Select one or more devices in the Satellite Servers list.
4. Click the **Uninstall the Satellite Server** toolbar button. The Credentials window opens.
5. Type the User ID and password with administrator level access on the Satellite server.
6. Click **Next**. The Schedule window opens.
7. Select **Run: Now** to uninstall the Satellite Server immediately after the wizard is complete, or select **Run: Later** and type a date and time for the uninstall.
8. Click **Next**. The Summary window opens.
9. Review the summary information and click **Submit**.
   A Satellite Server Removal job is created. You can check the status of the job in the Jobs area of the Management tab.
10. Click **Close** to exit the wizard.

Server Pool Creation Wizard

Use the Server Pool Creation Wizard to create new Server Pools for Core and Satellite Servers. Server Pools enable software load balancing of client connections.

To add a new Server Pool:

1. On the Configuration tab, go to the Infrastructure Management, Satellite Management area.
2. Click the **Server Pools** tab.
3. Click **Create a New Server Pool** toolbar button to launch the Server Pool Creation Wizard. The properties page of the Server Pool Creation Wizard opens.
4. In the Properties area, specify the following:
   - **Name:** Type a name for the new Server Pool.
   - **Description:** Type a user-friendly description. This is optional.

- **Enabled:** Indicates if this Server Pool should be enabled or not. A Server Pool must be enabled in order for client devices to contact the Server Pool and its Servers. A Server Pool can be disabled to prevent connections to the Server Pool during maintenance periods.

5. Click **Next**. The Server Selection window opens.
6. Select the Servers that will be members of this Server Pool. Members of this Server Pool will be randomly selected by each agent when resources are needed. A Server Pool can contain a maximum of 30 Servers.
7. Click **Create** to exit the wizard.
   The new Server Pool is displayed on the Server Pools tab showing the number of Servers that are members in this pool.

Location Creation Wizard

Use the Location Creation Wizard to add new Locations. You can assign subnets and resources to these Locations and also set a priority order. Setting priority ensures that devices located in the subnets connect to resources in the indicated order.

To create a new location:

1. On the Configuration tab, go to the Infrastructure Management, Satellite Management area.
2. Click the **Locations** tab.
3. Click the **Create a New Location** toolbar button. The Location Creation Wizard opens.
4. In the Properties area, specify the properties for this Location. Name is the only required field, and it must be unique.
5. Click **Next**. The Subnet Selection window opens.
6. Select the Subnets to assign to this Location.
7. Click **Next**. The Connections window opens. You can either add a new connection or import an existing one.
   To add a connection:
   - Click an **Add Connection** link to define a connection assignment for this Location. The Location Connection Selection window opens.
   - Select a resource from the available types to assign to this Location. Agent connections will attempt to use resources from the selected Server or Server Pool.
   - Click **Add Connection**.

   To import a connection:
   - Click **Import Connections**. The Location Selection window opens.
   - Select a Location to import its connections.

     Note: An existing connection is be lost if you import the connections of another Location.

   - Click **Import Connections**.

8. Change the order of the Connections as required. Use the up and down arrows in the Reorder column to establish the required order. The devices attempt to contact the Servers or Server Pools in this new order.
9. Click **Create**.
   The new Location appears on the Location tab.

Subnet Creation Wizard

Use the Subnet Creation Wizard to add new Subnet addresses to which managed devices can be assigned. Managed devices will connect to Satellite Servers based on Subnet assignment to Locations.

To add a new subnet location:

1. On the Configuration tab, go to the Infrastructure Management, Satellite Management area.
2. Click the **Subnets** tab.
3. Click the **Create a New Subnet** toolbar button. The Subnet Creation Wizard opens.
4. In the Properties area, specify the following:
   - **IP Address**: Type a valid IP address.
   - **Subnet Mask**: Type a valid subnet mask.
   - **Subnet**: This field automatically generates the Classless Inter-Domain Routing (CIDR) address if you have entered a valid IP address and subnet mask.
   - **Name**: Type a name for the new Subnet.
   - **Description**: Optionally type a user-friendly description.
   - **Assigned Location**: Select a Location from the pull-down menu. The Locations available are the Default Location and Locations that you have added through the Location Creation Wizard.
5. Click **Create**.
   The new Subnet IP address is displayed on the Subnets tab.

Chapter 11

Patch Management Using Metadata

RCA provides a lightweight model for acquiring and delivering patch updates to your Agent devices. Because the model only uses Metadata to perform the patch scans on your agents, it is called Patch Management using Metadata.

The chapter discusses the concepts, configuration and implementation details needed to take advantage of Patch Management using Metadata.

Patch Management using Metadata is only available for:

- Microsoft operating systems using a Microsoft Update Catalog data feed.
- Adobe Reader, Adobe Acrobat, and Flash Player updates
- Java (JDK and JRE) updates
- RCA Core and Satellite Enterprise-level environment.

Note: To use the Metadata model for Java patches, download all Java (JDK or JRE) patches manually before creating an acquisition job and make sure that all patches are available at a specific location. It recommends to maintain a single location to download all patches.

Overview

The lightweight Patch Management using Metadata model offers several advantages that are described below and illustrated in "Patch Management using Metadata Model" on next page.

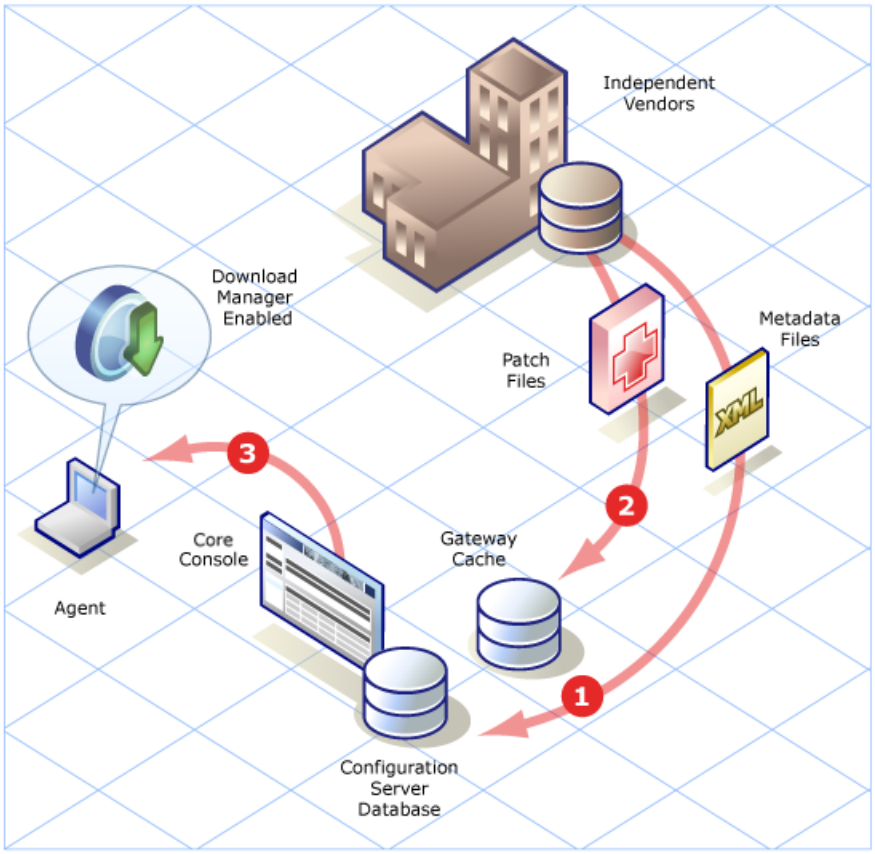
The Metadata Patch Management model differs from the traditional RCA patching model in that:

1. Only the bulletin Metadata information is stored in the Core server Configuration Server Database (CSDB), and not the actual patch binaries.
   This model makes patch acquisition run faster and also eases the load on the infrastructure traffic when running the Patch Discovery on an Agent and when synchronizing the RCA servers.
2. The actual patch binaries are downloaded and cached on the Patch Gateway, a component of both the Core and Satellite server. The Gateway downloads the patch binaries on the first request from an agent machine and caches them for other agent machines to use. Optionally, the Patch Gateway can have patch binaries preloaded onto it when you run an acquisition.
3. When using the Metadata model, the Agents must have the Download Manager enabled which allows them to contact the Patch Gateway at the end of the scanning phase with requests for applicable patch binaries.
4. The Download Manager handles the passive transfer of the patch files to the Agents. Once the file transfer is complete, an Agent connection is triggered to have the patches installed.

"Patch Management using Metadata Model" below illustrates the Patch Management using Metadata model.

For comparison, "Patch Management Model - traditional" on next page illustrates the traditional Patch Management model.

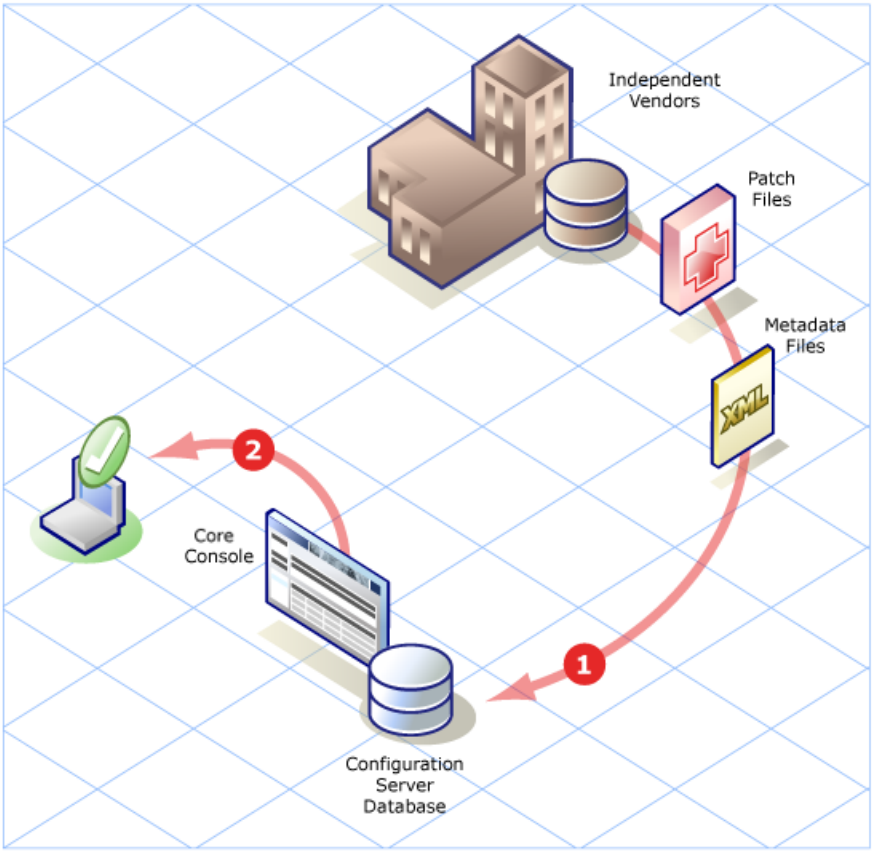
Patch Management using Metadata Model



Legend:

1. A Patch Acquisition downloads only patch metadata files from the Vendor. The patch metadata is published to the Core RCA database and used to discover the exact list of patch files required by the Agents being managed.
2. On request by an Agent (or optional preload), the Patch Gateway downloads the patch files from the Vendor and caches them for additional Agents to use. The patch files never need to be published to the RCA database.
3. Patch Agents require the Download Manager to be enabled. The Download Manager uses a background process to handle the passive download of the required patch files onto the Agent.

Patch Management Model - traditional



Legend:

1. A traditional Patch Acquisition downloads both metadata and all related patch files for bulletins from the Vendor. All of these files are published to the Core RCA database, regardless of whether Agents in the enterprise require them or not.
2. Patch Agents can be patched with or without the use of the Download Manager option. Without it, the Agent connect handles the download of the required patch files in a foreground process. In contrast, the Download Manager uses a background process to handle the passive download of the required patch files onto the Agent.

The following topics discuss how to take advantage of using Metadata distribution and the Patch Gateway for Patch Management in your enterprise:

- "Configuring Patch Management for Metadata Distribution " on next page
- "Configuring the Patch Gateway" on next page
- "Configuring the Patch Agents on Core" on page 360
- "Entitling Agents to Patches" on page 362
- "Patch Acquisition and Core Patch Gateway Operations" on page 363

Configuring Patch Management for Metadata Distribution

Metadata distribution is enabled by default. It can also be enabled from the Core console on the **Configuration** tab as explained in the following procedure.

Note: Download Manager must be enabled for Metadata Distribution.

1. From the Core Console, click the **Configuration** tab, open the **Patch Management** group and click **Distribution Settings**.
   The Patch Distribution Settings page opens, with areas for Patch Metadata Download and Patch Gateway Operations.
2. Use the **Patch Metadata Download** area to check the option:
   Enable Download of Patch Metadata only.

   Note: When you enable Metadata distribution, Microsoft patch management switches the Vendor feed named to **MSFT** from MICROSOFT.

   Note: When you enable Metadata distribution, Microsoft bulletins previously published to the CSDB (not using Metadata) are deleted if they are re-acquired using Metadata distribution. This behavior occurs because it is not possible to have the same bulletin acquired by using multiple feeds. As a result, the Metadata distribution acquisition process wipes out the published bulletins from the CSDB.

Configuring the Patch Gateway

The Gateway is a component of the Patch Manager Server that downloads and caches the patch binary data that are requested by the Agents. This can be enabled either on the Core or on the Satellite server or both (as when the Core is acting as the failover server for the Satellite). The Patch Gateway on the Core server provides some additional options from those on the Satellite server. See the chapter "Operations" on page 221 for details.

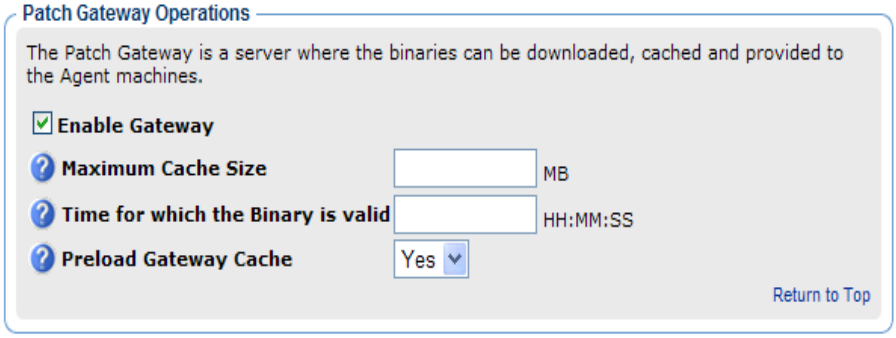
Enabling on the Core

To enable the Patch Gateway on the Core server:

Use the **Patch Gateway Operations** area to enable and configure the Patch Manager Gateway. Specify the following:

1. Check **Enable Gateway**. This must be turned on for Metadata Distribution.
   Enabling the Gateway displays additional fields to configure it.
2. Specify a **Maximum Cache Size** in megabytes. Leave this blank if the cache size is to be unlimited.

3. Specify the maximum **Time for which the Binary is valid** in hours:minutes;seconds (HH:MM:SS). If a requested binary is older than this when an Agent requests it, the Gateway will check to see if there's a later version before providing it.



4. The **Preload Gateway Cache** option is set to **Yes** to cache the patch binaries on the gateway when you run the acquisition; however, it recommends using the preload gateway option with caution.
   The advantage of preloading is that the first agent to request a specific patch binary does not have to wait for the Gateway to download it.

   The disadvantage of preloading is that the Gateway downloads all the patch binaries related to an acquisition—*regardless of whether the agents require them or not*.

5. Leave the **Preload Gateway Cache** option set to **No** to have the Gateway download and cache the patch binaries on the first agent request (on-demand download).

6. Click **Save** to save your settings.

Enabling on the Satellite

To enable the Patch Gateway on the Satellite server:

1. From the Satellite Console, select the Configuration tab and click **Patch Management**. This option allows you to enable or disable the Patch Gateway.
   When you disable the Patch Gateway, the Satellite server will forward the request for the patch binaries to the upstream server. This is the default setting for this option.

   When you enable the Patch Gateway, the Satellite server will retrieve the patch binaries directly from the Internet. This is the recommended way for acquiring binaries. See "Satellite Console Patch Management" on page 334.

2. If you enable the Patch Gateway, you will have to configure additional options. See "Satellite Console Patch Management" on page 334.

3. Click **Save** to save your settings.

Enabling Acquisition Jobs

Use the Configuration tab, Patch Management area's **Acquisition Jobs** panels to define a job to acquire bulletins. This task is no different whether you are using Metadata Distribution or not.

Server Access Profiles

Ensure your Core and Satellite servers are defined with Server Access Profiles, as discussed in "Configure Client Operations Profiles" on page 36.

For Patch Management using Metadata and the Gateway, use the RCA Administrator CSDB Editor to verify the SAP entries normally created with a Type of DATA for the Core and Satellite servers all include the Role of P.

The P role passes Agent requests for patch binaries to the Patch Manager Gateway.

This completes the Patch Gateway Configuration for Metadata Distribution on the server side.

Configuring the Patch Agents on Core

The next step is to configure the Patch Agents to access the Patch Manager Gateway using Client Operation Profiles (COP) and enable the silent preload of patch binaries. These are discussed below.

Agent Configuration for Offline Scanning

When managing patches through the Metadata acquisition model, once the acquisition file for the MSFT Vendor is downloaded to the Agents, the scanning phase takes place without relying on any connection to the network or the RCA Core or Satellite servers.

At the end of the scanning phase, the list of patch binaries required for each Agent to be in compliance is available.

The Agent starts the Download Manager, which will begin the preload of the binary files once a network connection is available.

Offline Scanning Requirements

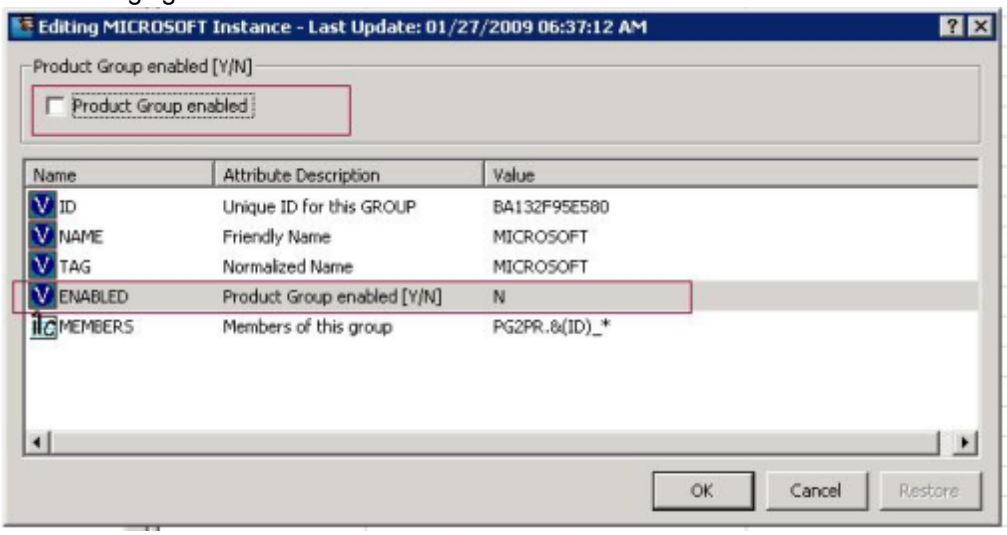
The patch offline scanning ability is built into the Agents and is automatically enabled under the following conditions. Be sure to meet these conditions for offline scanning if you are using Patch Management using Metadata.

- Configure the Patch Management > Distribution Settings to have **Patch Metadata Download** enabled.
- Configure the Patch Management > Agent Options to have the **Download Manager** enabled. For details, see "Agent Configuration for Download Manager" on next page.
- The Core's Configuration Server Database must have the following entry disabled:
  - The MICROSOFT instance in the PRIMARY.PATCHMGR.PROGROUP class must be disabled. This configuration is discussed below.

To disable the MICROSOFT instance in the PATCHMGR.PROGROUP Class:

1. On the Core server, login to the RCA Administrator CSDB Editor.
2. Navigate to the MICROSOFT instance of the PRIMARY.PATCHMGR.PROGROUP class.

3. Edit and remove the check mark to set the Product Group Enabled attribute to N, as shown in the following figure:



Make sure this Enabled attribute is set to N to allow Offline Scanning to take place on the Agents.

Agent Configuration for Download Manager

With Metadata distribution, the Agents request a set of binary files to be downloaded from the Patch Gateway at the end of the scanning phase.

The Patch Agents must be configured to use the Download Manager. This works silently in the background to bring down the patch files to the Agents as an asynchronous process. The Download Manager allows this passive file transfer to stop and start, as needed, but continues the download from where it left off.

When enabled, the Download Manager for Patch Agents allows you to set several options to control how the binaries are downloaded to the Agents. The Download Manager options include network utilization in normal mode and in screen saver mode, delay after initialization, and apply patch updates after download completion.

The Download Manager option is not enabled by default. To enable it, use the Console **Configuration** tab > **Patch Management** Area > **Agent Options** page. Details are given below.

When you enable the Download Manager and save the options on the Console, the Patch Manager DISCOVER instances in the CSDB Database are modified to reflect your selections.

Enabling the Patch Agents to use the Download Manager

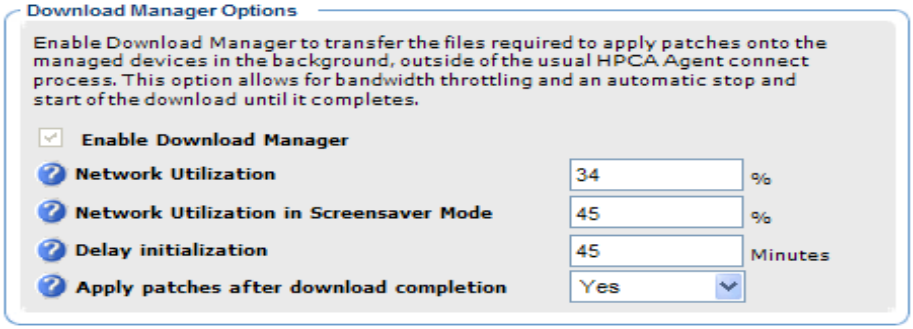
Use the Console **Configuration** tab > **Patch Management** area > **Agent Options** page to enable the Download Manager and set related options.

Caution: The Download Manager must be enabled to patch Microsoft devices when using Patch Metadata Distribution.

1. From the Console **Configuration** tab, click **Patch Management** and **Agent Options**.
2. On the Agent Options page, go to the Download Manager Options area.

3. Check the box for **Enable Download Manager**.
   When checked, the Download Manager options are displayed.
4. Set the Download Manager options. Set specific options for network utilization, network utilization in Screen Saver Mode, delay after initialization, and whether or not to apply the patches after download completion.
   For details on setting these options, see "Agent Options" on page 316.

   Example: The following entries enable the Download Manager for Patch Agents with up to 34% Network Utilization during device activity, up to a 45% Network Utilization in Screen Saver Mode, and a 45-second delay after initialization. After the patch files are downloaded, they will be available to be applied during the next Patch Agent connect



5. Optionally, use the Agent Options area to set additional Agent Options:
   - Disable Automatic Updates
   - Delete Software Distribution Folder

   For details on setting these options, see "Agent Options" on page 316.

   Note: Saving the Patch Agent options modifies the Patch Manager DISCOVER instance for all methods in the Configuration Server Database (Create, Delete, Verify, Update and Repair).
6. Click **Save** to save your changes.

Entitling Agents to Patches

Entitle the Agents to the appropriate patches using the standard patch deployment procedures. For more information, see the chapter, *"Managing the Enterprise" on page 131*.

The Patch Agent downloads the applicable binaries through the patch Gateway, utilizing the Download Manager's background process for asynchronous transfer of the applicable patch files.

Caution: The Patch Agents will not receive patch binaries unless the Agents have been entitled to those services.

As the Gateway obtains requested patch files, it caches them for other Agents to use.

Patch Acquisition and Core Patch Gateway Operations

Patch Acquisition using Metadata takes minutes as opposed to hours, on average, because it is lightweight—meaning only the patch information is downloaded and published to the CSDB.

1. Use the Operations tab, Patch Management area to run an Acquisition.
   From the Console, click the **Operations** tab and go the **Patch Management** group. Select **Start Acquisition**.

   After acquisition, the CSDB only contains the patch metadata information and not the actual patch binary data.

2. Optionally, you can view the status of an acquisition.
   From the Console, click the **Operations** tab. Expand the **Patch Management** group and click **Report Acquisition Status**.

3. Entitle the Agents to the appropriate patches using the standard patch deployment procedures. The Patch Agent downloads the applicable binaries through the patch Gateway. The Gateway then caches the binary for other clients to use.

4. Once the files are downloaded and cached on the Gateway, the available patches are listed on the Cache Content Details page
   To access this page from the Console, click **Operations** and select **Patch Manager**, **Gateway Operations**, and **Cache Content Details**.

Chapter 12

Preparing and Capturing OS Images

In this chapter, you will learn how to prepare and capture the following operating system images for deployment to managed client devices in your environment:

- Windows 8
- Windows 7
- Windows Server 2008 R2 (x64)
- Windows Vista
- Windows Server 2008

To capture images of older operating systems, see "Capturing Windows XP and Windows Server 2003 OS Images" on page 465.

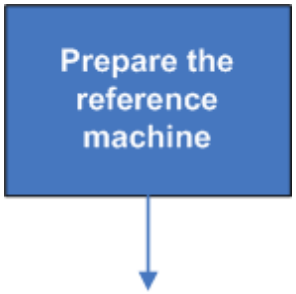
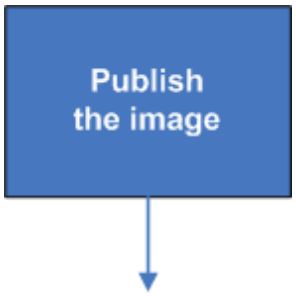
Note: If the HPCA boot loader and `WINPE.WIM` (by customer) files have been updated, make sure the same files are available in the RCA CSDB, boot directory on RCA server (*<InstallDir>\Data\BootServer\X86PC\UNDI\boot*), and ImageCapture and ImageDeploy CDs before you start the capture process. HPCA boot loader files gets updated if any hotfix is released by HP. WINPE.WIM file can be updated by RCA administrators to include various drivers.

Caution: If you are prompted for the OS Manager Server's IP address and port number, you must specify the RCA server port number (by default 3466).

Note: If you are using an existing OS WIM image (this includes the OS `.WIM` files on the Microsoft Windows OS installation media) or have created an OS WIM image using the Microsoft Windows Automated Installation Kit (AIK), you do not need to prepare or capture the image, and you and can skip to the next chapter.

Process Overview

In RCA, the process of managing operating systems has four steps:

	The reference machine is the system that you use to create the “gold” OS image that can be deployed to the managed devices in your environment. See "Preparing the Reference Machine" on page 369.
	RCA provides interactive OS image capture tools that enable you to easily capture an OS image on a reference machine. See "Capture the OS Image" on page 372.
	After you capture an OS image, you must publish it to the RCA database. RCA provides an interactive Publisher tool that helps you do this. See "Publishing Operating System Images" on page 392.
	You can then use the RCA console to deploy operating system images to groups of managed client devices in your environment. See "Managing Operating Systems " on page 168.

The focus of this chapter is preparing and capturing OS images. Publishing and deployment are discussed in the chapters noted above.

Preparing and Capturing Desktop OS Images

The information in this section pertains to desktop, laptop, notebook, netbook, and workstation client devices. For information about Thin Client devices, see "Preparing and Capturing Thin Client OS Images" on page 374.

Prerequisites

- Before you attempt to capture an OS image using the HPCA OS Image Capture tool, make sure that the Microsoft Windows Automated Installation Kit (AIK) is installed on the RCA Core server.

For more information, see the *Installing RCA Core Server* chapter in the *Radia Client Automation Enterprise Installation and Upgrade Guide*.

- Make sure that the Microsoft .NET Framework version 2.0 (or later) is installed on the reference machine. The .NET Framework is available at the Microsoft download center: http://www.microsoft.com/downloads

  To determine which version of the .NET Framework is present on the reference machine, list the folders in the following directory:

  `%SYSTEMROOT%/Microsoft.NET/Framework`

- RCA does not verify that enough free disk space exists on the Core server to successfully upload the OS image after it is captured. If sufficient free space is not available, the upload will fail.
  Make sure that enough free disk space exists on the Core server so that the OS image upload can be successfully completed.

- To capture Microsoft Windows Vista and above OS with a separate boot partition successfully, the size of the boot partition must be 300 MB at minimum. If it is less than 300 MB, increase the size to a minimum of 300 MB. The recommended boot partition size is one GB.
  If you have customized the *winpe.wim* image file, set the size of the boot partition to double of the size of your winpe.wim file. For example, if the size of the *winpe.wim* file is 200 MB, set the size of the boot partition to a minimum of 400 MB.

Deployment Methods

There are two methods that you can use to deploy an OS image using RCA:

- Use **ImageX** to capture an image in `.WIM` format that will be deployed using Windows PE and the ImageX utility.
- Use **Windows Setup** to capture an image in `.WIM` format that will be deployed using Windows PE and Windows Setup.

Windows Setup provides greater control over the installation. ImageX is more comparable to a simple file extraction. You can perform unattended installations or upgrades with images captured using either method.

Caution: To successfully capture an image using the Windows Setup deployment method, you must have sufficient free disk space in the OS partition on the reference machine. For example, to capture a 7 gigabyte (GB) image, you will need 50-60 GByte of free disk space.

The following table provides a summary of each deployment method. The OS image preparation and capture steps that you perform will vary slightly based on the operating system and deployment method that you choose.

Deployment Methods

Method	Service OS Type*	Resulting Files**	Supported Platforms
Microsoft ImageX	WinPE	`ImageName.WIM` `ImageName.EDM`	Windows XP SP2 (or later) Professional x86 or x64

Method	Service OS Type*	Resulting Files**	Supported Platforms
			Windows Vista Enterprise, Business and Ultimate Edition x86 or x64 Windows 7 Windows 8 Windows Server 2008 Standard and Business edition x86 or x64 Windows 2003 Server SP1 and Advanced Server x86 or x64 Windows Server 2008 Release 2 (R2) x64
Microsoft Windows Setup	WinPE	`ImageName.WIM` `ImageName.EDM`	Windows Vista Enterprise, Business and Ultimate Edition x86 Windows 7 Windows 8 Windows Server 2008 Standard and Business edition x86 Windows Server 2008 Release 2 (R2) x64

*You must have the compatible drivers for the target device in the SOS. If you are using Windows PE, and the drivers are not available, see "Building a Custom Windows PE Service OS" on page 483. If you are using a Linux SOS, It will provide periodic updates of the Linux SOS.

**Resulting files are stored in the following directory on the RCA server after the image is captured:

<InstallDir>`\Data\OSManagerServer\upload`

Note: For more information about the ImageX and Windows Setup deployment methods, see Microsoft's documentation.

About the OS Image Capture Tool

The HPCA OS Image Capture tool performs the following tasks:

1. Collects and stores information (including hardware and OS information capabilities) about the reference machine.
2. Executes the exit points that are available for your use as needed. `PRE.CMD` is executed before the Image Preparation Wizard starts SysPrep to seal the image. `POST.CMD` is executed after Sysprep has sealed the image. See "Image Preparation Wizard Exit Points" on page 466 for details.

> **Note:** Image Capture exit points are only supported for ImageX and Windows Setup capture types

3. Runs Microsoft Sysprep.
4. Restarts the reference machine into the Service OS (booted from the appropriate media). The Service OS runs to collect the image and its associated files.
5. Creates and copies files to the following directory on the RCA server:
   <InstallDir>`\Data\OSManagerServer\upload`

   The files uploaded are:

   - `ImageName.WIM`
     This file contains a set of files and file system information from the reference machine.
   - `ImageName.EDM`
     This file contains the object containing inventory information.

> **Note:** The OS Image Capture tool requires the Microsoft .NET Framework version 2.0 (or later), which is available at the Microsoft download center:
>
> http://www.microsoft.com/downloads
>
> To determine which version of the .NET Framework is present on the reference machine, list the folders in the following directory:
>
> `%SYSTEMROOT%/Microsoft.NET/Framework`

Preparing the Reference Machine

The process of preparing the reference machine is slightly different depending on the operating system that you are capturing. See the following topics for detailed instructions:

- "Windows 8, Windows 7, or Windows Server 2008 R2 x64" below
- "Windows Vista or Windows Server 2008" on page 371

Windows 8, Windows 7, or Windows Server 2008 R2 x64

You can capture from either a single or dual-partition OS setup. In case of a dual-partition OS setup, the System Reserved partition will contain the boot manager and HPCA Service OS (SOS) files. The OS partition will contain the boot loader and the OS itself.

Complete the following steps to prepare the reference machine. Note that the following procedure uses Windows 8 as an example.

1. Install the operating system from the original product media. The reference machine must be capable of running the operating system that you are installing. Make sure the reference machine is using DHCP.
   - When you are prompted for the type of installation, select the **Custom (advanced)** option.
   - When you are prompted for where to install Windows 8, click **Drive Options (advanced)**.

2. Click **New** to create a new partition that will hold Windows 8.
3. In the **Size** box, select the maximum value.
4. Click **Apply**. A dialog box opens to warn you that Windows creates additional partitions. Click **OK** to close this dialog box and proceed.
5. To create a **single partition** installation, follow these steps:
   a. Select the small System Reserved partition, and click **Delete**. A dialog box opens to warn you that any data stored on this partition will be lost.
   b. Click **OK** to close the dialog box and proceed.
   c. Select the remaining partition, and click **Next**. The Windows 8 installation then proceeds.

   To create a **dual-partition** installation, follow these steps:
   a. Select the partition that you created in step 4, and click **Delete**. A dialog box opens to warn you that if you delete this partition, any data stored on it will be lost.
   b. Click **OK** to close the dialog box and proceed.
   c. Select the System Reserved partition, and click **Extend**.
   d. In the **Size** box, specify 1024 MB.
   e. Click **Apply**. Once again, a dialog box opens to warn you that extending a partition is not a reversible action.
   f. Click **OK** to close this dialog box and proceed.
   g. Select the partition that you created in step 4 again, and click **New**.
   h. In the **Size** box, select the maximum value.
   i. Click **Apply**. Once again, a dialog box opens to warn you that Windows may create additional partitions.
   j. Click **OK** to close this dialog box and proceed.
   k. Click **Next**. The Windows 8 installation then proceeds.
6. When you are prompted to select your computer's location, select **Work Network**.
7. Customize the OS as necessary. This may include installing a set of basic or required applications. Be sure to include the latest service packs for the OS and applications and all required drivers for the devices to which you will deploy the image.

   Note: Installing the RCA agent on the reference machine is not recommended. When the OS is deployed, the RCA agent will be installed (or upgraded, if it is already installed).
8. Configure the BIOS power management so that the device does not power down after a few minutes of keyboard or mouse inactivity before the upload process to the RCA Server is finished.
9. Using the Control Panel, set the User Access Control level to **Never notify**.

10. Keep the file system as small as possible (this will minimize the size of the `.WIM` file).

    Caution: To successfully capture an image using the Windows Setup deployment method, you must have sufficient free disk space in the OS partition on the reference machine. For example, to capture a 7 GB image, you will need 50-60 GByte of free disk space.

    a. Delete unnecessary files and directories from the files system.

    b. Turn off System Restore.

11. As part of the capturing process for Windows 8, Windows 7, and Windows Server 2008 R2 x64, the system will be set up to boot into Capture mode if it reboots from the local disk. There is no need to have Image Capture media present on CD or network.

Windows Vista or Windows Server 2008

1. Install the operating system from the original product media. The reference machine must be capable of running the operating system you are installing. Make sure the reference machine is using DHCP.

   Caution: Store the OS on the C: drive. It is the only drive that will be captured.

   Customize the OS as necessary. This may include installing a set of basic or required applications. Be sure to include the latest service packs for the OS and applications and all required drivers for the devices to which you will deploy the image.

   Note: Installing the RCA agent on the reference machine is not recommended. When the OS is deployed, the RCA agent will be installed (or upgraded, if it is already installed).

2. Configure the BIOS power management so that the device does not power down after a few minutes of keyboard or mouse inactivity before the upload process to the RCA Server is finished.

3. Turn off User Access Control.

4. Keep the file system as small as possible which will minimize the size of the `.WIM` file.

   Caution: To successfully capture an image using the Windows Setup deployment method, you must have sufficient free disk space in the OS partition on the reference machine. For example, to capture a 7 GByte image, you will need 50-60 GByte of free disk space.

   Note: For Windows operating system before Windows 7, HP supports deploying the image to the primary boot partition of the primary boot drive.

   a. Delete unnecessary files and directories from the files system.

   b. Turn off System Restore.

5. As part of the capturing process for Vista and Windows Server 2008, the system will be set up to boot into Capture mode if it reboots from the local disk. There is no need to have ImageCapture media present on CD/DVD or the network.

Capture the OS Image

You can use the OS Image Capture tool to capture an image of a reference machine and upload that image to the RCA server. You can then publish that image and deploy it to managed devices in your environment.

The Image Capture tool can be used with the following operating systems:

- Windows Vista
- Windows 7
- Windows 8
- Windows Server 2008
- Windows Server 2008 R2 (64-bit)

Note: The OS Image Capture tool supports Windows Preinstallation Environment (Windows PE) based captures only. To perform Thin Client captures, see "Preparing and Capturing Thin Client OS Images" on page 374. To capture older OS images, see "Capturing Windows XP and Windows Server 2003 OS Images" on page 465.

To access the OS Image Capture Tool:

Log on to the reference machine using an account with administrator privileges.

1. Insert the ImageCapture media CD into the reference machine.
   See *Product Media* in the *Radia Client Automation Enterprise OS Management Reference Guide* if you need more information about where to get this media.
2. On the ImageCapture CD, browse to the following folder:
   `image_preparation_wizard\win32`
3. Run **oscapture.exe**.
   The OS Image Capture tool opens. The Welcome page provides information about the reference machine hardware and operating system.

   Note: If the operating system on the reference machine is older than those listed above, the HPCA Image Preparation Wizard opens instead. See "Capturing Windows XP and Windows Server 2003 OS Images" on page 465 for more information.
4. Click **Next** to proceed. The "Imaging Options" below page opens.

Imaging Options

Use the Imaging Options page to specify the following information:

- **Imaging Method** – Select ImageX or Windows Setup.
  - ImageX captures an image in `.WIM` format that will be deployed using Windows PE and the ImageX utility.
  - Windows Setup captures an image in `.WIM` format that will be deployed using Windows PE and Windows Setup.

  Windows Setup provides greater control over the installation. ImageX is more comparable to a simple file extraction. You can perform unattended installations or upgrades with images captured using either method.

  For more information about ImageX and Windows Setup, see the Windows documentation available at http://technet.microsoft.com.
- **Image Name** – A name that you choose for this image. The files that are uploaded to the RCA server and used to deploy this image will use this name.
  The image name can be up to eight characters long. It is not case-sensitive.
- **Image Description** – Any descriptive information that you want to provide. When this image is published, this information will be displayed in the list of available operating system images on the RCA server.
  The image description can be up to 80 characters long.
- **Destination Server** – Host name or IP address of the RCA server to which this image will be uploaded after it is captured.
  The Image Capture Tool will attempt to contact the RCA server to ensure that the image can be uploaded after the capture. If it cannot connect, you will see an error message. Be sure that the system proxy and firewall settings on the reference machine will allow it to communicate with the server.
- **Port** – Port number on which the RCA server specified above is listening. The default port is 3466.

Click **Next** to proceed to the "Summary" below page.

Summary

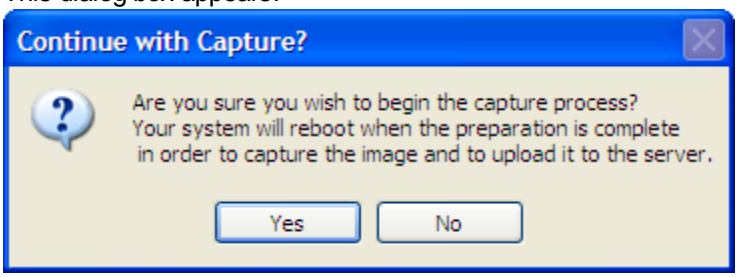
The Summary page shows you information about the image that you are about to capture, including the name that you specified and the estimated size of the image.

To change any of the parameters that you have specified for this capture, click the **Back** button to return to the "Imaging Options" on previous page.

To capture the image and upload it to the specified RCA server, click **Capture**.

The following steps take place:

1. This dialog box appears:



2. Click **Yes** to prepare the machine, reboot, and capture the image.
   The capture can take 15-20 minutes to complete, depending on the size of the image. During the capture, status information is displayed on the Service OS screen. See "About the Windows PE Service OS Screen" on page 385 for more information.
3. After the image is captured, the OS Image Capture tool connects to the network and stores the image in the following directory on the RCA server:
   <InstallDir>`\Data\OSManagerServer\upload`
4. When the upload process is complete, you will be asked whether to reboot or shut down the machine.

Next, you will want to publish your image to the RCA database. See “Publishing” in the RCA Console online help.

Preparing and Capturing Thin Client OS Images

Caution: Do not publish factory OS images for thin client devices. All thin client images must be captured before they are deployed to target devices.

During the OSM capture process additional information about the OS is retrieved and later used for image deployment. As a result, the administrator should not publish a factory image directly, as required information would be unavailable and the deployment would not succeed.

Windows XPe and WES 9 OS Images

This section explains how to prepare and capture a Windows XPe or Windows Embedded Standard (WES) 9 or 2009 thin client operating system image.

Note: You can capture an image on an XPe or WES thin client device and subsequently deploy the captured image to an XPe or WES thin client device with a larger flash drive.

Task 1: Prepare the Windows XPe or WES 9 Reference Machine

To prepare a Windows XPe or WES thin client for image capture, you will need the following:

- HPCA media
- Image Preparation CD-ROM

- If you select the Legacy method, the boot order must be set to CD before you start the capture process.

Before you can capture a Windows XPe or WES image, you must do the following:

1. Log on to the Windows XPe or WES device as Administrator.
2. Install the RCA agent on the Windows XPe or WES device.
   See "Installing the RCA Agent on HP Thin Client Devices" in the *Radia Client Automation Enterprise Installation and Upgrade Guide* for details.

Task 2: Run the Image Preparation Wizard

The Image Preparation Wizard performs the following tasks:

1. Checks if there is enough free disk space on the machine and verifies that the RCA agent is installed. If there is not enough free disk space, the Image Preparation Wizard displays a message and terminates.
2. Creates an object that contains information (including hardware and BIOS capabilities) about the reference machine.
3. Restarts the reference machine into the service operating system (booted from the Image Preparation CD you created). Based on the type of the capture, the capture process boots into either Linux or Windows PE Service OS.
4. Creates and copies the following files to this directory on the HPCA server: *<InstallDir>*`\Data\OSManagerServer\upload.`
   - `ImageName.IMG`: This file contains the image. Windows XPe or WES images can be deployed to target machines with flash drives of equal or greater size.
   - `ImageName.MBR`: This file contains the Master Boot Record information.
   - `ImageName.EDM`: This file contains the object containing inventory information.
   - `ImageName.PAR`: This file contains the object containing disk partition information.

   Note: While these files are transferred, network speed will be less than optimal.

   A comprehensive log (*machineID*`.log`) is available in *<InstallDir>*`\Data\OSManagerServer\upload` after the image is deployed.

Using the Image Preparation Wizard

To use the Image Preparation Wizard:

1. Insert the Image Preparation Wizard CD-ROM that you created into the CD-ROM drive of the reference machine. (Thin client devices require a USB CD-ROM drive). This CD is created using the `ImageCapture.iso` found within the `Media\iso\roms` directory on your HPCA media.
2. If autorun is enabled, the HPCA OS Preparation and Capture CD window opens.
3. Browse to the `\image_preparation_wizard\win32` directory.
4. Double-click **prepwiz.exe**. The Welcome window opens.

5. Click **Next**.
   The End User Licensing Agreement window opens.
6. Click **Accept**.
7. Type the IP address or host name and port for the RCA server. This must be specified in the following format:
   xxx.xxx.xxx.xxx:port

   The RCA server port used for OS imaging and deployment in an RCA Core and Satellite installation is 3466. In an RCA Classic installation, port 3469 is reserved for this purpose.

   If the Image Preparation Wizard cannot connect to the RCA server, a message opens and you must:

   - Click **Yes** to continue anyway.
   - Click **No** to modify the host name or IP address.
   - Click **Cancel** to exit the Image Preparation Wizard.
8. Click **Next**.
   The Image Name window opens.
9. Type a name for the image file. This is the image name that will be stored in the `\upload` directory on the RCA server.
10. Click **Next**.
    A window opens so you can type a description for the image.
11. Type a description for the image file.
12. Click **Next.**
    The Options window opens.
13. Select the option, **Perform client connect after OS install** or **Redeploy OS after the upload is completed**.
    Select the **Perform client connect after OS install** check box to connect to the RCA server after the OS is installed to verify that the OS was installed properly. If this is not selected, the OS Connect will not occur automatically after the OS is installed.
14. Accept the defaults and click **Next**.
    The Summary window opens.
15. Click **Start**.
16. Click **Finish.** The wizard prepares the image.
    The device boots to the Image Preparation Wizard CD in the CD-ROM drive. Make the necessary configuration adjustments to ensure this will happen (for example, with some BIOS versions, you can hit F10 during the reboot process and change the boot order in the configuration settings).

    Note: You may want to create copies of the files stored in the `\upload` directory so that you can retrieve them if necessary.

    During the capture, status information is displayed on the Service OS screen. See "About the Windows PE Service OS Screen" on page 385 for more information.

OS Image Preparation Wizard connects to the network, and stores the image on the HPCA

server in the following directory:
<InstallDir>`\Data\OSManagerServer\upload`

When the upload process is complete, you will see the following messages

```
OS image was successfully sent to the OS Manager Server

**** If you had inserted a CD remove it now and reboot
```

17. Reboot the reference machine and readjust your boot settings, if necessary, to return to the original operating system.

Next, you will want to publish your image to the CSDB. See "Publishing" on page 387.

WES 7 OS Images

You can capture the WES 7 OS images using Legacy and Imagex capture options. This section explains how to prepare and capture a WES 7 thin client operating system image.

Task 1: Prepare the WES 7 Reference Machine

To prepare a WES 7 thin client for image capture, you will need the following:

- HPCA media
- Image Preparation CD-ROM
- If you select the Legacy method, the boot order must be set to CD before you start the capture process.

Before you can capture a WES 7 image, you must do the following:

1. Log on to the WES 7 device as Administrator.
2. Install RALF and RCA agent on the WES 7 device. See “Installing the RCA Agent on HP Thin Client Devices” in the *Radia Client Automation Enterprise Installation and Upgrade Guide* for details.
3. Run a manual agent COP connect and reboot the device.
4. Disable Enhanced Write Filter (EWF) and reboot the device to disable the EWF successfully.
5. Customize the `Unattend.xml` file.
   - **For Legacy**: customize and save the `Sysprep_Unattend.xml` file located at `C:\Windows\System32\sysprep` as per your requirements.
   - **For ImageX**: customize and save the `unattend-capture.xml` file located at `<InstallDir>\Data\OSManagerServer\capture-conf\wes7\x86` as per your requirements. Use the `unattend-capture.xml` file while publishing the OS image.

Task 2: Run the Image Preparation Wizard

The Image Preparation Wizard performs the following tasks:

1. Checks if there is enough free disk space on the machine and verifies that the RCA agent is installed. If there is not enough free disk space, the Image Preparation Wizard displays a message and terminates.

2. Creates an object that contains information (including hardware and BIOS capabilities) about the reference machine.
3. Checks if the disk size is greater than 4 GB, the user is given an option to choose between ImageX and Legacy capture methods. It is recommended to use ImageX based capture for devices with disk size greater than 4 GB. If the disk size is less than or equal to 4 GB, the capture happens through the Legacy method.

   Note: By default, the ZSTOP expression in CSDB Editor under PRIMARY.OS.PACKAGE.Local Service Boot WinPE x86 SOS has the following value:

   ```
   WORDPOS(EDMGETV(ZCONFIG,PRODTYPE),'EmbeddedNT')<>0 &
   INDEX(EDMGETV(ZCONFIG,HALPVER),'6.1')<>1
   ```

   This expression facilitates ImageX based deployments and enables the WinPE SOS files to be downloaded to WES 7 clients. For Legacy deployments for WES7, the WinPE SOS files are not be used for the deployment. To download only the required Linux SOS files for Legacy deployments, manually set the ZSTOP expression to the following value:

   ```
   WORDPOS(EDMGETV(ZCONFIG,PRODTYPE),'EmbeddedNT')<>0
   ```

4. Restarts the reference machine into the service operating system (booted from the Image Preparation CD you created). Based on the type of the capture, the capture process boots into either Linux or Windows PE Service OS.
5. Creates and copies the following files to this directory on the RCA server:
   <InstallDir>`\Data\OSManagerServer\upload.`
   For Legacy capture

   - `ImageName.IMG`: This file contains the image. WES 7 images can be deployed to target machines with flash drives of equal size.
   - `ImageName.MBR`: This file contains the Master Boot Record information.
   - `ImageName.EDM`: This file contains the object containing inventory information.
   - `ImageName.PAR`: This file contains the object containing disk partition information.

   For ImageX capture

   - `ImageName.WIM`: This file contains the image. WES 7 images can be deployed to target machines with flash drives of equal size.
   - `ImageName.EDM`: This file contains the object containing inventory information.

   Note: While these files are transferred, network speed will be less than optimal.
   A comprehensive log (*machineID*`.log`) is available in *<InstallDir>*`\Data\OSManagerServer\upload` after the image is deployed.

Using the Image Preparation Wizard

To use the Image Preparation Wizard:

1. Insert the Image Preparation Wizard CD-ROM that you created into the CD-ROM drive of the reference machine. (Thin client devices require a USB CD-ROM drive). This CD is created using the `ImageCapture.iso` found within the `Media\iso\roms` directory on your HPCA media.
2. If autorun is enabled, the HPCA OS Preparation and Capture CD window opens.
3. Browse to the `\image_preparation_wizard\win32` directory.
4. Double-click **prepwiz.exe**. The Welcome window opens.
5. Click **Next**.
   The End User Licensing Agreement window opens.
6. Click **Accept**.
7. Select the capture method, **Legacy** or **ImageX**. You get this option only if the disk size is greater than 4 GB. Else, the capture happens through the Legacy method without showing any capture options.
8. Type the IP address or host name and port for the RCA server. This must be specified in the following format:
   xxx.xxx.xxx.xxx:*port*

   The RCA server port used for OS imaging and deployment in an RCA Core and Satellite installation is 3466. In an RCA Classic installation, port 3469 is reserved for this purpose.

   If the Image Preparation Wizard cannot connect to the RCA server, a message opens and you must:

   - Click **Yes** to continue anyway.
   - Click **No** to modify the host name or IP address.
   - Click **Cancel** to exit the Image Preparation Wizard.
9. Click **Next**.
   The Image Name window opens.
10. Type a name for the image file. This is the image name that will be stored in the `\upload` directory on the RCA server.
11. Click **Next**.
    A window opens so you can type a description for the image.
12. Type a description for the image file.
13. Click **Next.**
    The Options window opens.
14. Select the option, **Perform client connect after OS install** or **Redeploy OS after the upload is completed**.

    Select the **Perform client connect after OS install** check box to connect to the RCA server after the OS is installed to verify that the OS was installed properly. If this is not selected, the OS Connect will not occur automatically after the OS is installed.
15. Accept the defaults and click **Next**.
    The Summary window opens.
16. Click **Start**.

17. Click **Finish.** The wizard prepares the image.

    The device boots to the Image Preparation Wizard CD in the CD-ROM drive. Make the necessary configuration adjustments to ensure this will happen (for example, with some BIOS versions, you can hit F10 during the reboot process and change the boot order in the configuration settings).

    Note: You may want to create copies of the files stored in the `\upload` directory so that you can retrieve them if necessary.

    During the capture, status information is displayed on the Service OS screen. See "About the Windows PE Service OS Screen" on page 385 for more information.
    OS Image Preparation Wizard connects to the network, and stores the image on the HPCA server in the following directory:
    <InstallDir>`\Data\OSManagerServer\upload`

    When the upload process is complete, you will see the following messages

    ```
    OS image was successfully sent to the OS Manager Server

    **** If you had inserted a CD remove it now and reboot
    ```

18. Reboot the reference machine and readjust your boot settings, if necessary, to return to the original operating system.

Next, you will want to publish your image to the CSDB. See "Publishing" on page 387.

Windows CE OS images

This section explains how to prepare and capture a Windows CE thin client operating system image.

Note: Deploying an OS through LSB is not supported on Windows CE based HP thin client models t5550 and above.

Prepare the CE Reference Machine

- Product media
- Image Preparation CD-ROM
- If you select the Legacy method, the boot order must be set to CD before you start the capture process.

Before you capture the image, you must install the RCA agent on the Windows CE device.

See “Installing the RCA Agent on HP Thin Client Devices” in the *Radia Client Automation Enterprise Installation and Upgrade Guide* for details.

When you deploy an OS to a Windows CE device using Local Service Boot (LSB), there must be sufficient space available on the device to install and extract the LSB service. If the device reboots but fails to boot the Linux Service OS (SOS), the amount of “storage memory” allocated on the device may be insufficient—at least 10 MByte is required.

Follow these steps on the Windows CE device:

1. Click **Start**.
2. Select **Settings** > **Control Panel**.
3. Click the **System** icon.
4. Select the **Memory** tab.
5. Use the slider on the left to increase the **Storage Memory** to 10 MByte or more.

Run the Image Preparation Wizard

1. The Image Preparation Wizard performs the following tasks:
2. Creates an object that contains information (including hardware and BIOS capabilities) about the reference machine.
3. Restarts the reference machine into the service operating system (booted from the ImageCapture media). Based on the type of the capture, the capture process boots into either Linux or Windows PE Service OS.
4. Creates and copies the following files to *<InstallDir>*`\Data\OSManagerServer\upload` on the RCA server.
   `ImageName.IBR`
   This file contains the image. Thin Client image files are the same size as the reference machine's flash drive. Windows CE images can be deployed to target machines with flash drives of equal size. The file contains an embedded file system that will be accessible when the image is installed.

   `ImageName.EDM`
   This file contains the object containing inventory information.

   Note: While these files are being transferred, network speed will be less than optimal.

   A comprehensive log (*machineID*`.log`) is available in *<InstallDir>*`\Data\OSManagerServer\upload` after the image is deployed.

Using the Image Preparation Wizard

1. Insert the Image Preparation Wizard CD-ROM that you created into the CD-ROM drive of the reference machine (thin client devices require a USB CD-ROM drive). This CD is created using the `ImageCapture.iso` found within the `Media\iso\roms` directory on your HPCA media.
2. If autorun is enabled, the HPCA OS Preparation and Capture CD window opens.
3. On the CD, browse to the `\image_preparation_wizard\WinCE` directory.
4. Double-click `prepwiz.exe`. The Image Preparation Wizard opens.
5. Type the IP address or host name and port for the RCA server. This must be specified in the following format:
   xxx.xxx.xxx.xxx:*port*

The RCA server port used for OS imaging and deployment in an RCA Core and Satellite installation is 3466. In an RCA Classic installation, port 3469 is reserved for this purpose.

If the Image Preparation Wizard cannot connect to the RCA server, a message opens and you must:

- Click **Yes** to continue anyway.
- Click **No** to modify the host name or IP address.
- Click **Cancel** to exit the Image Preparation Wizard.

6. Click **OK**.
The wizard prepares the image.

   The device boots to the Image Preparation Wizard CD in the CD-ROM drive. Make the necessary configuration adjustments to ensure this will happen (for example, with some BIOS versions, you can hit F10 during the reboot process and change the boot order in the configuration settings).

   > **Note:** You may want to create copies of the files stored in the `\upload` directory so that you can retrieve them if necessary

   During the capture, status information is displayed on the Service OS screen. See "About the Windows PE Service OS Screen" on page 385 for more information.

7. The Image Preparation Wizard connects to the network, and stores the image in the following directory on the RCA server:
   <InstallDir>`\Data\OSManagerServer\upload`

   When the upload process is complete, you will see the following messages

   ```
   OS image was successfully sent to the OS Manager Server

   **** If you had inserted a CD remove it now and reboot
   ```

8. Reboot the reference machine and readjust your boot settings if necessary to return to the original operating system.

Next, you will want to publish your image to the Configuration Server DB. See "Publishing" on page 387.

ThinPro OS Images

This section explains how to prepare and capture a ThinPro operating system image.

Prepare the ThinPro Reference Machine

To prepare ThinPro client for image capture, you will need the following:

- HPCA media
- Image Preparation CD-ROM
- If you select the Legacy method, the boot order must be set to CD before you start the capture process.

Before you capture the image, you must install the RCA agent on the ThinPro device.

See “Installing the RCA Agent on HP Thin Client Devices” in the *Radia Client Automation Enterprise Installation and Upgrade Guide* for details.

To create a custom connection for xterm:

Note: If the HPCA Registration and Loading Facility (RALF) is not pre-installed on the reference machine, it should be installed after the HPCA agent is installed.

If you are using the ThinPro operating system, you may need to create a custom connection to create an xterm connection.

1. From the HP menu in the lower left corner, select **Shutdown**.
2. 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 will change from blue to red.
3. From the Control Center, click the **Add** drop down list and select the **custom** option.
4. Set Name to **xterm**.
5. Set Command to run to:
   `sudo xterm -e bash &.`
6. Click **Finish**.

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

Run the Image Preparation Wizard

The Image Preparation Wizard performs the following tasks:

1. Checks if there is enough free disk space on the machine and verifies that the RCA agent is installed. If there is not enough free disk space, the Image Preparation Wizard displays a message and terminates.
2. Creates an object that contains information (including hardware and BIOS capabilities) about the reference machine.
3. Restarts the reference machine into the service operating system (booted from the Image Prep CD you created). The Linux-based portion of the Image Preparation Wizard runs to collect the image and its associated files.
4. Creates and copies the following files to <*InstallDir*>`\Data\OSManagerServer\upload` on the RCA server.
   `ImageName.DD`
   This file contains the image. Thin Client image files are the same size as the reference machine’s flash drive. Linux-based images can be deployed only to target machines with flash drives of equal size. The file contains an embedded file system that will be accessible when the image is installed.

   `ImageName.EDM`
   This file contains the object containing inventory information.

Note: While these files are transferred, network speed will be less than optimal.

A comprehensive log (*machineID*`.log`) is available in <*InstallDir*>`\Data\OSManagerServer\upload` after the image is deployed.

Using the Image Preparation Wizard

1. Insert the Image Preparation Wizard CD-ROM you created into the CD-ROM drive of the reference machine (thin client devices require a USB CD-ROM drive). This CD is created using the `ImageCapture.iso` found within the `Media\iso\roms` directory on your HPCA media.

   Caution: On certain Linux thin client models, the CD-ROM may be mounted by default with the `noexec` option, which prevents execution from the CD-ROM. This will result in a permissions error or otherwise failed execution when trying to run the Image Preparation Wizard. Re-mounting the CD-ROM without the `noexec` option will resolve this issue.

2. On the Image Preparation CD, go to /`image_preparation_wizard/linux` and run `./prepwiz`.
   The Welcome window opens.
3. Click **Next**.
   The End User Licensing Agreement window opens.
4. Click **Accept**.
5. Type the IP address or host name and port for the RCA server. This must be specified in the following format:
   xxx.xxx.xxx.xxx:*port*

   The RCA server port used for OS imaging and deployment in an RCA Core and Satellite installation is 3466. In an RCA Classic installation, port 3469 is reserved for this purpose.

   If the Image Preparation Wizard cannot connect to the RCA server, a message opens and you must:

   - Click **Yes** to continue anyway.
   - Click **No** to modify the host name or IP address.
   - Click **Cancel** to exit the Image Preparation Wizard.
6. Click **Next**.
   The Image Name window opens.
7. Type a name for the image file. This is the image name that will be stored in the `\upload` directory on the RCA server.
8. Click **Next**.
   A window opens so you can type a description for the image.
9. Type a description for the image file.

10. Click **Next.**
    The Options window opens.
11. Select the appropriate options:
    Perform client connect after OS install

    Select this check box to connect to the RCA server after the OS is installed to verify the OS was installed properly. If this is not selected, the OS Connect will not occur automatically after the OS is installed.
12. Accept the defaults and click **Next**.
    The Summary window opens.
13. Click **Start** to start the preparation for image capture.
14. Click **Finish.**The wizard prepares the image.

    The device boots to the Image Preparation Wizard CD in the CD-ROM drive. Make the necessary configuration adjustments to ensure this will happen (for example, with some BIOS versions, you can hit F10 during the reboot process and change the boot order in the configuration settings).

    Note: You may want to create copies of the files stored in the `\upload` directory so that you can retrieve them if necessary.

    The Image Preparation Wizard connects to the network, and stores the image in the following directory on the HPCA server:
    <InstallDir>`\Data\OSManagerServer\upload`

    When the upload process is complete, you will see the following messages:

    ```
    OS image was successfully sent to the OS Manager Server

    **** If you had inserted a CD remove it now and reboot.
    ```
15. Reboot the reference machine and readjust your boot settings if necessary to return to the original operating system.

Next, you will want to publish your image to the CSDB for distribution to managed devices. See "Publishing" on page 387.

Publishing and Deploying OS Images

After you have captured an image, use the Publisher to publish it to the RCA database. For instructions, see "Publishing" on page 387.

After you publish an OS image to RCA, refresh the OS Library page on the Operations tab to view the new image. Use the RCA Console toolbar to deploy the image to selected devices.

About the Windows PE Service OS Screen

A Service OS is a pre-installation environment that is based on a lightweight operating system such as Linux or Windows PE. The Service OS does the following things:

1. Boots into the target hardware
2. Loads all the drivers that are needed in order for that hardware to function correctly
3. Downloads and runs RCA programs which, in turn, download and install OS images

The Service OS is used to perform the following types of operations:

- Operations to hardware on a target device (for example, a BIOS update or hardware configuration)
- Provisioning target devices (for example, deploying an OS)
- Capturing an OS image

Whenever a Service OS starts, the Service OS screen appears on the pertinent device. When an OS image is being captured, for example, the Service OS screen appears on the reference machine. When an OS is being deployed, the Service OS screen appears on the target device.

The Windows PE Service OS screen shows you the status of the operation. The right side of Windows PE Service OS screen shows you a scrolling log of the steps that are being performed.

- A green checkmark icon indicates that a particular step either is in progress or has been successfully completed.
- A yellow triangle icon is a warning that something may be wrong.
- A red X icon indicates that this step in the capture or deployment has failed.
- A blue question mark (?) icon indicates that input is required.

Information about the current step always appears at the bottom of the list of messages. A scroll bar appears on the far right if there is not enough room to list all of the messages.

If the operation is successful, a green check mark appears on the left side of the Service OS screen with further instructions.

At this point, you can take one of two actions:

- Click **Reboot** to reboot the device into the installed operating system.
- Click **Shutdown** to shut the device down.

After you click one of these buttons, a status message will appear briefly under the progress bar on the right side of the screen before the reboot or shutdown occurs.

If the operation is not successful, a red X appears on the left side of the Service OS screen with information about the nature of the failure. If the operation fails, you can use the scroll bar on the right side of the screen to view information about the hardware detected and determine where in the process the failure occurred. At this point, you can take one of three actions:

- Click **Reboot** to reboot the device into the installed operating system.
- Click **Shutdown** to shut the device down.
- Click **Exit to console** to close the Service OS screen and reveal the console window.

After you click one of these buttons, a status message will appear briefly under the progress bar on the right side of the screen before the action that you selected occurs.

Chapter 13

Publishing

Use the RCA Publisher to publish the following items to Radia Client Automation (RCA) database:

- Software
- Mobile Applications
- BIOS configuration settings
- HP Softpaqs
- Operating system images
- Virtual Applications

Published software is available in the Software Library on the Operations tab of the main RCA console. Published operating systems are available in the OS Library on the Operating Systems tab.

Note: The Publisher is installed automatically during the installation of the RCA Core. If the RCA agent is already installed on the machine, the Publisher will be installed in the agent's folder. If you want to install it in a different location, you can use the Radia Client Automation Administrator installation file on the product media or use the HPCA Administrator Publisher service in the Software Library. See *Installing RCA Administrator Tools* chapter in the *Radia Client Automation Enterprise Installation and Upgrade Guide* for more information.

Caution: Publishing is an administrative task that should be done in a non-production lab environment.

After you publish one of the items listed above, it can be entitled and deployed to managed devices in your environment. For additional information on HPCA Publisher, see *HP Client Automation Enterprise Administrator User Guide*.

Starting the Publisher

1. Go to **Start** > **All Programs** > **Radia Client Automation Administrator** > **Radia Client Automation Administrator Publisher**.
2. To log in to the Publisher use your RCA Administrator user name and password. By default, the user name is `admin` and the password is `secret`.

Note: Publishing options vary based on the intended target devices.

The following table lists the publishing options available in RCA Enterprise edition.

Publishing Options

Publishing Option	Enterprise
Component Select	Yes
Hardware Configuration	Yes
HP BIOS Configuration	Yes
HP Softpaqs	Yes
Mobile Application	Yes
OS Add-ons/extra POS drivers	Yes
OS Image	Yes
Windows Installer	Yes
Thin Client Component Select	Yes
Thin Client OS Image	Yes
Publishing Virtual Applications	Yes

Publishing Software

Depending on the type of software you intend to publish, you will use one of two publishing options. At the login screen, you are given the choice of Windows Installer to publish Windows Installer files (`.msi`) or Component Select to use when publishing non-Windows Installer files. The following sections explain the steps for publishing each file type.

- "Publishing Windows Installer Files" below
- "Publishing Using Component Select" on page 390

Publishing Windows Installer Files

Windows Installer uses MSI files to distribute software services to your operating system. The Publisher uses the files to create a service that is then published to RCA. When the software service is contained in RCA, it is ready for distribution to managed devices in your environment.

Publishing Windows Installer files

1. Start the Publisher (see, "Starting the Publisher" on previous page).
2. At the Logon window, type your administrator User ID and Password and click **OK**.

   Note: Log in to the Publisher using the RCA user name and password. By default, the user name is `admin` and the password is `secret`.

3. In the Publishing Options area, select **Windows Installer** and click **OK**.

4. Navigate to the Windows Installer file in the left pane. The right pane displays any information that is available for the MSI file you select.
5. Click **Next**.
6. Review the available Publishing Options.
   - **Management Options**
     To create an administrative installation point (AIP) select **Use setup** or **Use msiexec**..

     Note: The AIP path is a temporary location and will be removed after the publishing session completes.

   - **Transforms**
     Select and reorder the application of any transform files associated with the Windows Installer file.
   - **Additional Files**
     Include additional files as part of the AIP.
     - Click **Select all** to select all available files listed.
     - Click **Select none** to deselect all files.
   - **Properties**
     View and modify the msi file properties. Some Windows Installer files may require additional command line parameters to deploy correctly. For example, an application may require a custom property to pass a serial number during installation. Use the Properties dialog to include any additional parameters.
     - Click **Add** to add a new property.
     - Click **Remove** to delete an existing property.
     - To modify a property **Name** or **Value**, click the item you want to change and type the new value.

   When you are finished editing your publishing options, click **Next**.
7. Use the Application Information section to type the software service information.
8. Use the **Limit package to systems with** section to limit the service to any specific operating system or hardware. Click any link to display the configurable options.
9. Click **Next**.
10. Review the Summary section to verify the service information you provided during the previous steps. When you are satisfied, click **Publish**.
11. Click **Finish** when the publishing process is finished to close the Publisher.

The Windows Installer service is now ready for distribution to your enterprise.

Applying additional parameters using a transform file

1. Create the transform using Orca or another MSI editor. Be sure to save the transform in the same directory as the Window Installer file that you are publishing.
2. Start a Windows Installer publishing session. Follow the instructions above for details.
3. At the Edit step, click **Transforms**.

4. Select the available transform file and continue with the publishing session.
   When the software service is deployed, the transform file will be applied, supplying the additional command line parameters.

Publishing Using Component Select

To publish software other than Windows Installer files, use the Component Select option and select the software you want to publish.

Publishing using Component Select

1. Start the Publisher (see "Starting the Publisher" on page 387).
2. At the Logon window, type your administrator User ID and Password and click **OK**.

   Note: Log in to the Publisher using the RCA user name and password. By default, the user name is `admin` and the password is `secret`.

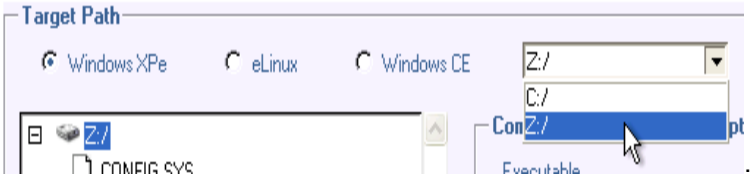
3. In the Publishing Options area:
   - If you are publishing for thin clients, select **Thin Client Publishing**.
   - From the drop-down list, select **Component Select**.
4. Click **OK**. The Select files to publish window opens.
5. Select the files to publish and click **Next**.

   Note: The directory path where the software is located (and published from) will be the directory path to where the software is deployed on target devices.

   Note: Although network shares are displayed, they should not be used to publish software (since they may not be available during deployment).

   The Target Path window opens.

6. If you are publishing for thin clients, select the install point, as shown in the following figure.



7. Enter the commands to run on application install and uninstall. For example, a command to run on install might be: `C:\temp\installs\install.exe /quietmode /automatic c:\mydestination`
   A command to run on uninstall could be: `C:\temp\installs\uninstall.exe /quietmode /automatic`

   Note: You can right-click any file to set it as the install or uninstall command.

8. Click **Next**. The Application Information window opens.

9. Use the Application Information section to type the software service information.
10. Use the **Limit package to systems with** section to limit the service to any specific operating system or hardware. Click any link to display the configurable options.
11. Click **Next**.
12. Review the Summary section to verify the service information you provided during the previous steps. When you are finished, click **Publish**.

Note: The Package Description you type while publishing is not displayed complete in the Publisher Summary UI. The service gets published to the CSDB without truncating the text in the Package Description field.

13. Click **Finish** when the publishing process is finished to exit the Publisher.

The software service is now ready for distribution to your enterprise.

Publishing Mobile Applications

Using RCA, you can publish Android application package (APK) files for the mobile devices on Android platform.

Complete the following steps to publish the `.apk` files to the CSDB:

1. Open the Radia Client Automation Administrator Publisher.
   a. From the computer where you have Administrator Tools installed, click **Start**>**All Programs**>**Radia Client Automation Administrator**>**Radia Client Automation Administrator Publisher**.
   b. Enter the user ID and password, and click **OK**. The default user ID is admin. The default password is secret.
   The Radia Client Automation Admin Publisher window opens.
2. Select **Mobile Application** from the Publishing Options drop-down list, and click **OK**. The Edit page opens.
3. Under Select Mobile application to publish, select the folder that contains the `.apk` file required to create the package for Android devices. The Summary area shows the details of the file that you have selected.
4. Click **Next**. The Configure page opens.
5. Under the Package Information area, type the following details:

Package Information details

Field	Description
Name	The name of the package. An instance with the value you provide in this field is created in the PACKAGE class of the MOBILESOFTWARE domain. This is a mandatory field.
Display Name	The friendly name of the package. This is a mandatory field.

Field	Description
Domain	The domain in which this instance is stored. The MOBILSOFTWARE domain is selected by default for mobile applications.
Description	Description of the package.
Release	The version number of the application that you are packaging.
Class	The class for which this package instance will be created.

6. Under the Limit package to systems with area, select the operating system and hardware settings for the device on which you want to deploy the application. Using Hardware settings, you can limit distribution based on minimum RAM or processor speed.
7. Click **Next**. The Service Information window opens. You can create a new service or use an existing service to deploy the package. Select No service if you do not want to associate this package with a service.
8. Click **Create new** and type the values for the Name, Display Name, Web URL, and Author field

   Note: In the current release, you can publish only mandatory applications using RCA. Additionally, you cannot select the events for which the details are sent to the upstream server. By default, all APPEVENTS for the mobile device agent are sent to the upstream server.
9. Click **Next**. The Publish window opens.
10. Review the Summary section to verify the service information you provided in the previous steps. When you are finished, click **Publish**.
11. Click **Finish** when the publishing process is completed to exit the Publisher.
12. Click **Yes** to confirm that you want to close the Publisher window.

Publishing Operating System Images

Operating system images created using the Image Preparation wizard are stored on the RCA server in the following directory:

<InstallDir>`\Data\OSManagerServer\upload`

You can use the Publisher to publish operating system image files for distribution to managed devices. The specific files that you will need depends on the deployment method that you intend to use (see "Publishing Operating System Images" above).

If you captured an OS image from a reference machine, you will need the files that resulted from that capture process. For more information, see "Preparing and Capturing OS Images" on page 365.

Caution: Do not publish factory OS images for thin client devices. All thin client images must

be captured before they are deployed to target devices.

See "Preparing and Capturing Thin Client OS Images" on page 374 for additional information.

Note: If you will be publishing `.WIM` images, see "Prerequisites for Publishing .WIM images" on next page before you begin the publishing process.

Files Needed to Publish OS Images

Deployment Method	Files Required	Refer To
Directly from a DVD	DVD `WIM` file RCA `unattend-dvd.xml`	"Pre-requisites for Publishing Directly from a DVD" on page 395

Microsoft ImageX	`ImageName.WIM`
	`ImageName.EDM`
	RCA `unattend-capture.xml`
		"Prerequisites for Publishing .WIM images" on next page

Windows Setup	`ImageName.WIM`
	`ImageName.EDM`
	RCA `unattend-capture.xml`
		"Prerequisites for Publishing .WIM images" on next page

Legacy	`ImageName.IMG`
	`ImageName.MBR`
	`ImageName.EDM`
	`ImageName.PAR`
	Windows CE:
	`ImageName.IBR`
	`ImageName.EDM`
	For Linux:
	`ImageName.DD`
	`ImageName.EDM`
		"Publish OS Images" on page 395

Note: The names of the `unattend` files shown in the table, Files Needed to Publish OS Images, see the files provided in the Image Capture ISO. You can change the name of this file as you see fit.

For information about customizing the `unattend` file, see "Customizing the Windows Answer File" on page 455.

Prerequisites for Publishing .WIM images

Note: The information in this section pertains to the following Windows operating systems:

- Windows XP SP2/SP3
- Windows 2003 SP1/SP2
- Windows Vista
- Windows Server 2008
- Windows 7
- Windows 8
- Windows Server 2008 Release 2 (R2)

If you are publishing a `.WIM` image of one of these versions of Windows, you must:

- Have access to the `Media\client\default` folder on the HPCA media.
  This folder is only required the first time you publish a `.WIM` file or if you want to publish an updated agent package. The RCA agent will be published as a separate package, which ensures that all future deployments of your `.WIM` files will automatically receive the latest agent available.
- For Windows Vista, Windows Server 2008, Windows 7, or Windows 8:
  If you are deploying using Windows Setup, you must be able to access the `\sources` folder from the Windows installation media (used to obtain or create the `.WIM` file) on the device where you are publishing the image.
- This does not apply to Windows XP or Windows 2003 `.WIM` files.
  The Windows Automated Installation Kit (AIK) for Windows 7 and Windows 8 must be installed on the device where you are publishing the image. This is a Core installation prerequisite. See the *Radia Client Automation Enterprise Installation and Upgrade Guide* for more information.
- If you are using an existing *filename*`.WIM`, copy the file to the device where you are publishing the image.
- If you prepared and captured a `.WIM` file using the Image Preparation Wizard, copy *filename*`.WIM` and *filename*`.edm` from the RCA server's `\upload` directory (*<InstallDir>*`\Data\OSManagerServer\upload`) to the device where you are publishing the image.
  If your file was spanned, copy `filename.swm`, `filename2.swm`, and so on from the `\upload` directory. The publishing process will rename these files automatically to *filename*`.WIM`, *filename*`.002`, *filename*`.003`, and so on.
- RCA provides a Windows Setup answer file that you can use for unattended installations. When you run the Publisher, you can choose to either use the answer file that RCA provides (preferred

method) or create your own. See "Specifying the Windows Setup Answer File" below for more information
The answer file that RCA provides is called `unattend.xml`. Each operating system and architecture (for example, 32-bit or 64-bit) has its own `unattend.xml` file. The files are located in subdirectories of:

<InstallDir>`\Data\OSManagerServer\capture-conf`

If you want to use the `unattend.xml` file that HP provides, you must modify it for your environment before you run the Publisher. At a minimum, you must specify the ProductKey for the image that you are publishing. You may also want to modify other settings in this file—for example, the TimeZone and the RegisteredOrganization. See "Customizing the Windows Answer File" on page 455 for details.

Caution: Confirm that all files and folders in the directory are not set to read-only. If they are set to read-only, the image may not deploy.

Pre-requisites for Publishing Directly from a DVD

Publishing an OS image directly from a DVD is the easiest method to use. This implies that the deployment will be done using Windows Setup. If you want to use straight image deployment, you must:

- Use the Image Preparation Wizard and select ImageX as the deployment method.
- Copy `install.wim` file from the DVD to a local folder on the device where you are publishing the image and mount the image capture ISO.

Specifying the Windows Setup Answer File

Before RCA version 7.90, it was necessary to manually modify and rename files used by RCA to support unattended installation of a particular OS image.

Now, you can specify the source of this information when you run the Publisher. This new method is much simpler and less prone to error than the manual method. It is the preferred method for specifying this information.

For backward compatibility, the old method is described in an appendix to this guide. See "Customizing the Windows Answer File" on page 455.

Publish OS Images

The following section describes how to use the Publisher to publish operating system images. There are four basic steps:

- Select the OS image
- Select the Windows Answer File for unattended installations (if needed)
- Specify the package options
- Publish

The following procedure provides detailed instructions. Note that the steps vary depending on the options that you choose.

Caution: Be sure to satisfy the "Prerequisites for Publishing .WIM images" on page 394 or "Pre-requisites for Publishing Directly from a DVD" on previous page before you start the Publisher.

Publishing Operating System Images

1. Start the Publisher. See "Starting the Publisher" on page 387.
2. In the Publishing Options area:
   - If you are publishing for thin clients, select **Thin Client Publishing**.
   - From the drop-down menu, select **OS Image**.
3. Click **OK**. The Select OS Image File page opens.
   Images created using the Image Preparation Wizard are stored on the RCA server in the following folder:

   <InstallDir>`\Data\OSManagerServer\upload`
4. Select the OS image file that you want to publish.
5. Use the **Description** area to verify that you have selected the correct file before you continue. You can also add information to the description if you choose.
6. Click **Next**.
7. If you did NOT select a `.WIM` file in step 4—for example, if you are publishing a thin client image—skip to step 18.
8. If you manually created `*.subs` and `*.xml` files for this image, skip to step 10. This is not recommended. See "Customizing the Windows Answer File" on page 455 for more information.
9. In the directory tree, select your Unattended Windows Answer File (`unattend.xml`).
   See "Prerequisites for Publishing .WIM images" on page 394 for additional information.
10. Click **Next**.
11. If you selected a `.WIM` file in step 4, perform *either* Action 1 or Action 2:
    Action 1: If you selected a `.WIM` file that was created using the Image Preparation Wizard method for ImageX deployment:

    a. From the **Deployment method** drop-down menu, choose **Microsoft ImageX**.

    b. Ignore the **Sources Directory** box.

    or

    Action 2: If you selected a `.WIM` file in step 4 that was created using the Image Preparation Wizard for Windows Setup deployment OR you are publishing a `.WIM` file from DVD media:

a. From the **Deployment method** drop-down menu, choose **Microsoft Setup**.

b. In the **Sources Directory** box, use the **Browse** button to select the `\sources` directory from the Windows installation media DVD. This Windows installation media DVD would be the same that was used to set up the reference machine that you captured using the Image Preparation Wizard.

> **Caution:** Always use the `\sources` directory from 32-bit Windows installation media DVD, even if you are publishing a 64-bit image file.

12. In the Client media location, browse to the correct path for the RCA Agent media (this is in the `Media\client\default` folder on the HPCA media).
Select the appropriate subdirectory, depending on the target platform that you are publishing for (either a regular machine or thin client).

    If you have already published this, you can select **Use an existing package published previously** and then select the appropriate package.

13. Click **Next**.

14. Use the **Package Information** section to type the details about this package. Note that the **Limit package to systems with** section is not available when publishing OS images.

15. Click **Next**.

16. In the **Service Information** section, select **Create new**.

> **Caution:** If you are publishing the agent, select **No service**.

17. Enter the appropriate Application Information in the remaining fields.
In the **Assignment type** group box, select **Mandatory**.

18. Click **Next**. The Summary window opens.

19. Review the **Summary** information to verify the package and service information that you provided during the previous steps. When you are satisfied, click **Publish**.

20. Click **Finish** to exit the Publisher when the publishing process is complete.

The service is now ready for distribution to managed devices in your enterprise.

You can view the published operating system image service in the OS Library on the Operations tab.

Publishing OS Add-Ons and Extra Production OS (POS) Drivers

> **Note:** For a detailed discussion of this process, see Customizing OS Deployment by Using Exit Points and Add-Ons in the *Radia Client Automation Enterprise OS Management Reference Guide*.

You can add drivers to previously prepared images by creating **delta packages** that are deployed after the image is installed on a new local partition. This is limited to the Microsoft Windows Setup and ImageX deployment methods.

Prerequisites

- Publish your OS service. The Publisher automatically creates a connection, OS.ADDON.ServiceName_*, under this service.
- If you are publishing OS drivers:
  - Create the following directory:
    `C:\MyDrivers\osmgr.hlp\drivers`
  - Store the individual drivers that you want to publish in this directory.

Publishing delta packages

1. Go to **Start** > **All Programs** > **Radia Client Automation Administrator** > **Radia Client Automation Administrator Publisher**. The Logon screen opens.
2. Type your RCA Administrator user ID and Password (by default, `admin` and `secret`).
3. In the Publishing Options windows select **OS Add-ons/extra POS drivers** from the drop-down list.
4. Click **OK**.
5. Use the Select Drivers Directory window, specify the following:
   a. In the directory tree, select the `C:\MyDrivers` directory.
   Everything below this directory will be recursively scanned, included, and published.
   b. From the **Add-on type** drop-down list, select **OS Driver** file.
   c. From the **Select Target Service** drop down list, select the OS service to which you want to add these drivers or add-ons.
   d. In the optional **Suffix** text box, you can type a number that can be used to track packages. For example, if the instance is called VISTA_PDD and you type 0 in this text box, then the new ADDON instance name will be VISTA_PDD_0.
   In the **ADDON Instance Name** text box, the instance name will be pre-populated based on the OS service name you selected. It is recommended that you leave this as is.

   It is recommended that you leave this name as is. If you modify this name, there will be no connection between the OS service and the ADDON instance unless you create the connection yourself.
6. Click **Next**.
7. Review the summary screen and click **Publish**.

You can use the CSDB Editor to review the new ADDON instance in PRIMARY.OS.ADDON. The next time the operating system service is deployed, the delta packages will automatically be deployed with it.

When this operating system service is deployed to a target device, the OS drivers are stored in the `C:\OSMGR.HLP\Drivers` directory on the target device.

Publishing HP Softpaqs

HP Softpaqs are bundles of support software, which may include device drivers, configuration programs, flashable ROM images, and other utilities available to keep devices up to date and performing at their optimum level.

Softpaqs are available as executable (.EXE) files.

Use the Publisher to publish HP Softpaqs to HPCA for distribution to managed devices.

Note: Publisher does not generate methods to uninstall HP Softpaqs. Therefore, HP Softpaqs cannot be uninstalled, once deployed.

To publish a Softpaq:

1. Start the Publisher (see To start the Publisher on page 339).
2. At the Logon window, type your administrator User ID and Password and click **OK**.

   Note: Log in to the Publisher using the HPCA user name and password. By default, the user name is admin and the password is secret.
3. In the Publishing Options area, select HP Softpaq and click **OK**.
4. The Select window opens. Select the Softpaq file to publish.
   - The Summary section shows the selected Softpaq information, including whether or not the Softpaq is SSM compliant. If the selected Softpaq is not SSM compliant and no silent install is included as part of the Softpaq, you must extract the Softpaq contents and read the accompanying documentation. Publish the required files and set up the installation method as instructed.
   - The System information dialog box shows all of the hardware the selected Softpaq supports.
5. Click **Next**. The Application Information window opens.
6. View, and if necessary, modify the Softpaq information. The application information is pre-determined based on what is available from the Softpaq file.
7. Click **Next**. The Summary window opens.
8. Review the summary information and when satisfied, click **Publish**.
9. When the publishing process is complete, click **Finish** to close the Publisher.

The Softpaq is published to HPCA and is available for distribution to managed devices. View the published Softpaq in the HPCA console Software Management, Software Library. Deployed Softpaqs are included within the HP Softpaq category group in the Application Self-Service Manager on managed devices.

Publishing BIOS Settings

Use the Publisher to publish a BIOS settings file as a service for distribution to client devices. You can use the settings file to update or modify BIOS settings (for example, boot order) or to change the BIOS password on the client device.

Two sample BIOS settings files (`HP desktop sample BIOS settings.txt and HP notebook sample BIOS settings.txt`) are included with the Publisher installation and located by default at: *<InstallDir>*`\Agent\BIOS`. Use these files to modify BIOS settings on target devices.

If the sample BIOS settings file does not include the options you require, or you would like to create a settings file for a specific device, see the *Publishing BIOS Settings* section below.

Publishing BIOS settings

1. Start the Publisher (see "Starting the Publisher" on page 387).
2. At the Logon window, type your administrator User ID and Password and click **OK**.

   Note: Log in to the Publisher using the RCA user name and password. By default, the user name is `admin` and the password is `secret`.
3. In the Publishing Options area, select **HP BIOS Configuration** and click **OK**. The Select window opens.
4. Select the BIOS settings file to publish. Two sample BIOS settings files (`HP desktop sample BIOS settings.txt and HP notebook sample BIOS settings.txt`) are included with the Publisher installation and located by default at: *<InstallDir>*`\Agent\BIOS`.
5. In the **Current BIOS Admin Password** area, type and then confirm a BIOS password if required. This is required to change any settings if the target devices have a BIOS password.
6. If you want to change the current BIOS password, select **Change BIOS Password**, then type and confirm the new password. This is required only if you want to change the BIOS password on a client device.
7. Click **Next**. The BIOS Options window opens.
8. To select the BIOS settings to be publishes select the check box to the left of the BIOS setting names.
9. If you need to change the value of a BIOS setting, click the setting name and adjust the available options as necessary.
10. Click **Next**. The Application Information window opens.
11. View, and if necessary, modify the application information. Application information is pre-determined based on what is available from the settings file.
12. Click **Next**. The Summary window opens.
13. Review the summary information. If it looks fine, click **Publish**.
14. When the publishing process is complete, click **Finish** to close the Publisher.

The BIOS settings service is available in the Software library of the RCA console.

Publish Hardware Configuration Elements

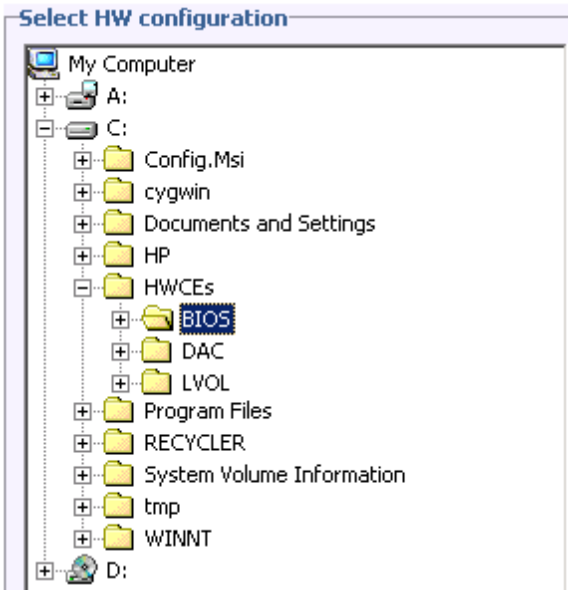
In this section, you will use the Publisher to publish Hardware Configuration Elements to the Radia Client Automation Configuration Server Database.

Before you publish your HWCEs, gather your resource files into a single folder. See the *Radia Client Automation Enterprise OS Manager Hardware Configuration Management User Guide* for more information.

Publishing a Hardware Configuration Element

1. Go to **Start** > **All Programs** > **Radia Client Automation Administrator** > **Radia Client Automation Administrator Publisher**. See the *Radia Client Automation Enterprise Administrator User Guide* for details on how to use the Publisher.
2. Type your User ID and Password.
3. From the Publishing Options drop-down list, select HW Configuration.
4. Click **OK**.
5. Select the folder that contains the resources needed to create your HWCE. In our example, we selected `C:\HWCEs\BIOS`.

   Caution: Make sure that you gathered the correct files that match the system to which you intend to deploy this. If you choose the wrong files you may leave your system in a damaged state.



6. In the Description field, type a description of the elements that you are publishing. For this example, type `Pro32 WS Bios Rev 1.00 Resources`.
7. In the Package Instance Name field, type the instance name for the package. For this example, type `P32_BIOS_100`.
8. Click **Next**.
9. Review the information and then click **Publish**. The package resources will be published in a non-compressed format.
10. When the Publisher is done, click **Finish**.
11. Click **Yes** to confirm that you want to close the Publisher.

Use the CSDB Editor to view the package that has been created in PRIMARY.OS.PACKAGE.

Publishing Virtual Applications

See *Radia Client Automation Enterprise Virtual Application Management User Guide*.

Viewing Published Services

View published software in the Management tab, Software Management area. Published operating systems are stored in the Operating System area.

Radia Client Automation Administrator Agent Explorer

Installed with the Publisher as part of the Radia Client Automation Administrator, the Agent Explorer is available to aid with troubleshooting and problem resolution and should not be used without direct instructions from Persistent Support.

Chapter 14

Configuring the Application Self-Service Manager

The Radia Client Automation Application Self-Service Manager (Self-Service Manager) is an agent sub-feature that is installed on the client devices during agent deployment. The Self-Service Manager provides users with a catalog that lists the applications to which they are entitled. The applications are entitled to the users by an RCA administrator. End-users can self-manage the installation, removal, and updating of the applications.

RCA Administrator Functions

As an administrator, you can define the applications that should be entitled to a user. You can also modify the display of the Self-Service Manager in user's environment.

The following section lists the tasks that you can perform to configure the Self-Service Manager.

- Modify the Self-Service Manager User Interface: Use the RADUICFG class in the CLIENT Domain to control the display of the Self-Service Manager user interface. For more information on RADUICFG class, see Appendix B, RCA Agent Settings Classes in CLIENT Domain (Client Operations Profile) in the *Radia Client Automation Enterprise Application Manager and Application Self-Service Manager Reference Guide*.
- Create Virtual Catalogs: Virtual catalogs are subsets of the default catalog defined by specifying a name in the CATGROUP value for a service. Any services with the same CATGROUP value will be grouped together in a virtual catalog. To set the CATGROUP attribute, complete the following steps:
  - Open the CSDB Editor.
    i. From the computer where you have Administrator Tools installed, click **Start** > **Programs** > **Radia Client Automation Administrator** > **Radia Client Automation Administrator CSDB Editor**. The RCA Administrator CSDB Editor Security Information dialog box opens.

    ii. Type the user ID and password, and click **OK**. The default user ID is `admin`. The default password is `secret`.
  - In the Database Tree View, double-click **PRIMARY** file, and then expand the **SOFTWARE** domain.
  - Double-click the name of the service you want to add to a virtual catalog.
  - Double click the **CATGROUP** attribute and type the name of the virtual catalog you want to add the service to, and then click OK.
- Service List Options: The Service List section in the Self-Service Manager lists the available applications to the end-user. You can modify the MSI installer behavior using the UIOPTMSI attribute, such that an end-user is able to view and interact with the installer using the interface. Based on your requirement, set the UIOPTMSI attribute of the MSI applications that are

deployed using the RadiaMsi to one of the following options:

- `UIOPTMSI=FULL`: Full interface is displayed. A modal dialog box is displayed and allows the user to interact with the interface.
- `UIOPTMSI=INFO`: Reduced interface is displayed. A modal dialog box is displayed and the user is not able to interact with the interface or cancel the installation. See the MSI installer log files and the Windows Event Viewer logs for errors or warnings.
- `UIOPTMSI=NULL`: No interface is displayed.

> **Note:** For Vista and above the Microsoft Installer UI will not be displayed if the variable `ZSERVICE.ZSYSACCT = Y`

- Provide Software Reconfiguration Options: Use the Reconfigure option in the Service List section to reconfigure the installation of software on your computer. The reconfigure option enables you to re-install the selected software to adjust different configurations, for example, the directory where the software was installed.

  > **Note:** The **Reconfigure** button is available only if the application is installed and the RECONFIG variable is set to `Y` in the ZSERVICE instance for the application.

- Scheduling Timed Events: After selecting an installed service, select **Schedule** from the Services menu to specify a schedule that will automatically update the applications that are installed on your computer. For example, you can schedule updates to occur during non-business hours, when you are not using your computer and network traffic is slower.

  > **Note:** The **Scheduling** dialog box is only enabled when an Application Service (ZSERVICE) has the SCHEDOK attribute set to `Y`, indicating the Administrator authorized local scheduling capabilities on the selected service.

RCA Agent Self-maintenance

Maintenance for the RCA agents is available from Persistent Technical Support. The maintenance includes import decks for the Configuration Server Database. New instances are created in the PRDMAINT Class in the PRDMAINT Domain; there is one PRDMAINT instance for each PRODUCT_PLATFORM combination. These instances are connected based on the RCA agent's platform and current product level. After you have identified the need to deploy the maintenance to the RCA agent computers, add the service to the user's entitlements.

To minimize the need for separate PRDMAINT bundles for different operating systems requiring the same maintenance, the ZMASTER.ZOSTYPE variables identify the Windows operating system type or family.

Usage Notes

- All packages are disabled by default. This is accomplished by setting a ZSTOP expression to `1` to prevent deployment. Either remove this value for general deployment, or use this ZSTOP expression to restrict its deployment to certain groups.

- The first REQUIRES connection is reserved for any possible hot fix, a fix that is sent to you directly by Technical Support is not yet available in a fix or service pack. This package, _ HOTFIX, will be used to chain any required fixes (and/or enhancements) and will be maintained by the customer. The second connection is for any locally customized code to be included as part of maintenance.
- Use the ACTMAINT attribute in the SETTINGS Class of the CLIENT Domain to specify how you want maintenance processed. You can choose to immediately download and install maintenance (**I**), download only and install later (**D**), or prompt users to install maintenance at another time (**P**).
  Maintenance runs only when the RADSKMAN parameter `mnt=Y`. For more information on ACTMAINT and mnt parameter, see the *Radia Client Automation Enterprise Application Manager and Application Self-Service Manager Reference Guide*.

HP provides an updated PRDMAINT instance with each new maintenance pack. The customer is not required to apply all maintenance.

Deploying RCA Agent maintenance packages

1. A maintenance package is made available on the Persistent support web site in the form of an export deck.
2. Download the files. There should be at least an `xpi` and `xpr` file.
3. Stop the Configuration Server service and copy the export files to the Configuration Server `\bin` directory.
4. Import the files using the ZEDMAMS utility.
   For example, if you are given two files, `MAINT_RAM_40_RC3.XPI` and `MAINT_RAM_40_RC3.XPR`, you might use the following command lines:

   ```
   ZEDMAMS VERB=IMPORT_INSTANCE,FILE=MAINT_RAM_40_RC3.XPI,PREVIEW=NO

   ZEDMAMS VERB=IMPORT_RESOURCE,FILE=MAINT_RAM_40_RC3.XPR,PREVIEW=NO
   ```

   Note: Your command line could vary depending on a number of factors. For detailed information on EDMAMS, see the *Radia Client Automation Enterprise Configuration Server Reference Guide*.
5. Restart the Configuration Server.
6. Assign the Maintenance Server to the appropriate users in the POLICY Domain.

   Note: To run the maintenance portion of an RCA agent connect process, the `mnt` parameter of the RADSKMAN command line must be set to `Y`.

During catalog processing, the RCA agent will process all services found in the PRDMAINT Domain, perform arbitration to determine appropriate maintenance, and deploy the maintenance to the maintenance staging directory. The default location for this is *<InstallDir>*`\Agent\_Maint_`.

HPCA System Tray

The bandwidth control shows when bandwidth throttling is available (based on the throttling type for the service, Reserved). In addition, the bandwidth slider will be displayed if the throttling type is valid and the UIOPTION attribute of the Application (ZSERVICE) instance is set to FULL. FULL is the default value. Set UIOPTION to INFO to show what is happening on the agent computer, but disable all the controls so that the subscriber cannot make any changes. Set the UIOPTION to NONE so that no dialog boxes are displayed. Set the UIOPTION using the RCA Administrator CSDB Editor.

User Actions for Mandatory Services

This section describes the user options available for Connect Deferral and Reboot Deferral.

Using Connect Deferral

The **Connect Deferral** (CDF) window enables an RCA administrator to give users several options when service "actions" (such as a software installation) are pending for their machine. This feature lets users decide—based on their current activity—whether to immediately take the required actions, or defer them to a more convenient time.

An RCA administrator can specify two "deadline" type counters for the required actions.

- The "deferral" days remaining is displayed on the right side of the window. The user will be able to repeatedly defer the actions—but only for the duration that is established by an administrator—to a point where the actions will be performed automatically on the user's machine.
- The dialog countdown timer that is displayed in the bottom of the window indicates the number of minutes before the dialog is automatically dismissed and the "Allow" action forced. When the countdown reaches 1 minute, the timer changes to display the number of seconds, and is refreshed every 5 seconds. If the counter reaches 0 (zero) and the user has taken no action, the "Allow" action will be forced.

If you run a connect to install user components of a service specifying `context=u` as a connect parameter in the command line, the CDF window is not displayed. For more information on the machine and user components of a service, see *Appendix E*, *Configuring Services Using Advanced Capabilities* in *Radia Client Automation Enterprise Administrator User Guide*.

Connect Deferral for Service Groups

Service Groups are a group of services. They consist of a master service and one or more member services. The master service is the container or representative for the member services, that contain the resources to be deployed. CDF displays only the master service for a particular service group. For more information on Service Groups, see *Radia Client Automation Enterprise CSDB Editor Online Help*.

Connect Deferral Options

The Connect Deferral window presents information about the required actions and offers several options to the user. The columns of the Connect Deferral window are described in the following table.

Connect Deferral Window Columns

Column	Description
Service	This column displays the service name that requires user action.
Action	This column displays the resulting effect on the machine when the user action is taken. This can be: • **Delete**: remove the service from the machine • **Install**: install the service on the machine • **Update**: update an existing service on the machine
Type	This column lists the type of service. A service type can be: • OS (operating system) • Patch • Software
Reboot	This column displays the values **Yes** or **No** based on the user action specified in the Action column for the service. For example, if a service with user action Install requires you to restart the computer after the installation process is complete, the Reboot column will display Yes.
Size (in MBs)	This column displays the size of the service.

Note: A Connect Deferral window for Patch connects does not display individual services and actions required by services.

Connect Deferral User Actions

The user options for pending services are:

- **Allow**
  This results in the immediate execution of the activities that are listed in the Action column.
- **Cancel**
  This causes the current connection to the Configuration Server to be ended; the action will remain pending in future connections.
- **Defer**
  This is used in conjunction with the **Defer for** drop-down list. The user can postpone taking action on the services by selecting a deferral interval.

- **15 minutes** makes the current connection to the Configuration Server sleep for fifteen minutes; a ZTIMEQ object will not be created.
- The other intervals will result in the creation of a ZTIMEQ object.

Using Reboot Deferral

The **Reboot Deferral** (**RDF**) feature enables an RCA administrator to configure reboot operations on user machines. This feature lets users decide whether to reboot the machine immediately or defer the reboot to a more convenient time.

An RCA administrator can specify two “deadline” type counters for the required actions.

- The “deferral” days remaining is displayed on the right side of the window. The user will be able to repeatedly defer the actions—but only for the duration that is established by anadministrator—to a point where the actions will be performed automatically on the user’s machine.
- The dialog countdown timer that is displayed in the bottom of the window indicates the number of minutes before the dialog is automatically dismissed and the “Reboot” action forced. When the countdown reaches 1 minute, the timer changes to display the number of seconds, and is refreshed every 5 seconds. If the counter reaches 0 (zero) and the user has taken no action, the “Reboot” action will be forced.

Reboot Deferral User Actions

The user options for reboot are:

- **Reboot**: reboots the machine immediately..
- **Cancel**: cancels the reboot process for now; the reboot action however, remains pending.
- **Defer**: defers the reboot to a later time. This is used in conjunction with the drop-down list. The user can postpone the reboot operation by selecting a deferral interval.

Enabling Reboot Deferral

If enabled, the Reboot Deferral window is displayed in place of the basic Reboot panel. To enable the Reboot Deferral window, see the *Radia Client Automation Enterprise Application Manager and Application Self-Service Manager Reference Guide.*

Applications: Alert Messages and Deferrals

Use the RCA Administrator CSDB Editor to show the subscriber that an application has a high priority or to display an additional message. An Application (ZSERVICE) Instance can be set to *normal* or *high* priority. An exclamation point (**!**) denotes that an application is high priority.

Note: If you are using HPCA Application Self-Service Manager with the HPCA System Tray to manage a high priority service and an alert condition arises, the alert bubble will “pop” and the message is displayed in the status bubble of the System Tray icon.

When an application is deployed, an administrator can—based on the network threshold, the data-download size, a date setting, or a deferral count—have a deferral message displayed. When an application has data that needs to be downloaded to the RCA agent computer, the RCA agent will check whether the application is configured for deferral. If it is, the Application Self-Service Manager checks the current bandwidth setting against the administrator-specified bandwidth threshold setting. A deferral message, asking whether the subscriber wants to defer the deployment, is displayed if:

- The current network speed is slower than the Network Threshold (DT) value AND the size of the service is greater than the *below-threshold size* (DBT) value
  Or
- The current network speed is faster than the Network Threshold (DT) value AND the size of the service is greater than the *above-threshold size* (DAT) value

An RCA administrator can configure “number-of-occurrences” and “last-deferral-date” application-deferral limits. If the number of deferrals or the deferral date is reached, the application is installed or updated without displaying a deferral message.

An RCA administrator can also configure a “minimum-byte-count” limit on which to alert. If the size of the data is less than the minimum byte count, the alert panel is skipped.

If an application has been configured for a deferral and all of the requirements that are listed below are met, the RCA agent displays the deferral message.

- The Alert Mode (DM) is configured (`=Install`, `Update`, or `Both`) for the current operation.
- The current network speed is slower than the Network Threshold Speed (DT) and the data to be downloaded is greater than the below threshold size (DBT).
- The current network speed is faster than Network Threshold Speed (DT) and the data to be downloaded is greater than the above threshold size (DAT).
- The UIOPTION attribute in the ZSERVICE instance is set to something other than `NONE`.
- If specified, the deferral date, Allow Install Deferral up to (DI), or Allow Update Deferral up to (DU) has been reached.
  Or
- The number of deferrals allowed (DN) has been reached.

If these requirements are met and you are using the Application Self-Service Manager, the deferral message is displayed to the user. Who can then choose to defer the action or continue with it.

If the user does not respond to the defer/continue, the action that is identified in the DA attribute is taken. For information on DA attribute, see DA .

The following sections describe how to create and configure alert/deferral instances in the Configuration Server Database.

Alert Message and Deferral Instances in the Configuration Server Database

To implement an application alert or deferral, you must create an instance in the Alert/Defer (ALERTDEF) Class of the CSDB and connect it to the appropriate Application (ZSERVICE) Class instance.

Creating a Deferral Instance

The Alert/Defer (ALERTDEF) Class has been added to the SOFTWARE Domain in the CSDB to facilitate the configuring of application alerts. To configure an alert, create an instance in the Alert/Defer (ALERTDEF) Class.

Creating an instance of the Alert/Defer (ALERTDEF) Class

1. Navigate to **Start** menu and invoke RCA Administrator CSDB Editor. The **Security Information** dialog box opens.

   Note: The default user ID and password are:

   User ID: `ADMIN`

   Password: `secret`

2. If necessary, type a User ID and Password, and then click **OK**. The RCA Administrator CSDB Editor window opens.
3. Navigate to the **SOFTWARE** Domain of the **PRIMARY** File, and right-click **Alert/Defer (ALERTDEF)**. A shortcut menu opens.
4. Click **New Instance**. The **Create Instance** dialog box opens.
5. Type a name (such as SalesAlert) for the new instance.
6. Click **OK**.

The new (SalesAlert) instance has been created.

Configuring a Deferral Instance

Once the instance is created, you need to configure it for your alert. The Alert/Deferral (ALERTDEF) Class includes two sample instances, Dial Up Sample Defer and LAN Sample Defer. In this exercise, we will use the SalesAlert instance that was previously created.

Configuring an Alert/Deferral (ALERTDEF) instance

1. Use the RCA Administrator CSDB Editor to navigate to the SalesAlert instance.
2. Double-click the **SalesAlert** instance.
3. Double-click the variable that you want to edit.
   For information on the attributes for this class, see the following table.

Variables in the ALERTDEF Class

Variable	Description
ALERTMSG	An exclamation point (**!**) preceding “Service Alert Message” denotes a high priority message.
DM	Alert Mode The type of activity for which a deferral alert is triggered. ▪ Set to `I` for **Installations**.

Variable	Description
	▪ Set to `U` for **Updates**. ▪ Set to `B` (the default) for **Both** (installations and updates).
DN	The maximum number of deferrals that is allowed before the DA (Deferral Action) action is taken. The default is **0**.
DT	The network bandwidth threshold, in bytes. The current network speed must be less than this value to meet the deferral requirement. The default is **86000**.
DBT	The minimum cumulative size (in bytes) of the files that are being downloaded on a slow network and which triggers the deferral. The default is **50000**. A deferral is triggered if the network speed is slower than the Network Threshold (DT) value AND the cumulative size of the files that are being downloaded exceeds this value (`DBT=`*n*). If `DBT=0`, it is ignored (there is no deferral if the speed of the network is below the Network Threshold (DT) value).
DAT	The minimum cumulative size (in bytes) of the files that are being downloaded, a fast network and which triggers the deferral. The default is **0**. A deferral is triggered if the network speed is faster than the Network Threshold (DT) value AND the cumulative size of the files that are being downloaded exceeds this value (`DAT=`*n*). If `DAT=0`, it is ignored (there is no deferral if the speed of the network exceeds the Network Threshold (DT) value).
DTO	The duration (in seconds) for which the **Defer Alert** dialog box displays; the default is **120**. After the timeout is reached, the DA (Action on timeout) action is taken.
DA	The action that is taken if the subscriber does not respond to the **Defer Alert** dialog box in the time that is allowed by the DTO (Alert Timeout) variable. ▪ Specify `C` (the default) to continue with the specified action. ▪ Specify `D` to defer the specified action.
DI	The threshold date (in YYYYMMDD format) after which the option to defer the application installation is no longer available—the application is installed.
DU	The threshold date (in YYYYMMDD format) after which the option to defer the application update is no longer available—the application is updated.
Name	The friendly name for the instance.
DEFOPTNS	This attribute is used to resolve the values of the other attributes of this class. The default is **&(DM),&(DN),&(DT),&(DBT),&(DAT),&(DTO),&(DA),&(DI),&(DU)**. Do not modify this value.

In this exercise, add an alert message with high priority. To do this, double-click the **ALERTMSG** variable.

4. In the text field, type the message that you want to be displayed.

5. Click on the next attribute, and type in the appropriate value.
6. Click **OK** when you are finished editing the attributes. The **Instance Edit Confirmation** dialog box opens.
7. Click **Yes** to confirm the changes.

The **SalesAlert** Instance has been configured with an alert message.

Connecting a Deferral Instance

Now that the Alert/Defer (ALERTDEF) Instance (SalesAlert) is created and configured, it must be connected to an Application (ZSERVICE) instance.

Use RCA Administrator CSDB Editor to click and drag the SalesAlert Instance to the Application (ZSERVICE) Instance with which you want the alert message to be associated.

For additional information on RCA Administrator CSDB Editor, see *Radia Client Automation Enterprise CSDB Editor Online Help*.

Chapter 15

Personality Backup and Restore

The RCA Personality Backup and Restore solution enables you to back up and restore user files and settings for applications and operating systems on individual managed devices. Files and settings are stored on the RCA Core server and are available for restoration to the original device or a new device. Alternatively, you can back up and restore files and settings locally on a managed device.

You can use the RCA Personality Backup and Restore solution to migrate files and settings as part of an operating system deployment.

The RCA Personality Backup and Restore solution is based on the Microsoft User State Migration Tool (USMT). It enhances USMT by providing both remote and local management of the migration store created by USMT. It also downloads the required USMT control files to eliminate the need to deploy those separately. RCA supports USMT versions 3.0.1 and 4.0.

Note: Backups created with versions of RCA before HPCA 7.5 cannot be restored, because they were based on a different backup technology.

The following sections explain how to implement the RCA Personality Backup and Restore solution in your environment.

- "Requirements" below
- "About USMT" on page 415
- "Using Personality Backup and Restore" on page 418

Requirements

Before you implement the Personality Backup and Restore solution, make sure that the USMT version on RCA agent and RCA Core server is same and your environment meets the following requirements.

- "Operating System" below
- "Disk Space" on next page
- "Software" on next page

Operating System

You can create backups from source computers with the following operating systems:

- Windows XP
- Windows Vista

- Windows 7
- Windows 8

You can restore files and settings to destination computers with the following operating systems:

- Windows XP
- Windows Vista
- Windows 7
- Windows 8

Note: The `/hardlink` option can only be used for restore operations on Windows Vista and Windows 7 operating systems. It can be used for backup on Windows XP SP2 and later operating systems.

See "Using the Command Line Interface" on page 422 for more information.

Disk Space

Before you begin, you must make sure that your source computer, destination computer, and the RCA Core server have adequate disk space to store the files and settings that will be backed up. To estimate the disk space that will be needed for the backup, see “Determine Where to Store Data” on the Microsoft TechNet website at the following URL:

http://technet.microsoft.com/en-us/library/cc722431.aspx.

Note that the storage location is automatically set by RCA, and each of the source computer, destination computer, and RCA Core server must have adequate disk space available for the files and settings being migrated.

Also note that the destination computer needs to have twice the disk space required by the files and settings being migrated.

If you use the RCA Personality Backup and Restore Utility, the RCA Core server stores the archived user files and settings that were created during the backup. During a restore, the archived files and settings are downloaded to a temporary location on the destination computer and then restored to their original location. After a successful restore, the archived files and settings are deleted from the destination computer.

If you use the `pbr.exe` command with the `/localstore` option, backups are stored locally on the disk under `C:/OSMGR.PRESERVE/PBR.work`. The backups are not deleted, because they are the only copy of those files.

Software

You need the following applications:

- **Microsoft USMT version 3.0.1 or 4.0**
  This application must be installed in the default location on the source and destination devices. See the "About USMT" on next page.

> **Caution:** This solution requires that you use Microsoft USMT version 3.0.1 or version 4.0. No other versions of USMT are supported.

- **Radia Client Automation Personality Backup and Restore**
  This application must be installed on both the source and destination devices. It is installed automatically when the RCA agent is installed on a managed device.

About USMT

Because the RCA Personality Backup and Restore solution is based on the Microsoft User State Migration Tool (USMT), you should become familiar with this tool and its capabilities by reviewing its documentation on the Microsoft Technet web site at the following URL:

http://technet.microsoft.com/en-us/library/cc722032.aspx.

This section describes Microsoft USMT; how to obtain it, install it, and how to use its migration files. For a description of the Hewlett-Packard user interface provided with the Personality Backup and Restore solution, which invokes USMT automatically during a backup and restore, see "Using the RCA Personality Backup and Restore Utility" on page 419.

Supported Files, Applications, and Settings

USMT migrates a wide variety of data including user files and folders (e.g., the My Documents folder on XP or the Documents folder on Vista), operating system settings (e.g., folder options and wallpaper settings), and application settings (e.g., Microsoft Word settings). For a comprehensive list see “What does USMT 3.0 Migrate?” on the Microsoft TechNet web site at the following URL:

http://technet.microsoft.com/en-us/library/cc722387.aspx

Also see “What’s New in USMT 4.0?” at the following URL:

http://technet.microsoft.com/en-us/library/dd560752.aspx

> **Note:** For application settings to migrate successfully, the version of an application should be identical on the source and destination computers. There is one exception. You can migrate Microsoft Office settings from an older version on a source computer to a newer version on a destination computer.

> **Note:** USMT only migrates application settings that have been accessed or modified by the user. Application settings that have not been accessed by the user on the source computer may not migrate.

> **Note:** Some operating system settings, such as fonts, wallpaper, and screen saver settings, are not applied until after a reboot on the destination computer.

Obtaining and Installing Microsoft USMT 3.0.1 or 4.0

You might want to install USMT for one or both of the following reasons:

- As an administrator, you want to become familiar with the capabilities of USMT and to learn how to customize the migration rules for your personalized solution.
- As an end user, you want to be able to back up and restore files and settings on managed devices.

If you want to implement Personality Backup and Restore, you must install Microsoft USMT 3.0.1 or 4.0 on the source computer for backup, and on the destination computer for restore. This section explains where you can obtain this application, and how to install it.

Caution: You must use Microsoft User State Migration Tool, version 3.0.1 or 4.0. No other versions of USMT are supported.

Obtaining Microsoft USMT 3.0.1

USMT 3.0.1 is available at the Microsoft Download Center:

http://www.microsoft.com/downloads

There are two versions: 32-bit and 64-bit. Select the appropriate version for your environment.

Obtaining Microsoft USMT 4.0

USMT 4.0 is part of the Windows Automated Installer Kit (AIK) for Windows 7, which is available at the Microsoft Download Center:

http://www.microsoft.com/downloads

There are two versions: 32-bit and 64-bit. Select the appropriate version for your environment.

Note: See "Using the Command Line Interface" on page 422 for information about how the `/hardlink` option can be used on the various supported operating systems.

Installing Microsoft USMT on Managed Devices

You can install USMT on managed devices in two ways. You can install it manually, or you can package it into a service using the RCA Administrator Publisher (see "Publishing" on page 387) and then entitle or deploy it to managed devices. USMT must be installed in the default location on both the source and destination client devices:

Default USMT Installation Locations

USMT Version	Default Location
3.0.1 (Standalone)	`C:\Program Files\USMT301`
3.0.1 (with Windows AIK)	`C:\Program Files\Windows AIK\Tools\USMT`

USMT Version	Default Location
4.0 (Standalone)	`C:\Program Files\USMT4.01`
4.0 (with Windows AIK)	`C:\Program Files\Windows AIK\Tools\USMT`

Be certain to install the appropriate version (32-bit or 64-bit) based on the operating system of the managed device. If USMT is not installed in the default USMT paths, listed in the table above, add the following environment variable with the path, where you have installed USMT, set.

`PBRUSMTPATH=<"Complete path where USMT is installed">`

Migration Files

The Personality Backup and Restore solution uses the following USMT migration files to specify the components to include in the migration.

- `MigSys.xml` – migrates operating system settings
- `MigApp.xml` – migrates application settings
- `MigUser.xml` – migrates user folders and files

Note: In USMT 4.0, the `MigSys.xml` is renamed as `MigDocs.xml`. If you are prompted for the MigSys.xml file, copy MigDocs.xml as MigSys.xml.

Before you implement this solution in your environment you must obtain these files and store them on the RCA Core Server (see "Storing the Migration Rules on the Core Server" below).

To obtain these files you must install USMT on one of its supported platforms (see "Obtaining and Installing Microsoft USMT 3.0.1 or 4.0" on previous page). The installation places these files in the directories shown in Installing Microsoft USMT on Managed Devices.

You can then edit these files (see "Editing the Rules" below) or use them as is.

Editing the Rules

In some instances you may want to edit the default migration rules. For example, you may not wish to migrate settings for a particular application or may want to exclude a particular file type. To modify the default migration behavior, you need to edit the migration XML files. See the following document to learn how to customize these files:

http://technet.microsoft.com/en-us/library/cc766203.aspx

Storing the Migration Rules on the Core Server

When you are finished editing the migration files—or even if you choose not to edit them—save the files in the following folder on the RCA Core server:

DataDir`\PersonalityBackupAndRestore\conf`

Here, *DataDir* is the user-configurable data directory specified during the RCA Core installation.

Note: The migration files must have the same file names as the original files obtained from the Microsoft USMT 3.0.1 or 4.0 installation: `MigSys.xml`, `MigApp.xml`, and `MigUser.xml`.

ScanState and LoadState Command Lines

The migration rules are downloaded from the Core Server by the Personality Backup and Restore Utility and are used by the USMT executables ScanState and LoadState that collect and restore the personality data. `ScanState.exe` is the executable that collects personality data on the source computer. Here is the ScanState command line that is used by the Personality Backup and Restore Utility:

```
ScanState.exe /i:MigApp.xml /i:MigUser.xml /i:MigSys.xml /o
/l:ScanState.log /localonly "Agent\Lib\PBR\work\store"
```

where *Agent* is the agent's installation directory.

LoadState is the executable that restores the personality data to the destination computer. Here is the LoadState command line that is used by the Personality Backup and Restore Utility:

```
LoadState.exe /i:MigApp.xml /i:MigUser.xml /i:MigSys.xml
/l:LoadState.log /lac:password /lae "Agent\Lib\PBR\work\store"
```

Here, *Agent* is the agent's installation directory.

These command lines are not customizable, but are provided here to facilitate your understanding of what is being backed up and restored. Note that these ScanState and LoadState command line arguments automatically migrate all user accounts on a system, including local user accounts. If, when the restore is performed, a local user account does not exist on the destination computer, LoadState will create it with a password of `password` (see command line above). Therefore, after the restore, you should change the password of any restored local user accounts.

Using Personality Backup and Restore

There are three ways that you can access the RCA Personality Backup and Restore feature:

- "Using the RCA Personality Backup and Restore Utility" on next page
- "Using the Personality Backup and Restore Services" on page 423
- "Using the Command Line Interface" on page 422

All three methods invoke the same RCA application, which is called `pbr.exe`. Each time that `pbr.exe` runs, it downloads the three migration XML files (see "Migration Files" on previous page) from the RCA Core server to the managed device and uses these files to perform the backup or restore.

By default, `pbr.exe` stores the backup files on—and restore them from—the following location on the RCA Core server:

DataDir`\PersonalityBackupAndRestore\backups`

Here, *DataDir* is the data directory specified during the installation of the RCA Core. A subdirectory is created under the `backups` folder for each managed device that is backed up, and it contains all of the information that is required for a restore.

Note: If you want to store the backup files on the local hard disk of the managed device instead of on the RCA Core server, you can use the `pbr.exe` command with the `/localstore` option. In this case, the files are stored on the local disk in the following location:

`C:/OSMGR.PRESERVE/PBR.work`

All of the information that is required for a restore is stored in this location.

If you are using USMT version 4.0 (included in the Windows AIK for Windows 7), you can specify the `/hardlink` option to create a hard-link migration store instead of physically copying the files. This speeds up the backup and restore operations.

See "Using the Command Line Interface" on page 422 for details.

Caution: Whether the backup files are stored on the RCA Core server or the local hard disk of a managed device, they are never automatically deleted. If backup data for a particular device is no longer needed, that backup data can be deleted manually by the RCA administrator

Using the RCA Personality Backup and Restore Utility

The RCA Personality Backup and Restore Utility is a user interface that simplifies the usage of USMT. The Utility is deployed to managed devices when the RCA agent is installed.

Caution: Before you begin, make sure you have enough disk space available on the RCA Core server and on both the source and destination computers (see "Disk Space" on page 414.)

Starting the Personality Backup and Restore Utility

On the managed client device, use the Start menu, and go to:

All Programs > **Radia Client Automation Personality Backup and Restore** > **Client Automation Personality Backup and Restore Utility**

The following sections explain how to use the Utility:

- "Personality Backup" below
- "Personality Restore" on next page

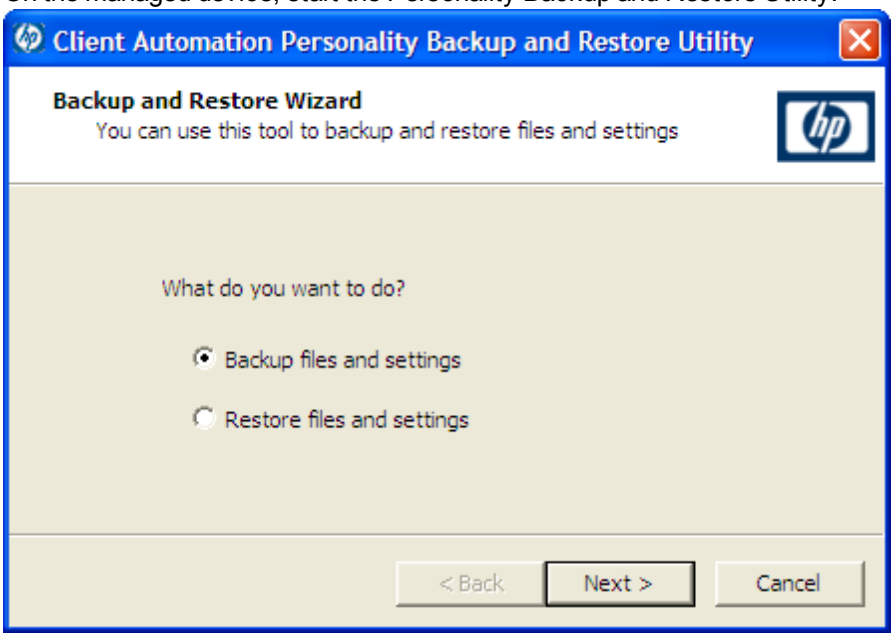
Personality Backup

You must run the Personality Backup and Restore Utility from a user account with administrator privileges.

Caution: To help ensure a successful backup, close as many open files and running applications as possible before you run the backup. Do not launch new applications or open files while the backup is running, as this can cause the backup to fail.

Backing up files and settings

1. On the managed device, start the Personality Backup and Restore Utility.



2. Select **Backup files and settings**, and click **Next**. The Backup dialog box opens.
3. Enter the computer name of the device that you want to back up.
4. Enter a password that is at least 7 but no more than 15 characters long, and click **Next**. The summary dialog box opens.
5. Review the summary information. Make a note of the computer name and password that you use, as you will need this information to restore your files and settings.
6. Click **Finish** to begin the backup process. Depending on the amount of data to be backed up, this process can take from a few minutes to several hours to complete. Wait for the Personality Backup and Restore Utility to indicate that the backup has completed before you close the application.

Personality Restore

You must run the Personality Backup and Restore Utility from a user account with administrator privileges.

Caution: To help ensure a successful restore, close as many open files and running applications as is possible before you run the restore. Do not launch new applications or open files while the restore is running, as this can cause the restore to fail.

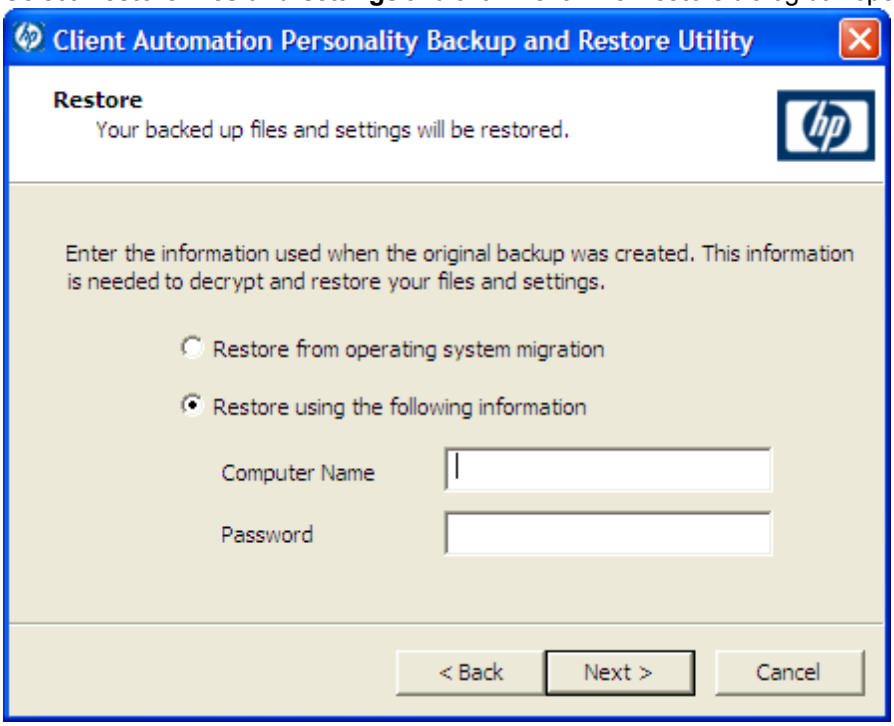
Before you begin the restore procedure, you must install (on the destination computer) all applications that have settings to be migrated. Note that for all applications other than Microsoft Office (where a newer version is allowed), the same application version must be installed on the destination computer as was installed on the source computer.

Note: You should do a restore to a computer on the same Windows domain that was used for the backup. You should also do a restore to the same locale (for example, US English) that was used for the backup.

Restoring files and settings

On the destination computer, start the Personality Backup and Restore Utility.

1. Click **Start** > **All Programs** > **Radia Client Automation Personality Backup and Restore** > **Client Automation Personality Backup and Restore Utility**
2. Select **Restore files and settings** and click **Next**. The Restore dialog box opens.



3. Perform one of the following actions:
   - To restore files and settings that were backed up using the Personality Backup and Restore Utility, select **Restore using the following information** and then type the `Computer Name` and `Password` that were used during the backup.
   - To restore files and settings that were stored during the last operating system deployment for which migration was enabled, select **Restore from operating system migration**.
4. Click **Next**. The Summary dialog box opens.
5. Click **Finish** to begin the restore process. Depending on the amount of data to be restored, this process can take from a few minutes to several hours to complete. Wait for the Personality Backup and Restore Utility to indicate that the restore has completed before you close the application.

6. Since some operating system settings, such as fonts, wallpaper, and screen saver settings, are not applied until after a reboot on the destination computer, you should now perform a reboot to ensure that all these settings are successfully applied.

Using the Command Line Interface

You can use the RCA Personality Backup and Restore command line interface to backup and restore files and settings for a managed device.

The syntax is as follows:

<*InstallDir*>`\Agent\pbr.exe /B|/R [/localstore] [/hardlink]`

Command Line Options for pbr.exe

Option	Description
`/B`	Perform a backup.
`/R`	Perform a restore.
`/localstore`	Store the backup files on (or restore them from) the local hard drive of the managed device instead of the RCA Core server.
`/hardlink`	For USMT 4.0 (included in the Windows 7 AIK), do not physically copy the backup files to the `OSMGR.PRESERVE` directory. Instead, create hard links to the files. This significantly saves backup space, because the backed up files are not duplicated. It also speeds up the backup and restore operations. If `/hardlink` is specified, `/localstore` is implied. When the `/hardlink` option is used, the target (restore) OS must be Windows Vista or Windows 7. The source (backup) OS, however, can be Windows XP SP2 or later. For USMT 3.0.1, this option is ignored. In this case, `/hardlink` is treated like `/localstore`.
`/xml`	Select xml files from RCA Core Server using wildcards. This option can be used when you perform a backup.
`/--`	Use this option to pass additional parameters for USMT utilities. The additional parameters are appended to the command line as set up by Personality Backup and Restore.

Example 1: Backup your files and settings on the RCA Core server

<*InstallDir*>`\Agent\pbr.exe /B`

Example 2: Restore from the RCA Core server

<*InstallDir*>`\Agent\pbr.exe /R`

Example 3: Backup your files and settings locally

<*InstallDir*>`\Agent\pbr.exe /B /localstore`

Example 4: Restore after a local backup

<*InstallDir*>`\Agent\pbr.exe /R /localstore`

Example 5: Perform a local backup using hard links

<InstallDir>\Agent\pbr.exe /B /hardlink

This example is valid for the following operating systems: Windows XP SP2, Windows XP SP3, Windows Vista, and Windows 7.

Example 6: Perform a local restore using hard links

<InstallDir>\Agent\pbr.exe /R /hardlink

This example is valid for the following operating systems: Windows Vista and Windows 7.

Example 7: Select xml files from RCA Core Server using wildcards

<InstallDir>\Agent\pbr.exe /B /xml myconfig*.xml

Example 8: Set log level for the USMT utilities ScanState and LoadState

<InstallDir>\Agent\pbr.exe /R /-- /v:4

Using the Personality Backup and Restore Services

There are two built-in services that RCA provides to help you automate the process of backing up and restoring user files and settings:

- RCA Personality Backup (RCA_PBR)
- RCA Personality Restore (RCA_RESTORE)

Both services invoke the `pbr.exe` application. These services are particularly helpful in the context of operating system deployment.

Caution: You can only use the HPCA Personality Restore service to restore user data if the HPCA Personality Backup service (or `pbr.exe /B`) was used to perform the backup. If the Utility was used to perform the backup, the Utility must also be used to perform the restore.

Migrating user data as part of an OS deployment in RCA Enterprise

1. Make sure that the following items are installed on all managed devices that will be part of this OS deployment:
   - The RCA agent
   - USMT
2. Make sure that the OS image that you will deploy includes USMT installed in the default location and configured properly for your environment.
   An alternative is to install and configure USMT on your managed devices immediately after the OS deployment (see "About USMT" on page 415).

   Caution: If RCA does not find USMT installed in the default location, neither the backup nor the restore will work.

3. Using the HPCA Policy Wizard, entitle the managed devices to the HPCA Personality Backup (HPCA_PBR) service.
4. Deploy the OS. The HPCA Personality Backup service will run on each managed device before the installation of the new OS. The backup files are stored on the RCA Core server.
5. After the OS deployment is completed, entitle each managed device to the HPCA Personality Restore (HPCA_Restore) service.
6. Create a Notify job to deploy the HPCA Personality Restore service to each managed device. The service will run once on each device to restore the user data. The service first checks the `C:/OSMGR.PRESERVE` folder to see if a local backup was performed. If it does not find local backup files, it restores the user data from the RCA Core server.

An Alternate Method for Capturing and Restoring Data during OS Deployment

HP also provides a ROM Client method (`romclimth.tkd`) that you can use to capture and restore data during operating system deployment. This method is stored in <*InstallDir*>`\Agent`, and it has two exit points.

The exit points call two optional scripts:

- `Novapdc.cmd` (data capture)
- `Novapdr.cmd` (data restore)

These scripts must also be stored in <*InstallDir*>`\Agent`.

You can use these scripts to customize data capture, recovery, and restoration for any product that you would like to use.

How romclimth.tkd Works

Capturing, recovering and migrating data using `romclimth.tkd` relies on the OS Manager User Agent. This is because data can only be captured when the operating system is running. The process works like this:

1. The Application Manager senses the change to a target device's desired state and triggers the data capture if `Novapdc.cmd` is available in <*InstallDir*>`\Agent`.
2. The target device reboots, and the new operating system is installed.
3. If `Novapdr.cmd` is available, the ROM Client method begins the restore process after the operating system has been installed on the target device.

Return Codes for HP Exit Points

The following return codes are returned from the HP exit points`Novapdc.cmd` and `Novapdr.cmd`. The values may vary depending on the software that you are using with these exit points. If the return value of the method is not equivalent to the following, use the standard batch error level conditional processing and the exit command to make them correspond to the following:

HP Exit Point Return Codes

Code	Description
0	Successful
1	An error occurred and will be logged, but processing will continue. The log is located in: *<InstallDir>*`\Agent\Logs\romclimth.log`.
2	• For `Novapdc.cmd` (capture): A fatal error has occurred and will be logged here: *<InstallDir>*`\Agent\Log\romclimth.log`. Processing of the service has ended. • For `Novapdr.cmd` (restore): An error has occurred and will be logged here: *<InstallDir>*`\Agent\Log\romclimth.log`. The service is flagged, but at the next RCA OS connect, the Application Manager will attempt to install the service again.

Chapter 16

Monitoring Radia Client Automation

Radia Client Automation (RCA) is deployed in a distributed and tiered environment. Monitoring this infrastructure ensures the availability of the associated services and components. Though the monitoring mechanism is optional, it recommends implementing this mechanism in your environment. The Radia Client Automation performance and availability depends on several factors, wherein the following three critical aspects must be monitored:

- RCA server availability
- RCA service availability
- RCA services responsiveness

RCA is capable of monitoring software deployments, but does not function as a monitoring tool. A monitoring solution is required to ensure that the infrastructure meets the service level requirements. The RCA log files and relational database tables provide information that monitoring tools can use to verify the infrastructure operations. You must ensure that the monitoring solution that you use in your environment is capable of performing the following tasks:

- Query Radia Client Automation components for availability status and response time
- Report the status of the server components, key application processes, log files, and display the component status as per the thresholds that are defined for that component
- Raise alerts when the set thresholds are not met

A solution with proactive and periodic test should be deployed that ensures these critical aspects are functioning.

RCA Infrastructure Components

Monitoring tools essentially monitor Windows system information, such as disk space usage, CPU utilization, and Windows service status. These tools can also monitor and extract log file contents to determine the success or failure of the task that the software performs. The RCA infrastructure monitoring relies on such inherent capabilities of the monitoring tools.

The RCA infrastructure monitoring solution is designed to ensure that the critical monitoring information is available to third-party external monitoring tools. In the Core-Satellite model, the individual infrastructure components are integrated into two major entities, a Core server and a Satellite server. For both these servers, most of the infrastructure components run as Windows Services. The key operational processes including DCS synchronization and Proxy server Preload are monitored by analyzing the corresponding log file content.

The following table lists the RCA components and the parameters that you should monitor if you plan to integrate a monitoring solution in your RCA environment.

RCA Infrastructure Components and Parameters to be Monitored

RCA Component				Availability	
Monitoring Type	Component Name	Severity	Monitoring Parameter	Core	Satellite
Server Monitoring	RCA Core/Satellite	Critical	Ping the Core/Satellite server at *<IP address/fully qualified device name>*	✓	✓
Windows Service Monitoring	RCA Configuration Server	Critical	Service Name: `ZTOPTASK` EXE: `ZTOPTASK.exe`	✓	✓
	RCA Apache Server	Critical	Service Name: `HPCA-Apache` EXE: `httpd.exe`	✓	✓
	RCA Tomcat Server	Major	EXE: `tomcat.exe`	✓	×
	RCA Boot Server (PXE)	Major	Service Name: `HPCA-PXE` EXE: `cygrunsrv.exe`	✓ Disabled by default	✓ Disabled by default
	RCA Boot Server (TFTP)	Major	Service Name: `HPCA-TFTP` EXE: `inetd.exe`	✓ Disabled by default	✓ Disabled by default
	RCA DB Server	Major	Service Name: `HPCA-DB` EXE: `mysqld-nt.exe`	✓	×
	RCA Directory Server	Major	Service Name: `HPCA-DS` EXE: `slapd.exe`	✓	×
	RCA Distributed Configuration Server	Major	Service Name: `HPCA-DCS` EXE: `nvdkit-hpca-dcs.exe`	✓ Disabled by default	✓
Windows Service	RCA Knowledge	Major	Service Name: `HPCA-KBM` EXE: `hpkbmanager.exe`	✓	×

RCA Component				Availability	
Monitoring Type	**Component Name**	**Severity**	**Monitoring Parameter**	**Core**	**Satellite**
Monitoring	Base Server			Disabled by default	
	RCA Management Portal Server	Major	Service Name: `HPCA-RMP` EXE: `nvdkit-hpca-rmp.exe`	✓	×
	RCA Messaging Server	Major	Service Name: `HPCA-MS` EXE: `nvdkit-hpca-ms.exe`	✓	✓
	RCA Multicast Server	Major	Service Name: `HPCA-MCAST` EXE: `nvdkit-hpca-mcast.exe`	✓ Disabled by default	✓ Disabled by default
	RCA OS Manager	Major	Service Name: `HPCA-OSM` EXE: `nvdkit-hpca-osm.exe`	✓ Disabled by default	✓ Disabled by default
	RCA Patch Acquisition Server	Major	Service Name: `HPCA-PATCH` EXE: `nvdkit-hpca-patch.exe`	✓ Disabled by default	✓
	RCA Policy Server	Major	Service Name: `HPCA-PM` EXE: `nvdkit-hpca-pm.exe`	✓	✓ Disabled by default
Service Response Monitoring	RCA Apache Server Response	Major	URL: http://< server>:<server_port>/server-status	✓	✓

RCA Component				Availability	
Monitoring Type	Component Name	Severity	Monitoring Parameter	Core	Satellite
	RCA Apache Tomcat Server Response	Major	URL: http://<core>:<core port> /console/flex/console.jsp	✓	×
	RCA Configuration Server Response	Critical	Run a batch script to internally execute the `nvdkit.exe` tpping. For example, `nvdkit.exe tpping -host`	✓	✓ Disabled by default
	RCA Management Portal Server Response	Major	URL: http://<core host>:<core port>/proc/Radia/?WebService.Name=AuthenticateUser&Response.Format=Text&getauthds=true	✓	×
	RCA Messaging Server Response	Major	URL: http://<host>:<port>/proc/msg	✓	✓
	RCA Policy Server Response	Major	URL: http://<server host>:<server port>/policy/ldap?dn=ldap%3a%2f%2f%2fcn%3ddevice%2ccn%3dhp%2ccn%3dradia	✓	✓ Disabled by default

RCA has the ability to integrate with existing HP monitoring products to provide flexible monitoring solution implementations.

RCA also provides SiteScope solution template that includes a pre-configured set of monitors that you can deploy to monitor multiple aspects of RCA components in the infrastructure. You can download the latest SiteScope HPCA template and documentation from HP Live Network at **https://hpln.hp.com//page/monitoring-hp-client-automation**.

Appendix A

SSL Settings on the RCA Core and Satellite Servers

In order to fully understand how to use the SSL settings that are available on the RCA Console, it is important to understand the various “parts” of SSL and their functions. This appendix offers a brief overview of SSL, including how it relates to an RCA environment. See the following sections:

- "SSL Parts" below
- "SSL in an RCA Environment" below
- "The SSL Certificate Fields on the Consoles" on next page

For additional information, see the *Radia Client Automation Enterprise SSL Implementation Guide*.

SSL Parts

SSL includes the following parts:

- Certificates
- Certificate Authorities (CA)
- Generating Certificates
- Private Key Files
- Public Key Files

See Chapter 1 of the *Radia Client Automation Enterprise SSL Implementation Guide* for a comprehensive overview of each.

In order to enable SSL, you will need the following:

- Public certificate and private key for each server that will have SSL enabled
- CA Certificates file if the servers' public certificates are signed by a CA not already included in the provided `ca-bundle.crt` file

SSL in an RCA Environment

SSL uses **digital certificates** to establish proof of identity, and to establish shared **encryption ciphers** to provide secure communications. How you use SSL is dependent on how your infrastructure components plan to communicate. RCA supports up to five levels of CA certificates. This means up to five CAs can be used in RCA environment. This section provides information on the two primary scenarios in which SSL should be enabled, and the role it plays in each.

Note: See Chapter 1 of the *Radia Client Automation Enterprise SSL Implementation Guide* for

information on SSL Certificate Authorities, SSL certificates, and generating SSL certificates.

Supporting SSL Communications to Remote Services

Assume that it is not necessary to secure the communications between the Core and Satellite servers; an SSL connection between them is not necessary. However, secure communications (LDAPS) are still required for the Core or Satellite server's communications with external servers (such as those hosting vendors' web sites), other RCA servers, and Active Directory.

In order to trust that these other servers are "who" they claim to be, the Core or Satellite must obtain each server's **public certificate**, or the signature of the issuing **Certificate Authority** (CA). The Core or Satellite must also have a **CA Certificates file**, which it has obtained from a Certificate Authority, and which must be available to other servers so that they can decrypt messages from the Core or Satellite. (The Core and Satellite installations include a set of default trusted authorities, `ca-bundle.crt`, which is suitable for most environments.)

Providing Secure Communications Services to Consumers

Assume an environment in which the communications between the Core and Satellite servers needs to be secure. In this case, the Core will assume the role of server and, as such, will need a public certificate that it can share with the Satellites. The Core server's public certificate contains its public key, server name, and a signature from a Certificate Authority (attesting to the identity of the server).

- A public certificate (also known as a **server certificate**) can be given to anyone whom you want to trust you.

Further, each Satellite server, in the role of "client," will need its own set of certificates so that it can encrypt and decrypt messages between it and the Core. A certificate represents the Satellite, identifying it to the Core.

Each Core and Satellite also needs its own private key to decrypt messages.

- A **private certificate** (also known as a **private key**) should be kept private; it should never be shared.

The SSL Certificate Fields on the Consoles

The Infrastructure Management area of the Configuration tab of the RCA Console contains two SSL Certificate areas: "SSL Server" on next page and "SSL Client" on next page. The differences between these areas and the necessity of each are explained in this section. To complete the SSL set up for the RCA, review the information in this appendix, then see "Infrastructure Management" on page 273.

Note: See Chapter 1 of the *Radia Client Automation Enterprise SSL Implementation Guide* for

information on SSL certificates, SSL Certificate Authorities, and generating SSL certificates.

SSL Server

This area of the panel is used to enable SSL, and upload and save the private key file (`server.key`) and server certificate file (`server.crt`) for the RCA servers. These files were either self-generated (within your organization) or obtained from a Certificate Authority. Check with your system administrator for access to these files.

- The private key file is needed to decrypt messages that were secured with the corresponding public key.
- The server certificate file is needed so that this host can identify itself to SSL-enabled servers.

After the files have been uploaded (located and **Save** clicked) these files are saved to:

<InstallDir>`\ApacheServer\conf\ssl.`

By default, these files will be saved with the names shown above, but the file names can be customized.

SSL Client

This area of the panel is used to upload and save the CA Certificates file (`ca-bundle.crt`) for the RCA servers. This file contains a default set of trusted authorities that should be sufficient for most environments, and is needed only when an RCA server communicates with another server over either LDAPS or HTTPS.

Note: It is possible to use an existing CA Certificates file that was obtained for your organization from a Certificate Authority. Check with your system administrator because you will need access to this file.

The CA Certificates file contains the signing certificates from trusted Certificate Authorities and is needed so that it can verify any incoming clients as “trusted.”

After the file has been uploaded (located and **Save** clicked) it is saved to:

<InstallDir>`\ApacheServer\conf\ssl.crt.`

By default, the file will be saved with the name shown above, but the file name can be customized.

Appendix B

Advanced Topics for Live Network

This section addresses more advanced topics about HP Live Network. They include the following:

- "Use the Command Line Utility" below
- "Run the HP Live Network Connector Manually" on page 439
- "Move HP Live Network Content from a Test Environment to a Production Environment" on page 441

Use the Command Line Utility

As an alternative to using the HP Live Network page (under Infrastructure Management on the Operations tab) to schedule or trigger a HP Live Network content update, you can use the `content-update.cmd` command-line utility located in the following directory:

Core and Satellite: *<InstallDir>*`\VulnerabilityServer\bin`

Note that this directory is not automatically placed in your PATH when RCA is installed.

This utility has the following syntax:

`content-update.cmd [-settingName` *<settingValue>*`]...`

This command has both "Required Settings" below and "Optional Settings" on next page. Note that you must always specify a value for the `content_source` setting.

Any values that you specify on the command line override the stored configuration settings specified elsewhere (see "Stored Settings" on page 438). If you do not specify a value for a particular setting, the stored configuration setting is used.

Note: The `content-update` command writes status and error messages to the `vms-commandline.log` file.

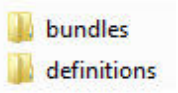
See "Examples" on page 438 for typical uses of the `content-update.cmd` command.

Required Settings

The following table lists the required settings for the `content-update.cmd` command.

Note: Any values that you specify on the command line override the stored configuration settings that were specified elsewhere (see "Stored Settings" on page 438). If you do not specify a value for a particular setting, the stored configuration setting is used.

Required Settings for content-update.cmd

Setting	Description
`content_source`	This setting is required. It specifies the source for the updated content. This must be one of the following: LIVENETWORK – Acquire the content from the HP Live Network subscription site by using the HP Live Network Connector. The HP Live Network settings and the path to the downloaded Connector must be properly configured for this option to work. See "Live Network" on page 305. FILESYSTEM – Acquire the content from a location in the file system. The content must have previously been downloaded from HP Live Network to this file system location. The `content_path` setting must also be specified, either on the command line or on the HP Live Network page under Infrastructure Management on the Operations tab. See "Live Network" on page 305. CSDB_MASTER – Acquire the content from master content previously published to the configuration server database (CSDB). This data will be used to load the Reporting database. Service deployment content will NOT be republished. This is intended for use when a test configuration server content deck has been imported into a production configuration server.
`content_path`	The fully qualified path to the file system location containing the content that you manually obtained from HP Live Network. This setting is only required if you specified FILESYSTEM as the **content_source**. This path can specify either a directory or a ZIP archive file. The directory structure (or ZIP file structure) must exactly match the structure of directories and files created when an automatic HP Live Network update is performed:  You must also replicate the sub-directories under these folders to match the automatic update structure. In some cases, HP Live Network updates only a subset of the content. In this case, some of these directories may not be delivered during a HP Live Network update. In any case, when you update from the File System, your directory structure must match that delivered by HP Live Network.

Optional Settings

The following settings for the `content-update.cmd` command are optional.

Note: Any values that you specify on the command line override the stored configuration settings that were specified elsewhere (see "Stored Settings" on page 438). If you do not specify a value for a particular setting, the stored configuration setting is used.

Optional Settings for content-update.cmd

Setting	Description
`csdb_host`	Configuration Server network addressable system name. This can be a fully qualified host name, localhost, or an IP address.
`livenetwork_connector_`	The fully qualified path to the HP Live Network Connector on the local file system. By default, this is:

Setting	Description
`executable`	Core and Satellite: *<InstallDir>*`\LiveNetwork` The HP Live Network Connector is a tool used by RCA to create a secure connection to the HP Live Network content distribution server and download the updated content.
`livenetwork_ connector_ maxruntimeminutes`	Time (in minutes) that the HP Live Network Connector will be allowed to run before forcing a failure. Minimum value should be 60.
`livenetwork_ contenturl`	URL for the HP Live Network content distribution site. This is the location that the HP Live Network Connector will use to download new content.
`livenetwork_ username`	User name for the HP Live Network subscription.
`livenetwork_ password`	Password for the HP Live Network subscription.
`livenetwork_ proxy_http_server`	HTTP proxy server used to connect to the HP Live Network download site. This option must have the following form: `<http|https>://<`*host*`>:<`*port*`>`
`livenetwork_ proxy_http_ username`	User name for the HTTP proxy server, if any, used to connect to the HP Live Network download site.
`livenetwork_ proxy_http_ password`	Password for the HTTP proxy server, if any, used to connect to the HP Live Network download site.
`reporting_db_ databasename`	Name of the database instance that you created before installing RCA, which is discussed in the "Create the RCA Database" section of the *Radia Client Automation Enterprise Installation and Upgrade Guide*.
`reporting_db_ drivername`	Name of the database driver to use (either `oracle` or `sqlserver`). This must map to a supported driver.
`reporting_db_ server`	Network addressable server name where the Reporting database is located.
`reporting_db_port`	Reporting database port number. This must be empty if the port is dynamic. If the port is static, it must be a value between 1 and 65536.
`reporting_db_ username`	User name for the Reporting database.
`reporting_db_ password`	Password for the Reporting database.

Stored Settings

If you do not specify a value for one of the `content-update` settings, the values specified on the following Live Network configuration pages are used by default:

Stored Settings for content-update.cmd

Option	Where Specified

`csdb_host`
`csdb_port`
`csdb_username`
`csdb_password`
	HPCA First-Time Setup wizard

`livenetwork_connector_executable`
`livenetwork_contenturl`
`livenetwork_username`
`livenetwork_password`
`livenetwork_proxy_http_server`
`livenetwork_proxy_http_username`
`livenetwork_proxy_http_password`
	Live Network page and Proxy Settings page

`reporting_db_databasename`
`reporting_db_drivername`
`reporting_db_server`
`reporting_db_port`
`reporting_db_username`
`reporting_db_password`
	Automatically configured when RCA is installed

Examples

Example 1 – Perform a content update using the previously configured HP Live Network settings

```
content-update.cmd -content_source LIVENETWORK
```

Example 2 – Perform a content update from a local directory

```
content-update.cmd -content_source FILESYSTEM -content_path
c:\mycontent
```

Example 3 – Perform a content update from a local ZIP file

```
content-update.cmd -content_source FILESYSTEM -content_path
c:\mycontent\content.zip
```

To view full usage information for `content-update.cmd`, type the following command from the <*InstallDir*>`\bin` directory:

```
content-update.cmd -?
```

Run the HP Live Network Connector Manually

In some situations, the RCA Core server may not have Internet access. In this case, you can still update your HP Live Network content using a system that does have Internet access and then manually transfer the content to the RCA Core server. This process includes four steps:

1. On the system with Internet access, manually download the HP Live Network Connector from the HP Live Network subscription web site. See your Persistent Software sales representative for instructions.
2. Execute the HP Live Network Connector on the system with Internet access.
3. Transport the content to the RCA Core server.
4. Update the HP Live Network content from the file system on the RCA Core server. See "Update HP Live Network Content" on page 55.

When you execute the HP Live Network Connector, it creates the folder structure described under `content_path` in "Required Settings" on page 435 and then stores its output files within this structure.

Caution: Before you run the HP Live Network Connector from the command line, make sure that the directory where you will “import” the HP Live Network content is empty before you execute the Connector.

This directory is specified by the following parameter:

`--setting=hpca.import_directory=`*<output-dir>*

In this case, *<output-dir>* is the location where the HP Live Network content is placed.

If the “import” directory is not empty, there is a possibility that you will move old content into HPCA when you subsequently use the `FILESYSTEM` option to update your HP Live Network content. This could have negative repercussions, such as incorrectly deploying an old scanner if a new one is released that has a new name.

This warning applies only when you run the HP Live Network Connector from the command line. It does not affect HP Live Network updates that you perform through the RCA Console.

The Live Network Connector command line has a long list of options passed to it to drive the actual acquisition. The command is dynamically assembled based on the settings selected in the HPCA Console. When new content is released over live network, the settings passed to the Live Network Connector may have changed also. If you plan to execute the Live Network Connector manually, it is very important to use the most current command line options.

Constructing the HP Live Network command line with the most current options

1. Go to **Infrastructure Management** > **Live Network** on the **Configuration** tab and set the options up correctly as you would if you were going to execute the Live Network Connector through the RCA Console.
2. Save the options.

3. Go to **Infrastructure Management** > **Live Network** on the **Operations** tab and perform an update now choosing Live Network as the source. Verify any other settings that apply to your environment.
4. Open the log file at `<install-dir>\VulnerabilityServer\logs\connector-exec-cmd.log`
5. Copy the most recent command executed.
6. Take the command to the system where you want to execute the Live Network Connector.
7. Modify the command to have the appropriate path, appropriate user name, appropriate password, and appropriate import directory. Note that passwords in the command will be displayed as asterisks **** and will not work if directly invoked.

It should be noted that if you execute this command using the same Live Network installation on the same system that the RCA Console is running on that you may cause RCA and HP Live Network to become out of sync. If you do this, see the Live Network Connector user guides for clearing the Live Network Connector cache.

Downloading the HP Live Network content

Run the command line constructed by following the procedure in "Constructing the HP Live Network command line with the most current options" on previous page. The following is an example of a command line to run on the system with Internet access:

```
<install-dir>\LiveNetwork\lnc\bin\live-network-connector.bat
--url=https://bsaen-dist.hp.com
--username=<name>
--password=<password>
--product=hpca --setting=hpca.installed_version=7.90.0
--setting=hpca.import_directory=<output-dir>
--stream=content.hpca_settings_mgmt
--stream=security.hpca_nvd
--stream=security.hpca_sectools_scanner
--stream=security.hpca_config
--stream=security.hpca_oval
--stream=security.hpca_scap_scanner
--stream=content.hpca_config
--stream=security.hpca_sectools_services
--stream=security.hpca_scap_cis
--stream=security.hpca_scap_fdcc
```

All items in <*brackets*> here are placeholders for values that you must supply.

In this case, <*install-dir*> is the file system location where you installed the HP Live Network Connector, and <*output-dir*> is the location where the Connector will create the folder structure that contains its output files. For example, if <*output-dir*> is `c:\temp`, the folder hierarchy is created under `c:\temp`.

The proxy server settings are only necessary if a proxy server exists between the system hosting the RCA Console and the HP Live Network subscription site.

Next Steps

After you run the HP Live Network Connector on the system with Internet access, you must manually copy the folder structure to the RCA core server hosting the RCA Console. You can place the folder structure either directly in the file system or in a ZIP archive.

At this point, you must tell RCA where to find this content. There are two ways to do this:

- On the HP Live Network page under Infrastructure Management on the Operations tab, select **From the File System**, and specify the location of the folder structure (or ZIP file).
  Or
- From the command line, run the `content-update` command, and specify the `FILESYSTEM` content source. Specify the location of the folder structure (or ZIP file) by using the `content_path` setting.

Move HP Live Network Content from a Test Environment to a Production Environment

You may find it useful to test your HP Live Network content in a small controlled environment before performing a large scale rollout. To do this, you will first create a test RCA environment with its own "test" Configuration Server Database (CSDB) and "test" Reporting database. After completing your testing, you will export the "test" relevant Domain and then import that CSDB content into your production RCA environment.

Note: The files used to export and import CSDB content are known as a "deck."

Before following these procedures, be sure to review "How HP Live Network Content is Updated" on page 50.

Testing your HP Live Network content in a controlled test environment

1. In the test environment, perform an HP Live Network content update—either automatically from the HP Live Network subscription site, or manually from the file system.
2. Test the updates by running scans and reviewing the pertinent reports and dashboard panes.

Moving your HP Live Network content from a controlled test environment to a production environment

Caution: In the `raddbutil` commands shown here, there are no spaces after the commas. If you cut and paste these commands from this guide or the online help, be sure to remove any spaces introduced by the paste operation.

1. Connect to the test CSDB and use the `raddbutil` tool to export the relevant deck:
   a. Go to the Configuration Server `bin` directory on the system where you want to export the data (the test environment).
   b. If the `admin` user has a password, use the following command:
   `raddbutil EXPORT DATA=TRUE,WALK=TRUE,OUTPUT=`*<tempDir>*`,USERID=admin,PASSWORD=`*<password>* `PRIMARY.`*<DOMAIN>*

If the `admin` user does not have a password, use the following command:

```
raddbutil EXPORT DATA=TRUE,WALK=TRUE,OUTPUT=
<tempDir>,USERID=admin PRIMARY.<DOMAIN>
```

In both cases, *<tempDir>* is the directory where the exported files will be placed on the test CSDB system.

For more information, see *Configuration Server Database Utility (RadDBUtil)* in the *Radia Client Automation Enterprise Configuration Server Reference Guide*.

2. Transport the relevant deck files to the production CSDB system using the file transfer mechanism of your choice.
3. On the production CSDB system, use the `raddbutil` tool to import the relevant deck:
   a. Go to the Configuration Server directory on the system where you want to import the data (the production environment).
   b. If the `admin` user has a password, use the following command:
   ```
   raddbutil IMPORT
   INPUT=<tempDir>,COMMIT=TRUE,ACCEPT=A+D+U,USERID=admin,PASSWORD=
   <password>
   ```
   If the `admin` user does not have a password, use the following command:
   ```
   raddbutil IMPORT
   INPUT=<tempDir>,COMMIT=TRUE,ACCEPT=A+D+U,USERID=admin
   ```
   In this case, *<tempDir>* is the directory on the production CSDB system where the files were placed in the step "Transport the content to the RCA Core server." on page 439.
4. In the production environment, load the production Reporting database using the “master” content in the relevant deck that you just imported.
   There are two ways to do this:
   - **Method 1:** Use the RCA Console
     i. Click Infrastructure Management under the **Operations** tab.
     ii. In the left navigation menu, select **Live Network**.
     iii. Click the **Update Now** tab.
     iv. Select the **From the Configuration Server Database** update option.
     v. Click the **Update Now** button.
     vi. See "Live Network" on page 305 for more information about the Update Now tab.
   - **Method 2:** Use the `content-update` command-line utility **content-update.cmd -content_source CSDB_MASTER**

     See "Use the Command Line Utility" on page 435 for more information about the `content-update` command.

   In either case, using the CSDB_MASTER content source forces the update tool to only update the Reporting database content and bypass performing any updates to the packages linked to the relevant content. This ensures that the service content you deployed in your test environment will exactly match the content that you will be deploying in your production environment.

Appendix C

Enhancing Reporting Performance

RCA (Usage Manager) provides several scripts and materialized views that can be applied to the Microsoft SQL Server and Oracle databases to enhance the reporting performance.

The scripts and views are available at:

- `Media\Usage\Optional Features\SQL Server` for Microsoft SQL Server database
- `Media\Usage\Optional Features\Oracle` for Oracle database

Using Views

There are two types of views, Standard Materialized Views and Filter Materialized Views. Both views enhance reporting performance. Either one can be optionally applied to a database. See the comments in the scripts for additional information about the functions of each view.

Note: The script names may abbreviate "Materialized" to "Mat", as in: `StepX_Define Filter Mat Tables` and `Indexes.sql`

Standard Materialized Views (SMV) - Converts all the views accessed by reports into tables. This view includes the index to enhance the query execution time. A feature where all the views (which is what the reports access) are converted into tables, and indexes are added to enhance the query speed.

Filtered Materialized Views (FMV) - Converts all the views accessed by reports into tables and requires filters to be applied before the views are converted into tables. The filters are stored in a separate table. For example, if a user selects `notepad.exe` as a filter, the FMV table is populated with the notepad details for all the devices. It is similar to SMV, but differs in that it requires filters to be applied at the time the views are converted into tables. The filters are stored in a separate table. As an example, if a filter for Notepad.exe is selected, the FMV table will be populated with only notepad details for all the devices.

Applying the scripts for SMV or FMV

1. Stop the service for the **HPCA Knowledge Base Server**. The service may be stopped and started through the `Administrative Tools\Services` options of Windows Control Panel.
2. Use normal procedures to execute the database scripts, in the given order, provided in the following locations:
   - For SQL Server:
     `\SQL Server\Optional Features\Filter Materialized Views`

     Or

     `\SQL Server\Optional Features\Standard Materialized Views`

- For Oracle:
  `\Oracle\Optional Features\Filtered Materialized Views`

  Or

  `\Oracle\Optional Features\Standard Materialized Views`

Each of the above locations also includes a corresponding script to remove the view from your database. For example, the script name for the Microsoft SQL Server and Filtered Materialized Views is:

`SQLServer - Remove All Filter Mat Tables and Indexes.sql`

Utility Scripts

You as a database administrator can use the following scripts to enhance the reporting view performance:

- Purge_Computer_Data.sql: Deletes all data associated with the computer name. The computer name should be provided at the appropriate place in the script. The default value is MYCOMPUTER.
- Purge_User_Data.sql: Deletes all data associated with the computer name and the user name. The computer name and the user name should be provided at the appropriate place in the script. The default values are MYCOMPUTER and BOB.
- Delete All Windows OS Files from Database.sql: Deletes all Windows Operating System (OS) related files from the Usage Manager database.

Miscellaneous Scripts for Oracle

Miscellaneous scripts are additional scripts that can be applied along with the utility scripts to enhance the reporting view performance.

- Optional_Create_Public_Synonyms.sql: Creates public synonyms. The script may have to be edited for the Usage Manager's user names.
- Optional_Drop_Public_Synonyms.sql: Drops the public synonyms created by using the Optional_Create_Public_Synonyms script.
- Step99a_DropAll.sql: Drops all the tables present in the Usage Manager database.

Appendix D

IPv6 Networking Support

Radia Client Automation (RCA) supports Internet Protocol version 6 (IPv6) for external communication among RCA components. The following topics are explained in this section.

Topics in this appendix include:

IP Networking Terms and Basics

This topic defines some terms and basic information related to IP version 4 and IP version 6.

An IP address was intended to be a unique number identifying a unique device or port of a device. The 32-bit address space of IPv4 addresses puts severe limits on the number of unique addresses available, and the supply is running out. The IPv6 128-bit address space was created to address this problem.

Terms

- **IPv4 Address:** An IPv4 address contains four sections separated by periods (or "dots"). Each section, called an octet, contains 8 bits expressed in decimal (0-255). When entering an IPv4 address, you can omit leading zeroes.
- **IPv6 Address:** An IPv6 address contains eight sections separated by colons. Each section contains 16 bits expressed in case-insensitive hexadecimals (0000-FFFF).
  Example: `2001:0db8:0000:0001:f8f3:a7bb:2bcb:6037`

  To make it easier to remember and type an IPv6 address, you can use one instance of a double colon (::) to indicate multiple contiguous sections of zeros. You can also omit leading zeroes. For example, you can simplify the address:
  `2001:0db8:0000:0001:f8f3:a7bb:2bcb:6037`
  to `2001:db8:0:1:f8f3:a7bb:2bcb:6037` or `2001:db8::1:f8f3:a7bb:2bcb:6037`.
- **IPv6 address types**:
  - **Global unicast address**: This is the IPv6 address that can be used for *external communication*. A sample global unicast address is:
    `2001:db8:0:1:f8f3:a7bb:2bcb:6037`.
  - **Link-local address**: This address can be used for *communication with neighbors on the same subnet (link), only*. Link-local addresses are not forwarded by routers. Their syntax includes "%n" at the end, for example: `fe80::20c:29ff:fed4:5ab%4`.

- **IPv4-mapped address**: This address can be used for tunneling an IPv4 address through an IPv6 network. For example: `fe80::5efe:192.168.6.154` tunnels the IPv4 address `192.168.6.154`.

IP Address Shortcuts: IPv4 versus IPv6

The Table below summarizes IP address shortcut conventions for IPv4 and IPv6.

IPv4 and IPv6 Reserved IP Address Values

Reserved Meaning	IPv4 Value	IPv6 Value
localhost	`127.0.0.1`	`::1`
Any address Any interface	`0.0.0.0`	`::`
Tunneling IPv4/IPv6	Not Applicable	`fe80::5efe:`<*IPv4addr*>where <*IPv4addr*> is the IPv4 address, as in: `fe80::5efe:192.168.1.2`

Bracketing IPv6 Addresses

You must enclose a literal IPv6 address in brackets "[" and "]" in URLs, URIs, or other syntax that allows the IP address to be followed by ":port". Examples include schemes for HTTP, HTTPS, LDAP and LDAPS entries. The brackets around the IPv6 address are required to distinguish the beginning and end of the IPv6 address (which includes colons) from the colon used to identify the port.

Example:

`http://[`*literal_IPv6_address*`]:port`

Omit the brackets when entering an IPv6 address through the Core or Satellite Console pages or a configuration file where the field does not allow for a port entry.

Examples:

- User Interface: **Upstream host:***literal_IPv6_address*
- Conf file: `HOST=`*literal_IPv6_address*
  `-host` *literal_IPv6_address*

Overview of IPv6 Support in RCA

RCA supports IPv6 for external communication on Core, Satellite, and Agent on Windows systems. The internal communication on these components takes place using IPv4. IPv6 is not supported on Agents on Linux and Macintosh systems. In RCA,

- The Core and Satellite servers have been enabled to perform RCA *server-to-server* communications using either IPv4 or IPv6.
- The Core and Satellite servers, as well as the RCA Configuration Server service, are automatically configured to listen on the available IPv4 and IPv6 stacks that are detected during

installation. If only IPv4 is detected, they are configured for IPv4. If IPv6 is also detected, they are configured to listen on both stacks.

- The Core and Satellite servers can perform RCA server-to-agent communications using either IPv4 or IPv6 and vice-versa.
- If the Core and Satellite servers are configured to listen on IPv4 only, the IPVER attribute in the Server Access Profile should be set to 4 for the RCA agent to use IPv4 to connect to the server. The IPVER attribute is used to for selecting the IP version on the client machine and not used for the server connection failover.
- If the IPVER attribute value is set to 64 in a dual-stack environment and RCA agent cannot connect to the RCA Satellite server over IPv6 for some unknown reason, the RCA agent connects to the upstream host over IPv6 instead of connecting to the same Satellite server over IPv4.

IPv6 Support Limitations

The following Client Automation components support IPv4 only and are not IPv6-capable:

- Client Automation Administrative tools
- Multicast Server and Multicast Agent
- Out of Band Management (OOBM) surfaces: IPv6 is intentionally excluded in this release across all OOBM surfaces, including:
  - Core engines to OOBM Web Services
  - OOBM to SCS (SCS is the Intel AMT Setup and Configuration Service)
  - OOBM to Agent
- HP Thin Client devices in your RCA environment
- RCA Registration and Loading Facility (RALF) component of RCA Agent
- Communication between Application Manager agent and Application Self-Service Manager agent
- radstgms internal communication to access the files from the DATAURL, during advanced MSI deployment using Local AIP.
- Pre-execution environment (PXE) deployment of OS is not supported on IPv6.
- OS Capture is not supported using IPv6.
- For OSM, policy resolution based on subnets is not supported on IPv6.

Support for IPv6 in a Core-Satellite Environment

RCA support for IPv6 focuses on enabling the IPv6 routing of traffic among its in Windows-based Core, Satellite, and Agent components.

The IP networking features in this release allow the Client Automation servers to use IPv6 or IPv4, as appropriate, to route the following traffic:

- Core and Satellite traffic to sync the Configuration Server metadata
- Core and Satellite traffic to sync the Cache data

- Core or Satellite Authentication and Policy traffic (HTTP and LDAP)
- Inter-Satellite and Core Messaging traffic
- Inter-Satellite and Core HTTP traffic
- Core or Satellite to Agent communication and vice-versa

IP Communications Support Table

The following table identifies the RCA communication pathways among the Core, Satellites, Agents and external directories. It identifies the communication pathways that support IPv4 only, and those that support IPv4 or IPv6 (IPv4/IPv6).

IP Communications Support Table

			Target (Server)		
		Agent	**Satellite**	**Core**	**AD/LDAP**
Source	**Agent**	N/A	IPv4/IPv6	IPv4/IPv6	N/A
Client	**Satellite**	IPv4/IPv6	IPv4/IPv6	IPv4/IPv6	IPv4/IPv6
	Core	IPv4/IPv6	IPv4/IPv6	IPv4/IPv6	IPv4/IPv6

The Core and Satellite servers listen on two points (an HTTP listening point and a Configuration Server listening point). Either of these communication points can be IPv4 or mixed, as needed.

How to Enable IPv6 Server Communications

If the Core and Satellite Setup programs detect an IPv6 stack on the host server, the Core and Satellite servers are automatically configured to listen on both IPv4 and IPv6 protocols.

Before you run the Core or Satellite installation, review the "Prerequisites for IPv6 Support" below.

Prerequisites for IPv6 Support

- The RCA Core and Satellite Servers must be installed on Windows XP, Windows 2003 Server or Windows 2008 Server Operating Systems that are IPv6-enabled and are running in IPv6-enabled networks. For more information on supported platforms, see the *Radia Client Automation Support Matrix* available at the following URL: http://support.persistentsys.com. For more details, contact your Persistent sales representative.
- RCA servers and agent must be run in a dual stack IPv4\IPv6 environment.
- Your DNS and DHCP must be configured for IPv6 support.
- In order to support IPv6 communications between an HPCA server and a customer-provided external **Active Directory Service** (**ADS**) being used for Policy and Authentication communications:
  - the ADS must be installed on Windows Server 2008
  - the ADS must be configured for IPv6
- The web browser is required to support IPv6.

Configuring RCA Windows Servers for IPv6 Support

This section identifies the IPv6-related configuration changes that are made to the RCA Core and Satellite Windows Servers and RCA agent components when they are installed on IPv6-enabled servers.

The configuration topics are discussed in this section:

Component: RCA Apache-based Core and Satellite Servers

The RCA Core and Satellite servers run under an Apache service which is IPv6-enabled by default. The Apache service does not require any configuration changes for IPv6. However, make sure your environment meets the previously stated prerequisites.

To verify that Apache is listening for IPv6 addresses:

1. Open a command prompt
2. Type `netstat -an`
3. On the resulting display, check that an entry for [::]:3466 exists. If present, this verifies that Apache is listening for v6 addresses.

Component: RCA Configuration Server

To enable the notify connect from RCA Core to RCA agent using IPv6, perform the following steps:

1. On RCA Core server, navigate to the `<InstallDir>\tomcat\webapps\ope\config` directory.
2. Open the `dtm.properties` file.
3. Set the value of the `ipvpreference` parameter to 6. The default value of the `ipvpreference` parameter is 4.
4. Save the `dtm.properties` file.

How IPv6 is Enabled for the Configuration Server Component

If the Core or Satellite is enabled for IPv6 when the Core and Satellite servers are installed, the Configuration Server is enabled automatically to listen on IPv4 and IPv6 stacks. This includes:

- Enabled session connectivity to accept connections on IPv6 as well as IPv4.
- Enabled session connectivity with the **Secure Sockets Layer** (**SSL**) for IPv4 as well as IPv6.

Verifying the Configuration Server is listening for IPv6 addresses in non-SSL mode

These modifications are made by the Core or Satellite setup program when IPv6 is enabled on the server. You can view and verify the Configuration Server configuration changes used to enable IPv6 using the steps below:

1. Use Microsoft Notepad to open `edmprof`, located in the `\bin` directory of where the RCA server was installed. Notepad supports UTF-8, which is the required encoding for the `edmprof` file.
2. Go to the `MGR_ATTACH_LIST` section and locate the `ATTACH_LIST_SLOTS` attribute. When IPv6 is detected, the Core Setup program explicitly adds the following `CMD_LINE` entry for IPv6 enablement. (The `edmprof` default for `ztcpmgr` to listen on IPv4 is also in effect.)
   ```
   CMD_LINE=(ztcpmgr, NAME=tcpmgr6,ADDR=::) RESTART=YES
   ```

   Note: This command line reflects an RCA Configuration Server using the default port of 3464. If a non-default port is being used, a PORT will also be specified after the ADDR attribute using the same syntax as shown in "Verifying the Configuration Server is listening for IPv6 addresses in SSL mode" below.
3. The Core setup program also increases the `ATTACH_LIST_SLOTS` value by 1 to accommodate the new `CMD_LINE` entry.

   Note: If the `edmprof` file has been changed manually, ensure it is save with UTF-8 encoding, and restart the service for the RCA Configuration Server (`ZTopTask.exe`).
4. To confirm these configuration changes are reflected in the RCA Configuration Server service (`ZTopTask.exe`), check the Configuration Server log files. You will see two TCP managers waiting to accept incoming requests. For examples, see "Log Messages" on next page.

Verifying the Configuration Server is listening for IPv6 addresses in SSL mode

These changes are done automatically by the Core and Satellite setup programs when IPv6 is enabled on the server.

1. Use Microsoft Notepad to view `edmprof`, located in the `\bin` folder of where the RCA Server was installed. Notepad supports UTF-8, which is the required encoding for the `edmprof` file.
2. The Core configuration program adds the following lines under the `MGR_ATTACH_LIST` section for SSL Manager IPv4 and IPv6 enablement:
   ```
   [MGR_ATTACH_LIST]
   CMD_LINE=(zsslmgr, NAME=sslmgr4,PORT=443) RESTART=YES
   CMD_LINE=(zsslmgr, NAME=sslmgr6,ADDR=::,PORT=443 RESTART=YES
   ```

3. The Core configuration program also increase the `ATTACH_LIST_SLOTS` value by 2 to accommodate the new `CMD_LINE` entries.

   Note: If the `edmprof` file has been changed manually, ensure it is saved with UTF-8 encoding, and restart the service for the RCA Configuration Server (`ZTopTask.exe`).

4. To verify the SSL configuration changes are reflected in the RCA Configuration Server service (`ZTopTask.exe`), check the log files; you will find two SSL managers waiting to accept incoming requests. See the examples shown in "Log Messages" below.

Log Messages

Session Log Messages with SSL Disabled

```
02I 22:22:04 <ztcpmgr /1DC> System Task --- TCP Manager task has started

NVD0404I 22:22:04 <TCP/IP Manager /1DC> System Task --- TCP/IP Manager accepting requests at address <RPS> on port <3464>

NVD0402I 22:22:04 <ztcpmgr /954> System Task --- TCP Manager task has started

NVD0404I 22:22:04 <TCP/IP Manager /954> System Task --- TCP/IP Manager accepting requests at address <::> on port <3464>
```

Session Log Messages with SSL Enabled

```
NVD0414I 15:04:36 <zsslmgr /7E8> System Task --- SSL Manager Task has started

NVD0472I 15:04:36 <SSL Manager /7E8> System Task --- SSL Manager accepting requests at address <RPS> on port <0443>

NVD0414I 15:04:36 <zsslmgr /188> System Task --- SSL Manager Task has started

NVD0472I 15:04:36 <SSL Manager /188> System Task --- SSL Manager accepting requests at address <::> on port <0443>
```

Component: HPCA Application Usage Manager

The usage data is stored at the destination point you define in the COLLDEST attribute of the PRIMARY.USAGE.UMDESTPT class. You must specify the IP version over which this communication should happen. Use the attribute IPVER in the PRIMARY.USAGE.UMDESTPT class to specify the IP version to be used. The following table summarizes the IP version that is used based on the values that you specify for this attribute:

IPVER	Description
4	The communication happens through IPv4.

IPVER	Description
6	The communication happens through IPv6.
46	The Core server first searches for IPv4 for communication. If IPv4 is not found, the Usage agent searches for IPv6. This is the default behavior.
64	The Core server first searches for IPv6 for communication. If IPv6 is not found, the Usage agent searches for IPv4.

Component: HPCA OS Manager

If you want to deploy OS using Linux Service OS using IPv6, you need to add an additional parameter in the configuration file based on where you are trying to deploy the OS from.

If you are deploying the OS using CD, add the IPVER argument in the `[_SVC_LINUX_]` section of the `rombl.cfg` on media.

If you are deploying the OS through the RCA Core server, and add the IPVER argument in the `[_SVC_LINUX_]` section of the `default` file located at `<InstallDir>\Data\BootServer\X86PC\UNDI\boot\linux.cfg` as follows.

```
[_SVC_LINUX_]

KERNEL=bzImage

APPEND=initrd=rootfs.gz root=/dev/ram0 rw quiet pci=nommconf vga=0x311
splash=silent IPVER=64
```

The following table summarizes the IP version that is used based on the values that you specify for this attribute:

Value	Description
4	Linux SOS enables IPv4 communication.
6	Linux SOS enables IPv6 communication.
46 or 64	Linux SOS enables IPv4 as well as IPv6 communication.

Component: RCA Agent

RCA Agent can listen on IPv4 or IPv6 for Core and Satellite servers communications. The agent installation program automatically enables the agent to listen on both IPv4 and IPv6 stacks, if it detects an IPv6 stack is available. In default RCA agent installation, IPv4 is searched first for all external communications. To change the default order, modify the `install.ini` before installing the RCA Agent.

The install.ini file is used 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. Settings in install.ini override the defaults stored in `HPCAE-MgmtApps.msi`. You can create your own customized

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

Set the following argument in the `[Objects]` section of the `install.ini` file:

`ZMASTER_IPVER` = 64

Value	Description
4	The external communication will happen through IPv4.
6	The external communication will happen through IPv6.
46	RCA agent will search for IPv4 first for external communication. If IPv4 is not found, the agent will search for IPv6. This the default behavior.
64	RCA agent will search for IPv6 first for external communication. If IPv6 is not found, the agent will search for IPv4.

Note: ZMASTER_IPVER should be either 64 or 6 for the RCA agent to connect to RCA Server using IPV6 subnet.

Log Messages

To verify if the RCA agent connects to the RCA Core server using IPv6, check the connect.log file under `<InstallDir>\Agent\logs` on the managed device.

```
NVD000010A [zbuild_identity] 09:53:24 [RADCONCT / 00000e9c] SYSTEM ---
Client IP address: [192.168.3.131]

NVD000010I [send_harbingers] 09:53:24 [RADCONCT / 00000e9c] SYSTEM ---
Client active IP = [2002:f9a:4a3a:0:3592:30d0:ddb9:bb2e]

NVD111111V [zsend_object ] 09:53:24 [RADCONCT / 00000e9c] SYSTEM ---
Sending [IDENTITY] to the Configuration Server
```

Appendix E

Customizing the Windows Answer File

This appendix contains the following topics:

These topics pertain to the process of capturing and publishing operating system images so that they can be deployed to managed devices in unattended mode (requiring no user interaction on the client devices).

Customizing the unattend.xml File

RCA provides an answer file that you can use for unattended OS installations. This answer file is called `unattend.xml`.

Each operating system and architecture (for example, 32-bit or 64-bit) has its own `unattend.xml` file. The files are located in subdirectories of:

<InstallDir>`\Data\OSManagerServer\capture-conf`

The header at the beginning of the file shows you the OS, architecture, and deployment method to which the file applies.

If you want to use the `unattend.xml` file that HP provides, you must modify it for your environment before you publish the OS image. Here are some settings that you will want to customize:

Caution: At a minimum, you must specify a valid product key (see "ProductKey" on next page). Modifying the other settings discussed here is optional.

Use a text editor to modify a copy of the pertinent `unattend.xml` file. You can name this copy anything that you like as long as it has the `.xml` file extension. When you publish the OS image, you will specify where your customized answer file is located.

Note: The Windows Automated Installation Kit (AIK) includes a file called `Unattend.chm`.

This is a compiled online help file that contains reference information about the contents of the `unattend.xml` file. See this help file for more detailed information about the settings discussed here and the other settings available that you can customize. To open the file, simply double-click `Unattend.chm`.

ProductKey

The `<ProductKey>` element appears in different places in the `unattend.xml` file depending on the specific OS image, architecture, and deployment method that you are using. The `<ProductKey>` is a string with 29 characters that is delimited like this:

`XXXXX-XXXXX-XXXXX-XXXXX-XXXXX`

Note: For all DVD installations, be sure that `/IMAGE/INDEX` is pointing to the correct image on the DVD (see "MetaData" on page 460).

Retail Editions

For retail editions of Windows (for example, Windows 7 Ultimate), make the following modifications:

- Put a valid product key in the `<Key>` element inside the `<ProductKey>` element. For example:

```
<UserData>

<AcceptEula>true</AcceptEula>

<ProductKey>

<Key>XXXXX-XXXXX-XXXXX-XXXXX-XXXXX</Key>

<WillShowUI>OnError</WillShowUI>

</ProductKey>

</UserData>
```

  This element is located in the "Microsoft-Windows-Setup" component in the “WindowsPE” in pass.

- Remove the entire `<ProductKey>` element located in the “Microsoft-Windows-Shell-Setup” component in the “specialize” pass:

```
<ProductKey>XXXXX-XXXXX-XXXXX-XXXXX-XXXXX</ProductKey>
```

Business Editions

For business editions of Windows (including Business, Enterprise, Professional, or Server editions), make the following modifications:

- Remove all characters in the `<Key>` element located in the located in the "Microsoft-Windows-Setup" component in the “WindowsPE” in pass (see example above):

```
<Key></Key>
```

- Put a valid product key in the `<ProductKey>` element located in the “Microsoft-Windows-Shell-Setup” component in the “specialize” pass:
  `<ProductKey>XXXXX-XXXXX-XXXXX-XXXXX-XXXXX</ProductKey>`

  If you are using a Volume License Multiple Activation Key (MAK), use that in the `<ProductKey>` element.

Note: In the Windows AIK, the `<Key></Key>` element supports an empty value, but the `<ProductKey>` element does not—hence `<ProductKey>` element must be deleted if it is not being used (see "Retail Editions" on previous page).

64-Bit Platforms

When you are using a DVD with the Windows Setup deployment method on some 64-bit architectures, be sure to make the following modifications:

- Remove all characters in the `<Key>` element located in the located in the "Microsoft-Windows-Setup" component in the “WindowsPE” in pass (see example above):
  `<Key></Key>`
- Put a valid product key in the `<ProductKey>` element located in the “Microsoft-Windows-Shell-Setup” component in the “specialize” pass:
  `<ProductKey>XXXXX-XXXXX-XXXXX-XXXXX-XXXXX</ProductKey>`
- Make sure that `/IMAGE/INDEX` points to the correct image on the media (see "MetaData" on page 460).
- Change `"amd64"` to `"x86"` in the following component specifications in the “WindowsPE” pass:

  ```
  <component name="Microsoft-Windows-International-Core-WinPE"
  processorArchitecture="amd64" ...
  ```

  ```
  <component name="Microsoft-Windows-Setup"
  processorArchitecture="amd64" ...
  ```

- During publishing, when you are prompted for the source directory, specify the one from the 32-bit media for the same operating system.
  - Special instructions for Windows 2008 R2 x64:
  - Use the Windows 7 Enterprise Edition 32-bit installation media.
  - Before you publish the OS image, follow these steps:
    i. a) From the Windows 7 32-bit installation media, copy the *mediaDrive*`:\sources` folder to `c:\temp`
    ii. b) Remove the Windows 7 media, and load the Windows 2008 R2 x64 media.
    iii. c) From the Windows 2008 R2 x64 installation media, copy the *mediaDrive*`:\sources\license` folder to `c:\temp\sources`

  If prompted to overwrite existing files, do so.

  This ensures that the Windows 2008 Server R2 EULAs are available from the Windows 7 installation folder.

Note: For more information, seethe “ProductKey” topic in the `Unattend.chm` help file included in the Windows AIK.

Caution: RCA does not currently support image capture for Windows Setup deployment on 64-bit platforms.

TimeZone

The `<TimeZone>` element appears in different places in the `unattend.xml` file depending on the specific OS image, architecture, and deployment method that you are using.

For example, in the `unattend.xml` file for a captured Windows 7 (x86) image, there are two places where the `<TimeZone>` element appears:

- In the `Microsoft-Windows-Shell-Setup` component under `<settings pass=”oobeSystem”>`
- In the `Microsoft-Windows-Shell-Setup` component under `<settings pass=”specialize”>`

Change the `<TimeZone>` to match the target devices to which the OS will be deployed. For example:

```
<TimeZone>Eastern Standard Time</TimeZone>
```

It is important that the spelling of the time zone exactly match the spelling used in the Windows Registry. For more information, see the “Language Pack Default Values” topic in the `Unattend.chm` help file included in the Windows AIK.

Note: Greenwich Mean Time is now known as Coordinated Universal Time.

Note: On a computer running Windows 7 you can use the `tzutil` command to list the time zone for that computer.

RegisteredOwner and RegisteredOrganization

These elements appear in different places in the `unattend.xml` file depending on the specific OS image, architecture, and deployment method that you are using.

For example, in the `unattend.xml` file for a captured Windows 7 (x86) image, there are two places where these two elements appear:

- In the `Microsoft-Windows-Shell-Setup` component under `<settings pass=”oobeSystem”>`
- In the `Microsoft-Windows-Shell-Setup` component under `<settings pass=”specialize”>`

Change these elements to the name of your company (or the entity to whom the operating system is registered). For example:

```
<RegisteredOrganization>Hewlett-
Packard</RegisteredOrganization>

<RegisteredOwner>Hewlett-Packard</RegisteredOwner>
```

These strings can be up to 256 characters in length.

See the "RegisteredOrganization" and "RegisteredOwner" topics in the `Unattend.chm` help file included in the Windows AIK for more information.

JoinDomain

You can instruct target devices to either join a domain or a workgroup after the OS is installed. Workgroup mode is the default. To instruct targets to join a domain, modify the following element:

```
<component name="Microsoft-Windows-UnattendedJoin" ... >

<Identification>

<Credentials>

<Domain></Domain>

<Password></Password>

<Username></Username>

</Credentials>

<JoinDomain></JoinDomain>

</Identification>

</component>

For example:

<component name="Microsoft-Windows-UnattendedJoin" ...>

<Identification>

<Credentials>

<Domain>lan.mycompany.com.de</Domain>

<Password>T3ch3d08</Password>

<Username>administrator</Username>

</Credentials>

<JoinDomain>lan.mycompany.com.de</JoinDomain>

</Identification>

</component>
```

Note: The user specified must have an access level sufficient to join the domain.

Note: If any of this information is missing or incorrect, the device will join a workgroup instead of a domain.

Note: If the target device was previously managed by RCA, and the device was previously a member of a domain, the stored domain information will override the contents of the `<Domain>` and `<JoinDomain>` elements in the `unattend.xml` file.

Note: Any information that is set centrally—for example, by using an OS management script to set the domain—will override information in `unattend.xml`.

See the "JoinDomain" topic in the `Unattend.chm` help file included in the Windows AIK for more information.

MetaData

If you are deploying an operating system image directly from a DVD, you must specify the location of that image within the WIM file on the DVD. In the WIM file, this information is organized like this:

```
<WIM>

<IMAGE INDEX="2">

<NAME>MyWIM</NAME>

<DESCRIPTION>MyCustomWindowsImage</DESCRIPTION>

</IMAGE>

</WIM>
```

In the `unattend.xml` file, the image information is specified in the `<MetaData>` element in the `Microsoft-Windows-Setup` component hierarchy under `<settings pass="WindowsPE">`. For example:

```
<MetaData>

<Key>/IMAGE/INDEX</Key>

<Value>2</Value>

</MetaData>
```

The `<Key>` element indicates which data item in the WIM file to match. It can be any of the following:

- `IMAGE/INDEX`
- `IMAGE/NAME`
- `IMAGE/DESCRIPTION`

The `<Value>` element indicates what the value of this data item should be. Here, the image to be deployed has an `IMAGE/INDEX` value of `2` in the WIM file.

You can extract a list of the images in a WIM file by using the following command:

```
imagex /info WIMFileName > c:\info.txt
```

Here, *WIMFileName* is the name of the WIM file (for example, `install.wim`). Be sure to redirect the output of the command to a text file (as shown here) so that you can easily search through the results.

For more information, see the *MetaData* topic in the `Unattend.chm` help file included in the Windows AIK.

XML File Processing in RCA

The `unattend.xml` file that you publish is overlaid on top of any `unattend.xml` file that is present in the image that was published.

Before RCA starts the image install, the published XML is combined with the `substitutes` file to generate the final `unattend.xml`.

This combining of files is done by RCA before it starts the actual image installation. The previously exposed `substitutes` file is now used behind the scenes. Each operating system and architecture (for example, 32-bit or 64-bit) has its own file. The files are located in subdirectories of:

<InstallDir>`\Data\OSManagerServer\capture-conf`

The correct file is selected automatically depending on the processor architecture of the image being published.

The following table lists the settings in the `unattend.xml` file that are updated when the `substitutes` file is published.

Caution: The settings in blue (`CommandLine`, `Path`, and both instances of `PartitionID`) are required for RCA to work. They cannot be removed.

substitutes File

Settings Pass	Component	Path	Setting	Override Value
windowsPE	Microsoft-Windows-Setup	DiskConfiguration/Disk/ModifyPartitions/ModifyPartition	PartitionID	DISKPART volume ID to which RCA will install the OS
windowsPE	Microsoft-Windows-Setup	ImageInstall/OSImage/InstallTo/	PartitionID	DISKPART volume ID to which RCA will install the OS
windowsPE	Microsoft-Windows-Setup	ImageInstall/OSImage/InstallFrom/	Path	WIM file to use for installation

Settings Pass	Component	Path	Setting	Override Value
oobe-System	Microsoft-Windows-Shell-Setup	AutoLogon/	Domain	Computer name (for auto-logon)
spe-cialize	Microsoft-Windows-Shell-Setup	AutoLogon/	Domain	Local computer name (for auto-logon)
spe-cialize	Microsoft-Windows-Unat-tendedJoin	Identification /Credentials/	Domain	Centrally set domain using get-machinename.tcl or pre-existing device entry in the RCA Core Console
spe-cialize	Microsoft-Windows-Unat-tendedJoin	Identification/	JoinDomain	Centrally set domain using get-machinename.tcl or pre-existing device entry in the RCA Enterprise console
spe-cialize	Microsoft-Windows-Shell-Setup		Com-puterName	Computer name
oobe-System	Microsoft-Windows-Shell-Setup	First-LogonCommands /Sy-nchronousCommand	Com-mandLine	Path to agent install media installer

You can, if required, customize the `substitutes` file to disable certain customizations or to add new ones. You cannot however remove or change the `PartitionID` or `CommandLine` settings.

About the .subs

Caution: RCA now enables you to specify the source of this information when you run the Publisher. See "Publishing Operating System Images" on page 392 for more information.

Note: This topic does not apply to Windows XP or Windows 2003.

The RCA Publisher is backward compatible. It supports publishing saved OS images that consist of a `.WIM` file, a `.EDM` file, a `.XML` file, and a `.SUB` file.

If you choose to manually pre-create `*.SUBS` and `*.XML` files, they must have the same prefix as the `*.WIM` file. For example: `vista.WIM`, `vista.SUBS`, and `vista.XML`. All three files must be stored in the same directory.

Note: When you run the RCA Publisher, if it finds a `*.SUBS` and `*.XML` file in the same directory as the `*.WIM` file, it will not prompt you for an `unattend.xml` file.

RCA provides samples of these files on the Image Capture media in subdirectories of the following folder:

```
\samples\unattend
```

If you choose to use the sample files, rename them and then modify them as needed—for example, setting the `<TimeZone>` and the `<ProductKey>`.

The `*.XML` file is an answer file that contains standard information as well as placeholders for information that will be included from `*.SUBS`. You can use the Microsoft Windows System Image Manager (SIM) tool to make additions to the `*.XML` file. If you do so, you must first open the corresponding `*.WIM` file before opening `*.XML`.

Caution: If you choose to use `*.XML` and `*.SUBS` files, you must specify your Windows installation product key in the `*.XML` file.

Do not delete any XML values from this file! If you modify the `*.XML` file incorrectly, you may cause your installation to fail.

If you see errors in the Messages section in the SIM tool similar to "`…The value $$SUBSTR$$ is invalid…`" you can ignore them.

When you save the file, you may also see a message similar to "`There are validation errors in the answer file. Do you want to continue?`" Click **Yes** to continue.

The `*.SUBS` file is the "substitutes" file that lists each XML item to be modified in `*.XML` and what its value should be. The lines in the `*.SUBS` file are known as XPATHs.

Note: Information entered in the `*.SUBS` file takes precedence over information in the `*.XML` file.

Example of Substitution

If you want to see how substitution works, you can review the following example which will show how the JoinDomain attribute gets changed from "`anything`" in the *filename*`.XML` file to "`VistaTeam`" in the `unattend.xml` file.

Note: Code that appears within <> should appear all on one line in the `*.XML` file.

1. Locate the appropriate `unattend*.xml` and `substitutes` files for your operating system, target device architecture, and deployment method. These files are located under `samples\` on the ImageCapture CD.

2. Make a copy of the `unattend*.xml` file, and name it *filename*`.XML`, where *filename* matches the name of your `.WIM` file. Store the copy in the same directory as your `.WIM` file.
3. Make a copy of the `substitutes` file, and name it *filename*`.SUB`. Store the copy in the same directory as your `.WIM` file.
   You should now have the following three files in one directory:
   - *filename*`.WIM`
   - *filename*`.XML`
   - *filename*`.SUB`
4. Locate the XML element for JoinDomain in the *filename*`.XML` file. It should look similar to this example:

```
<?xml version="1.0" encoding="utf-8"?>

<unattend xmlns="urn:schemas-microsoft-com:unattend">

 <settings pass="specialize">

<component name="Microsoft-Windows-UnattendedJoin"
processorArchitecture="x86" publicKeyToken="31bf3856ad364e35"
language="neutral"
versionScope="nonSxS"
xmlns:wcm="http://schemas.microsoft.com/WMIConfig/2002/State"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

 <Identification>

 <JoinDomain>anything</JoinDomain>

 </Identification>

 </component>

 </settings>

 <cpi:offlineImage cpi:source="wim://hpfcovcm/c$/vista_
inst/vista.wim#Windows Vista ULTIMATE" xmlns:cpi="urn:schemas-
microsoft-com:cpi"/>

</unattend>
```

5. Modify the following XPATH element in the *filename*`.SUB` file. Note that this XPATH element appears on a single line in the *filename*`.SUB` file.

```
//un:settings[@pass='specialize']//un:component[@name=Microsoft-
Windows-
Unat-
tendedJoin'][@processorArchitecture='x86']/un:Identification/un:
JoinDomain,VistaTeam
```

During deployment of the operating system, the *filename*`.SUB` and *filename*`.XML` files will be combined to create an `unattend.xml` file that is used to provide information during all phases of the Windows setup. In this example, the JoinDomain attribute will be set to **VistaTeam**.

Appendix F

Capturing Windows XP and Windows Server 2003 OS Images

The information in this appendix pertains only to Windows XP and Windows Server 2003 OS image captures. For information about capturing Windows Vista, Windows Server 2008, Windows 7, and all supported Thin Client operating systems—as well as important image capture process overview information—see "Preparing and Capturing OS Images" on page 365.

Note: RCA only supports capturing unencrypted partitions.

Caution: The Legacy OS image capture method is not supported for devices where the hard drive is configured for RAID0 through a SATA drive controller. Use the Windows ImageX method instead.

If you select the Legacy method, the boot order must be set to CD before you start the capture process.

About the HPCA Image Preparation Wizard

You can use the HPCA Image Preparation Wizard to capture Windows XP or Windows 2003 Server OS images for ImageX, Windows Setup, or Legacy deployment (see "Deployment Methods" on page 367 for more information).

The Image Preparation Wizard performs the following tasks:

1. Collects and stores information (including hardware and OS information capabilities) about the reference machine.
2. Executes the exit points that are available for your use as needed. `PRE.CMD` is executed before the Image Preparation Wizard starts SysPrep to seal the image. `POST.CMD` is executed after Sysprep has sealed the image. See "Image Preparation Wizard Exit Points" on next page for details.

   Note: Image Capture exit points are only supported for ImageX and Windows Setup capture types.

3. Runs Microsoft Sysprep (on supported operating systems).
4. Restarts the reference machine into the Service OS (booted from the appropriate media). The Service OS runs to collect the image and its associated files.
   During the capture, status information is displayed on the Service OS screen. See "About the Windows PE Service OS Screen" on page 385 for more information.

5. Creates and copies files to the following directory on the RCA server:
   <InstallDir>\Data\OSManagerServer\upload

   If you choose to create a Legacy image, the files uploaded are:

   - ImageName.IMG
     This file contains the gold image. This is a compressed, sector-by-sector copy of the boot partition from the hard drive system that may be very large. The file contains an embedded file system that will be accessible when the image is installed.
   - ImageName.MBR
     This file contains the master boot record file from the reference machine.
   - ImageName.PAR
     The file contains the partition table file from the reference machine.
   - ImageName.EDM
     This file contains the object containing inventory information.

   If you chose to create an image using ImageX or using Windows Setup, the files uploaded are:

   - ImageName.WIM
     This file contains a set of files and file system information from the reference machine.
   - ImageName.EDM
     This file contains the object containing inventory information.

Image Preparation Wizard Exit Points

You can use exit points for the Image Preparation Wizard as needed. For example, you may use them to clean up a device before performing a capture.

Note: Image Capture exit points are only supported for ImageX and Windows Setup capture types.

To use the exit points

1. Create the files PRE.CMD and POST.CMD.
2. Save these files and any supporting files in OSM\PREPWIZ\payload\default\pre and OSM\PREPWIZ\payload\default\post respectively.

The Image Preparation Wizard copies these files to %temp%\prepwiz\pre and %temp%\prepwiz\post on the reference device and removes them before the capture begins. PRE.CMD is executed before the Image Preparation Wizard starts SysPrep to seal the image. POST.CMD is executed after Sysprep has sealed the image.

A non-zero return value from either PRE.CMD or POST.CMD will cause the Image Preparation Wizard to halt. In interactive mode, you can decide to Stop or Ignore the error and continue. In batch mode, the Image Preparation Wizard will halt.

Prerequisites for Capturing Images

The following steps must be completed before performing an OS image capture for ImageX, Windows Setup, or Legacy deployment:

- "Prepare the Reference Machine" below
- "Install the Windows AIK" on next page
- "Install and Configure Sysprep" on page 469

Prepare the Reference Machine

Before installing the operating system, make sure that the OS partition on the reference machine should be aligned to 4 KB boundary. To prepare the reference machine, perform the following steps:

1. Install the operating system from the original product media. The reference machine must be capable of running the operating system you are installing. Make sure the reference machine is using DHCP.

   Caution: Store the OS on the C: drive. It is the only drive that will be captured.

2. Customize the OS as necessary. This may include installing a set of basic or required applications. Be sure to include the latest service packs for the OS and applications and all required drivers for the devices to which you will deploy the image. The following Microsoft knowledge base article contains information about including OEM drivers for Windows OS installations:
   Article: 314479 - How to Add OEM Plug and Play Drivers to Windows XP

   http://support.microsoft.com/default.aspx?scid=kb;en-us;314479

3. Make sure that the Microsoft .NET Framework version 2.0 (or later) is installed. The .NET Framework is available at the Microsoft download center:
   http://www.microsoft.com/downloads

   To determine which version of the .NET Framework is present on the reference machine, list the folders in the following directory:

   `%SYSTEMROOT%/Microsoft.NET/Framework`

4. If you plan to use the Legacy method to deploy this image, you must install the RCA agent on the reference machine. This is not necessary for Windows Setup or ImageX deployments, because RCA requires you to publish the agent along with the OS image for Windows Setup or ImageX.
   For Legacy deployment only:

   Install the agent from the RCA installation media as per your requirements—at a minimum, you must install the Application Manager and OS Manager agents. These are required so that when the OS image is deployed, the device can connect to RCA server. If you need to update the agents, you must use agent self-maintenance.

5. Configure the BIOS power management so that the device does not power down after a few minutes of keyboard or mouse inactivity before the upload process to the RCA server is finished.
6. Keep the image file size as small as possible. The ideal configuration is a partition just large enough to fit the operating system, plus additional space for the RCA agent.

   Note: For Windows operating system before Windows 7, Persistent supports deploying the image to the primary boot partition of the primary boot drive.

   Caution: To successfully capture an image using the Windows Setup deployment method, you must have sufficient free disk space in the OS partition on the reference machine. For example, to capture a 7 GB image, you will need 50-60 GB of free disk space.

   The following steps help to minimize the size of the `.WIM` image file:

   a. Create free space.
   It recommends that after you have created the smallest partition with the least amount of free disk space as possible, set `ExtendOemPartition = 1` in the `[Unattended]` section of the `Sysprep.inf` file to allow for the small image to be installed on a target device with a much larger drive.

   When `ExtendOemPartition= 1`, the Microsoft Mini-Setup Wizard will extend the OS installation partition into any available non-partitioned space that physically follows on the disk. The RCA agent can then use the free space on the volume for application installations.

   b. If you are using a laptop, disable hibernation.

   c. If necessary, remove the recovery partition.

   d. Disable the paging file. The page file will be enabled automatically when mini-setup is run after the deployment.

   e. Turn off System Restore.

   f. Turn off Indexing Service and Disk Compression.

   g. Turn off On Resume Password Protect.

Install the Windows AIK

If you will use ImageX or Windows Setup for deployment, the Windows Automated Installation Kit (AIK) must be installed on the RCA Core—where you will publish OS images to the CSDB. This is a Core installation prerequisite.

See "Installing RCA Core Server" in the *Radia Client Automation Enterprise Installation and Upgrade Guide* for more information.

Install and Configure Sysprep

Microsoft Sysprep is a program that enables you to distribute Microsoft operating systems using cloned images. The HPCA OS Image Preparation Wizard runs Microsoft Sysprep to strip out all of the security identifiers and reset the image.

After the operating system image is delivered to the target device, the Microsoft Mini-Wizard runs automatically when the target device is started. After using the answers provided by `Sysprep.inf`, the Microsoft Mini-Wizard deletes the Sysprep directory on the target device.

Installing Sysprep

To install Sysprep, complete the following steps:

1. Download Microsoft Sysprep to distribute Microsoft operating systems using cloned images.

   Note: Review Microsoft's documentation for information about how to use Sysprep, how to create a `Sysprep.inf` file, and how to set the available parameters.

2. On the Microsoft operating system installation media, locate the `DEPLOY.CAB` file in the `SUPPORT\TOOLS` folder. See Microsoft's documentation for details.

3. Extract the Microsoft Sysprep files from the `Deploy.cab` file. Copy these files to `C:\SysPrep` on the reference machine and make sure the directory and files are not set to read-only.

   Note: Be sure that you are using the latest Sysprep version. If you use an older version, you may receive an error.

   If you do not have the appropriate version of Sysprep, you can download it from the Microsoft web site.

   Even if you have administrator rights, make sure that you have the appropriate user rights set to run Sysprep. See article #270032, *User Rights Required to Run the Sysprep.exe Program* on the Microsoft web site. If you do not have the appropriate user rights, when Sysprep runs, you will receive the following error:

   ```
   You must be an administrator to run this application.
   ```

   The Image Preparation Wizard will exit and after you set up the appropriate user rights you will need to run the wizard again.

4. Be sure that the reference machine is part of a WORKGROUP and not a domain to use the Microsoft Sysprep.

5. Create a `Sysprep.inf` and save it to `C:\Sysprep`.

Creating Sysprep.inf

To create `Sysprep.inf`, complete the following steps:

You can create `Sysprep.inf` manually or use the Microsoft Setup Manager (`Setupmgr.exe`). The Setup Manager can be found in the `Deploy.cab` file in the `SUPPORT\TOOLS` folder of a Microsoft OS distribution media. See Microsoft's documentation for more information.

Sample `Sysprep.inf` files are available on the Image Capture media in the `\samples\sysprep\` directory.

Caution: The `Sysprep.inf` file should not be greater than 800 KB in size.

When creating the `Sysprep.inf` file:

- Adjust the `TimeZone` value for your enterprise.
- Set up the `AdminPassword`.
- Make sure to include a product key so that the user will not need to type this at the target device.
- In order to have an unattended installation, you must include `UnattendMode = FullUnattended` in the `[Unattended]` section.
- Set `ExtendOemPartition` to 1, so that Microsoft Sysprep will extend the OS partition into any available non-partitioned space that physically follows on the disk.
- If `JoinDomain` is present in `Sysprep.inf`, then `Sysprep.inf` has to have the Admin User ID and Password of an account in the domain that has the rights to join the computer to the domain. Note that `JoinDomain` is case sensitive.

Sysprep.inf File Prioritization

The `Sysprep.inf` file can be delivered with the operating system image, or it can be delivered as a package that is connected to the operating system image (known as an override Sysprep file). If the `Sysprep.inf` file is published separately, it will be merged with the `Sysprep.inf` file in the image's NTFS into a single, combined `Sysprep.inf`.

`Sysprep.inf` files are prioritized in the following order, from lowest to highest:

1. Sysprep embedded in the image (lowest priority). If there is no separately published `Sysprep.inf` (override Sysprep), just the `Sysprep.inf` in the image will be used.
2. Override Sysprep (a Sysprep file that is separate from the gold image. See "Using an Override Sysprep File" in the *Radia Client Automation Enterprise OS Management Reference Guide* for details).

   Note: Only one override `Sysprep.inf` will be resolved.

3. Sysprep attached to policy criteria (highest priority).

   Note:
   - To attach a Sysprep file to policy, you must publish the Sysprep file to the CSDB and then use the Administrator CSDB Editor to manually connect the Sysprep instance to the appropriate Policy instance.

- Even if you override the `Sysprep.inf`, the `ComputerName` (`COMPNAME`) and `JoinDomain` (`COMPDOMN`) are still updated by RCA based on the Computer Name and Domain stored in the ROM object.

Capturing OS Images

Refer to the instructions for the type of capture you want to perform:

Deployment Method	Instructions
ImageX, Windows Setup, Legacy	"Capture Images Using the Image Capture Wizard" below or "Capture Images Using the Image Preparation Wizard in Unattended Mode" on page 476
Windows Native Install Packager	"Capture Images for Deployment using the Windows Native Install Packager" on page 477

Capture Images Using the Image Capture Wizard

The following instructions pertain to OS image capture for ImageX, Windows Setup, or Legacy deployment.

To use the HPCA OS Image Preparation Wizard:

Note: If you are capturing an image locally, before continuing, set the reference machine to boot from the CD-ROM/DVD drive. You must do this because the ImageCapture media is bootable. When you run the ImageCapture media, it reboots the device to upload the image.

1. Insert the ImageCapture media into the reference machine. See “Product Media” in the *Radia Client Automation Enterprise OS Management Reference Guide* if you need more information about where to get this media.
2. On the ImageCapture media, go to `\image_preparation_wizard\win32`, and run `oscapture.exe`.

   Note: If the RCA agent is not installed on the reference machine, you will see the following message.

   ```
   This computer does not have the Application Manager installed.
   You may not be able to manage the target computers with the OS
   Manager product.
   ```

   If you want the device to be managed, you must install the RCA agent before running the Image Preparation Wizard.

Note: The `oscapture.exe` program requires the Microsoft .NET Framework version 2.0 (or later), which is available at the Microsoft download center:

http://www.microsoft.com/downloads

To determine which version of the .NET Framework is present on the reference machine, list the folders in the following directory:

`%SYSTEMROOT%/Microsoft.NET/Framework`

- If you are capturing an image to be deployed using the Legacy method, the Image Preparation Wizard verifies that the `C:\Sysprep` folder exists and that the RCA agent is installed before continuing.
- If you are capturing an image to be deployed using ImageX or Windows Setup, the Image Preparation Wizard will locate Sysprep in `C:\sysprep`.

Caution: When you deploy using Windows XP Service Pack 2 using either ImageX or Windows Setup, the RCA agent will be injected into the image during the deployment process.

If you want to install the agent to a location other than the default location on your target devices, you must edit the `INSTALLDIR` property in `install.ini`. See the *Radia Client Automation Enterprise Installation and Upgrade Guide* for details on modifying `install.ini`.

It is important to note that if you have already installed the agent to a location other than the default in your image, you must update the `INSTALLDIR` property in install.ini as well.

If the agent is installed in the default location, do not make any changes to`install.ini`*.*

You must edit `install.ini` before using the Publisher to publish the image to the RCA database.

Note: When using the Publisher, you will be given an option to select where to get the agent. This is advantageous, because you can package the agent independently and can update the agent as needed by publishing a new version to the CSDB. After you do this, all new `.WIM` deployments will automatically use the latest agent.

3. Click **Next**.
   The End User License Agreement window opens.
4. Click **Accept**.
   The deployment methods that may appear are:
   - `Legacy` captures a raw disk image of the partition (`.IMG` format).
   - `ImageX` captures an image in `.WIM` format that will be deployed using Windows PE and the ImageX utility.

- `Windows Setup` captures an image in `.WIM` format that will be deployed using Windows PE and Windows Setup.

If a deployment method is not supported for this OS, it will not appear.

5. Select the deployment method that you want to use, and click **Next**.
6. Type the IP address or host name and port for the RCA server. This must be specified in the following format:
   xxx.xxx.xxx.xxx:*port*

   The RCA server port used for OS imaging and deployment in an RCA Core and Satellite installation is 3466. In an RCA Classic installation, port 3469 is reserved for this purpose.
7. Click **Next**.
8. Type a name for the image file. This is the image name that will be stored in the *<InstallDir>*`\Data\OSManagerServer\upload` directory.
9. Click **Next**.
   The Span Disk Image window opens.
10. Type the amount of the total uncompressed disk space (in MB) to use for each image file. Type `0` (zero) if you do not want to create a spanned image.
    Use spanned images to break the image file into smaller segments. Each segment of a spanned image is restricted to 4000 MB. This is helpful so that you can comply with the restriction of whole images needing to be less than 4000 MB so that they can be stored in the CSDB.

    If this value is set to 0 (zero), and the size of the image resource files exceeds 4000 MB, the image will be spanned automatically.
11. Click **Next**.
    If appropriate, the Additional Sysprep Options window opens. The text box is pre-filled with a command that clears all the SIDs to prepare the machine for capture.

    If you want, you can type additional options to pass to Sysprep using a space as the delimiter.

    Caution: This is an advanced option. Any additional options that you add or changes that you make are not validated and may result in image capture or deployment failure. Use with caution or when instructed to do so by Persistent Software Support personnel.

    Review Microsoft's documentation for information about additional Sysprep options
12. Click **Next**.
13. If you chose ImageX for the deployment method, the Select Image Preparation Wizard payload window opens with the default option selected.

    Note: The payload contains Local Service Boot (LSB) data to be delivered to target devices.
14. Type a description for the image file and click **Next**.
    The Select the Windows Edition window may open.

    Select the Windows edition that you are capturing and click **Next**.

15. The Options window may open.

    Note: If you do not have the RCA agent installed, you will not see the **Perform client connect after OS install** check box. It is important to have this agent installed only if you are using the Legacy method to capture an image.

16. Select the appropriate options.

    Note: The options appear depending on the operating system that you are capturing.

    - **Build Mass Storage Section in Sysprep.inf**
      Select this check box to build a list of the Mass Storage drivers in the `[SysprepMassStorage]` section of the `Sysprep.inf` for Windows XP and above.

      Note: The list of Mass Storage Drivers is installed in the registry. This takes about 15-20 minutes, but provides fundamental mass storage device drivers to ensure success of image deployment across machine models and manufacturers.

      If there are any errors in these entries, subsequent Sysprep execution can fail.

    - **Optimize compression of unused disk space**
      Select this check box to optimize compression of unused disk space. This adds zeroes up to the end of the system drive partition. Note that this may take some time depending on the size of the hard drive.
      This increases the compressibility of the captured image, reducing its size. Smaller image files require less disk space to store and less bandwidth to move across the network.

    - **Resize partition before OS upload**
      Select this check box to resize the partition to make it as small as possible. If you do not select this check box, make sure that your partition is sized appropriately.

    - **Perform client connect after OS install**
      Select this check box to connect to the RCA server after the OS is installed. If this is not selected, the RCA OS connect will not occur after the OS is installed.
      This option will not appear if you are using a method where you do not have the agent installed (For example, if you are using the Legacy method and did not install the RCA agent or if you are capturing a Windows Vista (or later) image because the agent is installed during the deployment and a connect is run by default).

17. Click **Next**.
    The Summary window opens.

18. Click **Start**.

19. Click **Finish**.
    If you are working with an APIC device, the Make Image Compatible with PIC window opens. Note that Windows Vista (and later) operating systems can only be captured from and deployed to APIC compatible devices.

20. If necessary, select the **Make image compatible with machine with PIC** check box.

    Caution: Microsoft does not recommend this. Be sure to see their web site for more information before making this selection.

21. Click **Next**.
    If you selected the check box in the figure above, the Select Windows CD window opens.

22. Browse to the Windows CD-ROM and click **Next**.

23. Click **Finish** to run Sysprep.
    The Image Preparation Wizard will start Sysprep; this can take 15-20 minutes to complete, depending on the size of the image.

    Note: A message pops up if insufficient space is available on the System Reserve partition to hold the LSB injection files. You can either ignore this message or stop the Image Preparation Wizard. If you ignore the message (and have created enough space on this partition) the Image Preparation Wizard will continue. Otherwise, it will fail indicating that it cannot inject the LSB files.

    During the capture, status information is displayed on the Service OS screen. See "About the Windows PE Service OS Screen" on page 385 for more information. Sysprep will reboot the device when complete. You may need to click **OK** to restart the device.

    Note: If you are using the audit mode (previously known as factory mode), the machine will reboot to the operating system with networking enabled. After your customizations are completed, you must put the Image Capture CD/DVD into the machine and then go to a command prompt and run

    ```
    sysprep.exe –reseal –reboot
    ```

    After Sysprep restarts, the image must be uploaded to the server.

    - If the boot order is set to boot from CD-ROM first and the Image Capture media is loaded, the device will boot to the CD-ROM.
      If your device does not have a CD-ROM, you must have a PXE environment, and the device must be set to boot from the network first. Then, during the network boot you can press **F8** on your keyboard to capture the image using PXE. A menu appears and you must select Remote Boot (Image Upload).

    Caution: For Legacy capture mode, if the device does not boot to the CD (boots to operating system instead) you will need to restart the preparation process.

    Then, the device will connect to the network, and store the image on the RCA server

    Note:
    - The upload of the image may seem to take a long time. However, it is not the upload that is taking a long time, but rather the compression of the image and the optimization for compression of the unused disk space (especially if there is a lot of free disk space). This happens during the transfer of the image and therefore, the network pipe is not a

bottleneck. Transfer speeds will be approximately 300 KByte/sec to 1MByte/sec or more but may vary depending on processor speeds and your network environment.

- You may want to create copies of the files stored in the `\upload` directory so that you can retrieve them if necessary.

The Image Preparation Wizard connects to the network and stores the image on the RCA Core in the following directory:

<InstallDir>`\Data\OSManagerServer\upload`

When the upload process is complete, you will see the following message:

```
**** OS image was successfully sent to the RCA OS Manager Server.
```

Next, you will want to publish your image to the CSDB. See "Publishing" on page 387.

Capture Images Using the Image Preparation Wizard in Unattended Mode

You may use a configuration file to run the Image Preparation Wizard in unattended mode.

Using the Image Preparation Wizard in Unattended Mode

Insert the ImageCapture media into the reference machine. See “Product Media” in the *Radia Client Automation Enterprise OS Management Reference Guide* if you need more information about where to get this media.
Go to `\samples\prepwiz_unattend` and copy the OS-specific configuration file (`vista.cfg` or `xp.cfg`) to your local machine or a network location.
Make the necessary modifications. The following table lists the values that you may need to change.

Variables in the Configuration File to be Modified

Variable Name	Description	Sample Value
RISHOSTPORT	The RCA server's IP address.	*xxx.xxx.x.x:port*
IMAGENAME	The prefix used to create the uploaded files. This is appended to `.WIM` to create the name of the uploaded image.	Vista
IMAGEDESC	Description of the image that is published to the Database.	“Windows Vista Unattended Test Image”
PREPWIZPAYLOAD (for future releases)	Payload that the administrator wants to use. The payload contains Local Service Boot (LSB) data to be delivered to target devices.	Use the default value “`/OSM/PREPWIZ/payload/default/`”
OSEDITION	Specifies the edition of Vista used.	“Enterprise”

Variable Name	Description	Sample Value
(required for Vista)		
set ::setup(DEPLOYOS,SELECTED)	Set to 1 or 0 to indicate whether you want to redeploy the OS after the image capture.	"0"
set ::setup(ClientConnect,SELECTED)	Set to 1 or 0 to indicate whether you want the target device to perform an OS a connect after the image is deployed.	"1"

On the reference machine, open a command window and change to the CD/DVD directory. Go to `Image_Preparation_Wizard\win32`. Then, run the following command:
`prepwiz -mode silent -cfg <fully qualified path>\`*<config_file>*

Where *<config_file>* is the operating system-specific configuration file (for example, `setup.cfg`).

The Image Preparation Wizard starts Sysprep; this can take 15-20 minutes to complete. Sysprep reboots the device when complete, connects to the network and stores the image in the `/upload` directory on the RCA server.

Capture Images for Deployment using the Windows Native Install Packager

Note: Capture of Windows XP and Windows 2003 images for this deployment mode is only supported in RCA Enterprise Edition.

This is the only case in which you will use the HPCA Windows Native Install Packager to prepare an image. The image is of the installation media for a pre-Windows Vista operating system on a hard drive on the reference machine. The resulting image has completed the file copy phase of a Windows installation and contains the RCA agent. The image is sent to the *<InstallDir>*`\Data\OSManagerServer\upload` directory on the RCA server, and then you use the Publisher to publish the image to the CSDB.

When the image is deployed to a target device, the target device reboots, and the Windows Native Install setup continues with the text mode setup phase, followed by the GUI phase. These two phases are controlled by `unattend.txt` and allow for a completely unattended setup.

- "Task 1: Prepare the Reference Machine" on next page
- "Task 2: Create unattend.txt" on page 479
- "Task 3: Install the HPCA Windows Native Install Package" on page 479
- "Task 4: Run the HPCA Windows Native Install Package" on page 480

Task 1: Prepare the Reference Machine

The image of the original installation media created on the reference machine is deployed to target devices. Before using the RCA Windows Native Install Packager to create the image, ensure that you have the HPCA media, and that the reference machine meets the following requirements:

1. Connectivity to an RCA server.
2. A target drive, recommended being on an extended partition, that:
   - Will be used as if the target drive is currently formatted and empty (has no data). If the target drive is not formatted or it is formatted and contains data, the user will be prompted to format the drive.
   - A user can pre-format the drive with FAT32 if they format the drive and ensure that there is no data on the drive.

     Note: Note that FAT32 cannot be expanded after deployed. NTFS can be expanded and is the default.

   - Is at least 1.5 GB. If the target drive is larger, it will take more processing time when the drive is imaged or the image may be larger than necessary depending on how the "Optimize Compression of Unused Disk Space" check box is set in the Image Preparation Wizard.

     Caution: All data on the target drive will be lost.
3. A separate drive (to increase speed), such as the `C:` drive, with the HPCA Windows Native Install Packager software already installed. See "Task 3: Install the HPCA Windows Native Install Package" on next page.
4. You must also have access to the following items; specify their location when using the HPCA Windows Native Install Packager:
   - The setup files for the RCA agent.
   - The `i386` directory from your operating system media.
     You can slipstream any necessary service packs into this directory. See the `readme.txt` file associated with each service pack for more information about how to do this.

     Note: Windows setup will not allow you to run the setup for an older version of Windows. For example:

     If your device is running Windows 2003 Server, you cannot use the `i386` directory for Windows XP.

   - `unattend.txt`
     You can create the file manually or use Windows Setup Manager on your Windows media. Sample files are available on the Image Capture media in the `\samples` directory.

Task 2: Create unattend.txt

The `unattend.txt` file automates the installation of the OS so that no user input is necessary. The `unattend.txt` file must match the release of Windows specified in the i386 directory. These files may vary slightly depending on the version of Windows being installed.

Caution: The Unattend.txt file should not be larger than 800 KB.

The following are some tips about creating the `unattend.txt` file to be stored with the image:

- The settings in the file should be as general as possible so that the file can be used with any device in your environment.
- Include the statements `AutoLogon=YES` and `AutoLogonCount=1` in the `[GuiUnattended]` section of this file.
  You must use the `[GuiUnattended]` section, rather than `$OEM$\cmdlines.txt`, because the RCA agent setup uses the Windows installer to install the agent on the target device, and `$OEM$\cmdlines.txt` cannot run the Windows Installer.

  The `AutoLogon` and `AutoLogonCount` statements ensure that the agent is installed during the first user logon after the operating system is installed.
- Include the statement `extendoempartition=1` in the `[Unattended]` section of this file. This causes Windows to extend the file system and partition to include any unused space that follows the partition. If the target partition is too small, it is possible that the copy phase of the installation will work (the phase run on the reference machine). Then, when the image is deployed, the text mode phase will fail or install the OS on some other partition.
  If you use a large target partition, the process that zeroes unused space on the file runs for a long time.
- You can also create separate `unattend.txt` files for any necessary customizations. You can use the Publisher to publish these files to the SYSPREP class in the RCA DB, and then you can connect them to the appropriate OS image. When the image is deployed, the customized `unattend.txt` will be merged with the original file.

  Note: See "Publishing" on page 387 for details about publishing files. When publishing `unattend.txt` files, follow the instructions as if you were publishing a `Sysprep.inf` file.

Task 3: Install the HPCA Windows Native Install Package

1. On the Image Capture media, go to `\windows_native_install` and double-click `setup.exe`.
2. Click **Next**.
   The End User License Agreement window opens.
3. Review the terms and click **Accept**.
4. Select the directory to install the product in, and then click **Next**.
   The Summary window opens.

5. Click **Install**.
   When the installation is done, click **Finish**.

Task 4: Run the HPCA Windows Native Install Package

1. Double-click the HPCA Windows Native Install Packager icon on the desktop.
   You must complete the information in each of the three areas in the Configure Options window: Client Automation, Windows Setup, and Package.

   a. The Client Automation area contains options used to set up options related to Client Automation products.

   b. The Windows Setup area gathers information needed to perform the OS installation.

   c. The Package area gathers information needed by RCA about the package that you are creating.

   Note: If you click **Next** before completing the required fields on each of these windows, you will receive a message prompting you to complete the fields.

2. In the Client Automation Client Source Directory field, type the path for the RCA agent.
3. Select the check boxes for the Client Automation products that you want installed.
4. Select the **Run first connect after install** check box to perform an RCA OS connect after the OS is installed. If this is not selected, the RCA OS connect will not occur automatically after the OS is installed.
5. In the **Optional Packager Command Line Arguments** box, type parameters used by the WNI application. The options can be placed all on one line or on several lines. Specify the options in the keyword-value format, such as:
   `-trace_level 9`
   The keyword must always begin with a dash (`-`).

   Note: Usually you will use the Optional Packager Command Line Arguments text box only when directed by Technical Support.

   There are many parameters that can be used to create logs. The following example describes how to create a file called `C:\temp\nvdwni.log`:

   ```
   -trace_level 99

   -trace_dir c:\temp
   ```

   If you want to create a log with a different name, you can use the following:

   ```
   -trace_file filename.log
   ```

6. Click **Next**.
7. In the **unattend.txt File** box, browse to the appropriate `unattend.txt` file.
   Select a general `unattend.txt` file to be stored in the image. This file should contain options that are applicable for all devices that the image may be applied to. Later, you can attach a separate `unattend.txt` file to the image to make any necessary customizations.

> **Note:** The `unattend.txt` file must match the release of Windows specified in the `i386` directory. These files may vary slightly depending on the version of Windows being installed.

8. In the `i386 Directory` text box, select the Windows source distribution directory provided by Microsoft on its distribution media. You can use the Microsoft slipstream process to incorporate service packs and other fixes. See the `readme.txt` file that is associated with the service pack for more information about how to do this.

   > **Caution:** Be sure to copy the `i386` directory from the Windows CD-ROM to another location. If you use the CD-ROM, Windows setup assumes you will have the CD-ROM loaded on the target device and will not copy all of the necessary files.

9. In the **Target drive** drop-down list, select the drive where the native install package will be created. We recommend that this drive is on an extended partition.

   > **Caution:** All existing data found on this drive will be lost.

10. In the **Extra Command Line Parameters** text box, type any parameters that you want to pass to the Windows Setup program when it is run. See the Microsoft web site for more information about the parameters.
11. Click **Next**.
12. In the **Image Name** text box, type the name of the package that will be stored in the `\upload` directory. This name has a maximum length of eight characters and should be composed of alphanumeric characters only.
13. In the **Image Description** text box, type a description of the image (up to 255 characters).
14. In the **Client Automation OS Manager Server** text box, specify the IP address or host name for the RCA server where the image should be uploaded.
15. In the **Client Automation OS Manager Port** text box, specify the port for the RCA server.
16. Select the **Optimize Compression of Unused Disk Space** check box to null all unused disk space on the target drive before imaging it. This reduces the size of the image but causes the Image Preparation Wizard to run longer.
17. Click **Next**.
18. Review the Summary, and then click **Create**. Windows Setup runs and then returns to the HPCA Windows Native Install Packager.
19. When the HPCA Windows Native Install Packager is done, a message prompts you to reboot using the Linux CD-ROM/DVD. This refers to the Image Capture media.

    > **Note:** Remember the boot order must be set to boot from the CD-ROM/DVD first.

20. Insert the Image Capture media, and then click **OK**.
21. Click **Finish**.

22. Reboot the device, and the image is uploaded the *<InstallDir>*`\Data\OSManagerServer\upload` directory.
23. When a message appears that the OS Image has been successfully sent to the RCA Server, you can remove the media from the drive and reboot your device.

Publishing and Deploying OS Images

After you have captured an image, use the Publisher to publish it to the RCA database. For instructions, see "Publishing" on page 387.

When you have published the image, refresh the OS Library to view the list of available OS images. Use the RCA Console toolbar to deploy the image to selected devices.

Appendix G

Building a Custom Windows PE Service OS

This chapter includes the following topics:

About the Custom Build Script

It provides a script that enables you to:

- Add font support for Chinese and Japanese.
- Update the Windows Preinstallation Environment (PE) Service OS when a new `winpe.wim` file is made available through an updated Windows Automated Installation Kit (AIK).
- Add extra drivers or packages that do not exist in the Windows PE Service OS provided.
- Use the information in this chapter in conjunction with your knowledge of the Microsoft Windows AIK to rebuild the Windows PE Service OS with the drivers and packages necessary for your environment.
- Create a new `ImageCapture.iso` if you have updates that need to be applied, such as a change to the default Service OS or to the configuration of the boot menu.
- Create a new `ImageDeploy.iso` if you have updates that need to be applied such as a change to the default Service OS or to the configuration of the boot menu.

Prerequisites

Before you can use the script provided by HP to build a custom Windows PE Service OS, you must satisfy a number of prerequisites. See the following topics for details:

Caution: Do not attempt to run this script on a machine where incompatible software is installed. See the prerequisites for the "Administrator Machine" below.

Process Knowledge

You will need a basic understanding of Microsoft's preinstallation customization process to add drivers and other information to the Windows PE Service OS.

Administrator Machine

To run the script, you will need an “administrator” machine with the 32-bit version of the Windows Automated Installation Kit (AIK) installed. This is the machine that you will use to build the customized Windows PE Service OS.

Caution: Do NOT use a machine where any of the following are installed:

- RCA Boot Server
- RCA Core or Satellite server
- Cygwin

Note that with RCA 8.1, we have updated Windows AIK to version 3.1. This is a supplement over Windows AIK 3.0 installation. The supported Operating Systems are:

- Windows 7 Service Pack 1
- Windows Server 2008 R2 SP1
- Windows Server 2003 with Service Pack 2
- Windows Vista SP1
- Windows Server 2008 family
- Windows 7 family
- Windows Server 2008 R2 family.

Note: Be sure to download and install the 32-bit version of the Windows AIK.

Media

You will need the following media (DVD or CD-ROM):

- HPCA product media
- HPCA Image Capture media
- HPCA Image Deploy media

Files and Directories

- You will need the build scripts bundle, `build_scripts.zip`, from the RCA product media.
- If you are generating a new `ImageCapture.iso` or `ImageDeploy.iso`, you must do the following to include the updated files required.
  a. Create a build items directory on the "Administrator Machine" on previous page, such as `c:\build_items`.
  b. *Optional*: Copy any updated files that you have received from it to this build items directory. Create subdirectories as needed, based on the structure of the Image Capture or Image Deploy media.
  If any of the required files are not in this directory, you will be prompted to insert the previous Image Capture or Image Deploy media so the files can be copied.
  c. *Optional:* Include `rombl_capture.cfg` and `rombl_deploy.cfg` in the build items directory for use on the appropriate ISO. These files contain information such as the menu timeout settings and the default Service OS.
  To create these files, copy `rombl.cfg` from the previous `ImageCapture.iso` or `ImageDeploy.iso`, and modify and rename the files as necessary.

  If you do not include these files in the build items directory, the script prompts you for the previous CD-ROM and retrieves the files from the media. If you choose not to insert a CD-ROM, a standard `rombl.cfg` file will be created automatically.

Support for Other Languages

If you want to add support for Chinese or Japanese without making additional changes to the ISO:

- Remove any existing `winpe.wim` files from the `build_items` directory.
- Copy `winpe_cjk.wim` from the `\custom_build\lang_support` directory on the product CD-ROM to the build_items directory.
- Rename `winpe_cjk.wim` to `winpe.wim`.
- See "Building a Custom Windows PE Service OS" on next page to run the script.

  Caution: To use the Chinese or Japanese enabled `winpe.wim` file without rebuilding the `winpe.wim` file, be sure to type `N` when prompted to recreate the `winpe.wim` file.

- If you are using the ImageDeploy CD to install from CD—or you are installing from a cache and want messages to appear in your local language—copy the `\custom_build\lang_support\i18n` directory from the product media to the build items directory. You may remove the `.msg` files that are not needed for your local language.

Advanced Option

Caution: The following information is intended for experienced RCA administrators only. Do not attempt to customize an existing `winpe.wim` file unless you have a strong understanding of both OS Management under RCA and the Microsoft Windows AIK tools.

If you are using a pre-existing `winpe.wim` file:

- It is strongly recommended that the pre-existing `winpe.wim` was built using the same version of the Windows AIK that is installed on the machine where you are executing the build scripts.
- The `winpe.wim` file must have the following packages installed:
  - For Windows AIK version 1.1
    - `WinPE-HTA-Package`
    - `WinPE-Scripting-Package`
    - `WinPE-XML-Package`
    - `WinPE-WMI Package`
  - For Windows AIK version 2.0 and 3.1:
    - `WinPE-hta.cab`
    - `WinPE-scripting.cab`
    - `WinPE-wmi.cab`
    - `WinPE-setup.cab`
    - `WinPE-legacysetup.cab`
    - `WinPE-setup-client.cab`
    - `WinPE-setup-server.cab`
- If your `winpe.wim` file was prepared using the `peimg /prep` command, see the Microsoft documentation for the Windows AIK, peimg, and ImageX for restrictions (only applies to Windows AIK 1.1).

Adding Drivers to the Windows PE Service OS

You can add drivers to the Windows PE Service OS when you run the build scripts. For example, if you have a driver that requires a reboot, you must do it in "offline" mode. This means that the build script will pause, and you can make any necessary changes at that time. This is described in detail in the steps below.

Note: Additionally, you can add drivers to Windows PE while it is running ("online" mode). The drivers must be fully contained without need for a reboot, and the device must have connectivity to the RCA server.

During the startup of the Windows PE Service OS, any drivers that exist in *<InstallDir>*`\OSManagerServer\SOS\WinPE\drivers` will be downloaded and installed using `drvload.exe`.

Building a Custom Windows PE Service OS

The following topics show you how to obtain and use the script that RCA provides to build a custom Windows PE Service OS.

- To obtain the script and prepare to run it, see "Get the Script" below.
- To launch the script and specify the information that it requires, see "Run the Script" below.

  Note: Be sure to review and satisfy the "Prerequisites" on page 483 before you invoke the script.

- After you run the script, see "Additional Information" on page 490.

Get the Script

The script that you will need to build a custom Windows PE Service OS is located on the RCA installation media. Follow the procedure below to obtain the script and prepare to run it on your "Administrator Machine" on page 484.

To obtain the script and make it available on the Administrator Machine

1. Copy the following file from the installation media to a location on the "Administrator Machine" on page 484 (where the Windows AIK is installed).:
   <InstallDir>`\media\ISO\roms\build_scripts.zip`
2. Unzip this file to a directory of your choice (such as `C:\Build_scripts`).

Run the Script

Note: This procedure assumes that you have satisfied the prerequisites (see "Prerequisites" on page 483) and obtained the script (see "Get the Script" above).

For each question that the script asks, the default response is shown in brackets on the far right side of the window. For example:

```
Type a number between 1 and 9 [1]:
```

In this example, the default response is 1. To accept the default, press **Enter**.

Building a custom Windows PE Service OS

1. Go to a Windows command prompt, and change to the *<version>* folder in the directory that you just created.
   Here, *<version>* is the SOS version number. For example:

   `C:\ Build_scripts\`*<version>*
2. Type **run**
   In a few moments, a list of HPCA versions is displayed.
3. Type the number corresponding to the HPCA version that you want to use.
4. When asked whether you want to create a new WIM file, type `Y` or `N`.

   Note: If the script that you are running was provided with an OS management service OS

update (driver patch), you cannot create a WIM file. You can only create ISO files.

If you typed `Y`, follow these steps to specify the WIM file options:

a. You will be prompted to type the path to your Windows AIK tools directory. For example, `C:\Program Files\Windows AIK\Tools`

b. When asked whether you want to use the `winpe.wim` file from the Microsoft Windows AIK, type `Y` or `N`.

> **Note:** It is strongly recommended that you use the `winpe.wim` file from the Microsoft Windows AIK.
>
> If you type `N`, you will be reminded to ensure that your pre-existing `winpe.wim` file is built according to specifications. Then, you will be prompted to specify the fully qualified path of the pre-existing `winpe.wim` file.

c. When asked whether you want to include font support for Chinese, and Japanese, type `Y` or `N`.

d. When asked whether you want to pause the WIM creation process to add extra drivers or packages, type `Y` or `N`.

e. When asked whether you want to provide a path to a directory containing additional drivers to be added during the WIM creation process, type `Y` or `N`.

f. If you typed `Y`, you will be asked to type the fully qualified path to the directory containing the drivers.

5. The next group of questions determines whether you want to create a new Image Capture ISO or Image Deploy ISO and which Service OS to include.
   - You should create a new Image Capture ISO (type `Y`) if any of the following conditions are true:
     - You have received updated files from Persistent Software Support.
     - You have rebuilt `winpe.wim`, and you are using the ISO to perform the capture.
     - You need to change the configuration (`rombl.cfg`).
   - You should create a new Image Deploy ISO (type `Y`) if any of the following conditions are true:
     - You have received updated files from HP Software Support.
     - You have rebuilt `winpe.wim`, and you are booting from the CD during deployment.
     - You need to change the configuration (`rombl.cfg`).

   Follow these steps to specify the ISO options:

   a. When asked whether you want to create a new Image Capture ISO, type `Y` or `N`.

   b. When asked whether you want to create a new Image Deploy ISO, type `Y` or `N`.

   c. If you answered `Y` to question, you will be asked which Service OSs to include on the ISO. Type the appropriate selection. Then, press **Enter**.

d. When asked if you want to create a new `rombl.cfg` or use a pre-existing `rombl.cfg` file, choose one of the following actions:
   - To create a new `rombl.cfg` file, type `1`, and press **Enter**.
   - To use a pre-existing `rombl.cfg` file and skip to the next step, type `2`, press **Enter**.

e. When asked which Service OS you want to boot by default, type the appropriate selection. Then, press **Enter**.

f. Specify how the boot menu should be handled in each ISO that you are creating. There are three choices:

`0`	Hide the boot menu from the user of the target device. The default service OS that you specified in steps above will be used.
`-1`	Show the boot menu, and wait for a user response. The response will override the default Service OS setting.
`Number greater than zero`	Show the boot menu, and wait this number of seconds for a user response before booting into the default service OS specified in the step "Building a custom Windows PE Service OS" on page 487.

g. When asked if you want to change the port used to connect to the HPCA infrastructure, type `Y` or `N`. The default port is 3466.

h. When asked if want to specify the ISO boot load value that gets included in the ISO boot sector, type `Y` or `N`.

> **Caution:** Use this option only if you experience problems using the default value and you have been instructed by HP Software Support to change it.

Certain hardware models require a boot load segment of 0x2000 because of a BIOS issue. Other models cannot boot from the CD when the boot load segment is something other than the default loader segment of the El Torito ISO format: 0x0000.

To specify the boot load segment setting, type `1`, `2` or `3`:

1	HPCA default (0x2000) – works with most BIOSs
2	ISO default (0x0000) – gets translated to 0x07c0 by most BIOSs
3	Manually type a value

Then press **Enter**. If you typed `3`, specify the boot load segment setting as a hexadecimal string beginning with 0x.

i. When prompted for the fully qualified path to the build items, type the directory name (such as `C:\build_items`), and press **Enter**.

This completes the questions pertaining to the Image Capture and Image Deploy ISOs.

6. When prompted for the fully qualified path for the temporary work directory, type a directory name (such as `C:\build_work`). This directory will be referred to as the <*work-dir*> in later steps.

> **Note:** If the directory already exists and has information in it, you will be asked whether you want to delete the information or not. If you choose No, you will be asked to type a directory again. If you prefer to exit, press **Ctrl + C** to exit the process. If you choose Yes, the information will be overwritten.

7. When prompted for the fully qualified path for the output directory, type a directory name such as (`C:\build_output`).

   > **Note:** If you are prompted to create ISOs for CAS, type `N`.

8. The build process takes some time, as you will see from the on-screen messaging. When it is finished, you will see a message indicating that the Service OS creation process completed successfully and be returned to a command prompt.

After the build is completed, go to the directory where the `Windows PE.wim` was stored, such as `C:\WinPE_output`, and perform the following action:

Boot Method for Target Devices	Action Required
PXE	Copy `winpe.wim` from the output directory to *<InstallDir>*`\BootServer\X86PC\UNDI\boot`
LSB	Use the CSDB Editor to replace `winpe.wim` in the LSB package.
CD	Create a new ISO using the Windows PE scripts.

If you chose to create `ImageCapture.iso` or `ImageDeploy.iso`, they will be stored in the same output directory.

Additional Information

After you provide all the information that the custom Windows PE service OS build script requires, the following things happen:

1. If files that are required to build the ISO are not in the build items directory, you must insert the CD/DVD, and the files will be copied. If you choose not to insert the CD/DVD, the build process will terminate.
2. The information that you entered is saved, and the Windows PE directory creation begins.
3. If you indicated that you wanted to pause the WIM creation process to add extra drivers or packages, the process will pause after the Windows PE directory is created and the contents of `winpe.wim` are extracted into the WIM directory (for example, `C:\build_work\WIM`). There are two ways to do this:
   Method A: Use a Windows AIK tools to make your modifications.

   If you are using Windows AIK version 1.1, use the `peimg.exe` command. The default location of this executable file is:

   `C:\Program Files\Windows AIK\Tools\PETools\peimg.exe`

If you are using Windows AIK version 2.0 or 3.1, use the `dism.exe` command. The default location of this executable file is:

```
C:\Program Files\Windows AIK\Tools\Servicing\dism.exe
```

See the Windows AIK documentation for information about how to use these commands (or use the `/help` command line option).

Method B: Add the drivers to a driver list.

After you see a message indicating that all required information is gathered, the `build.config` file will be created in the `C:\ Build_scripts` directory to store the information that is needed to build the `winpe.wim` and the ISOs. You can use a text editor to open this file and add the appropriate drivers below the empty `DRIVERS` list.

For example:

```
declare DRIVERS = " cdrom.inf \
 e:\\tmp\\work\\WIM\\windows\\inf\\adp94xx.inf \
 e:\\tmp\\work\\WIM\\windows\\inf\\3com*.inf "
```

Note: Because the back-slash (`\`) is a special character, you must "escape" it by using two back-slashes, as shown in this example.

Note that all lines except the last end with a back-slash. In this case, the back-slash indicates a continuation of the declaration.

If you do not specify a directory, the script will search for the driver in the <*work-dir*>`\WIM\Windows\inf` directory.

If you prefer, you can provide a fully qualified path that specifies the location and driver, such as `c:\\anydirectory\\mydrivers.inf`

You can also specify a path with a filename containing a wild card, such as `c:\\anydirectory\\md*.inf`, which will install all `md*.inf` files found in `c:\anydirectory`.

After you are finished, type **run** to continue, and the drivers will be added to `winpe.wim`.

If you run the script again in the future, you will be prompted about whether you want to keep the `build.config` file or replace it with a new one. Also, the script will pause automatically. If you do not have additional packages or drivers to add, simply type **run** to continue.

Using Customized build.config Files (Advanced Option)

If you choose, you can take an existing `build.config` file and save it with another name. You may want to do this if you need to maintain various sets of configurations, or if you are testing based on an existing configuration. You can add drivers to the file as specified above.

Place the file in the directory where you unzipped the `build_scripts.zip` file, such as `C:\build_scripts`.

When you run the script, instead of typing `run` use the following command:

```
run.cmd -f mybuild.cfg
```

If you do not include the `-f` parameter, the default `build.config` file will be created and used.

Appendix H

Configuring a Full-Service Satellite for SQL Data Injection

By default, only the Core server is configured to inject messaging data to the ODBC reporting database for the RCA enterprise. The full-service Satellite servers forward all messaging data to the Core server for posting to the RDBMS. This results in potential bottlenecks for messaging at the Core server and creates major dependencies on the Core server. To provide failover capabilities and load distribution, multiple Messaging servers can be configured to inject data concurrently to the RDBMS.

You can configure RCA full-service Satellite server to enable direct posting to the SQL/Oracle reporting database using the HP-supplied settings template or by manually configuring the `.cfg` files.

Satellite Direct Injection Settings Template

HP provides a settings template that you can customize and deploy to your Satellite servers to automatically implement the direct injection feature.

Complete the following tasks to deploy the Satellite Direct Injection template to the Satellite servers in your environment.

Download the HPCA Satellite Direct Injection template

1. Log on to the HP Live Network using the following URL: https://hpln.hp.com/. The HPLN Portal web page opens.
2. In the Products tab, click **Client Automation**. The Client Automation web page opens that provides the details on the content available on the HP Live Network.
3. In the Client Automation area, click **CONTENT**.
4. In the Community column, click **Application Management Profiles for Client Automation**.
5. In the Application Management Profiles for Client Automation area, click **Content**. The Application Management Profiles for Client Automation - Content area is updated with the list of downloadable items available on the HP Live Network.
6. Expand **AMPs - HP Contributed**, click **Solutions**, and then click `HPCA Satellite Direct Injection.zip`. The File Download window appears. Save this zip file to the location where the HP Live Network Connector downloads content.

Update the HP Live Network content manually

1. Log on to the Radia Client Automation Core Console.
2. Click **Operations** tab.

3. Expand **Infrastructure Management** in the left pane, and then click **Live Network**. The Live Network section appears in the right pane.
4. Click **Update Now** tab.
5. In the HP Live Network Immediate Update area, click **From the File System** and provide the path for the HPCA Satellite Direct Injection zip file that you downloaded and saved in Task 1.
6. Click **Update Now**.

Configure the <HPCA Satellite Direct Injection> profile

After you update the HP Live Network, the profile <HPCA Satellite Direct Injection> is available under the Settings Templates. In this template, specify the SQL/Oracle reporting database details where the Satellite servers should directly inject the data.

1. On the Operations tab, expand Settings Management in the left navigation pane and click **Settings Templates**.
2. In the Display Name column, click **<HPCA Satellite Direct Injection>** profile. The <HPCA Satellite Direct Injection> window opens with the Profiles and Details tabs.
3. Click **<HPCA SAT DIRECT INJECTION>** to edit the profile properties. The <HPCA SAT DIRECT INJECTION> window opens with the Summary and Properties tabs.
4. Click the **Properties** tab and provide the following details under the Parameters area:
   - DSN: Enter the DSN for the SQL/Oracle reporting
   - User Name: Enter the user name for the DSN
   - Password: Enter the password for the ODBC user name
5. Click **Save** to save your changes.

You can deploy this profile on all the Satellites in your environment.

Manually Configuring the Satellite Servers

You can also perform the following steps manually to configure RCA full-service Satellite server to enable direct posting to the SQL/Oracle reporting database.

1. Install ODBC DSNs (type SYSTEM) on the full-service Satellite for RCA matching the names defined on the Core server (for Inventory and PATCH databases).
2. Stop the Messaging Server service on each Satellite server and delete the log files.
3. Open the `RMS.cfg` file and add the following section after the line "
   ```
   proc ServerType { } { return "satellite" }":
   proc ServerType { } { return "satellite" }
   ```

   ```
   #Add the following section( between" proc ServerType { } { return
   "satellite" } and atexit add log.flush" )
   ```

   ```
   proc ServerEnabled { mode } { return [string match -nocase $mode
   [ServerType]] }
   ```

   ```
   proc ForwardEnabled { option } {
   ```

```
#Compatibility for auto-selection based on server type, forward is
only available on SATELLITE

if {[string equal -nocase $option "auto"]} {

return [string equal -nocase [ServerType] "satellite"]

}

# Additional option processing

if {[string equal -nocase $option "upstream"] || [string equal -
nocase $option "both"]} {

return true

}

return false

}

proc LocalEnabled { option } {

#Compatibility for auto-selection based on server type, local is
only available on CORE

if {[string equal -nocase $option "auto"]} {

 return [string equal -nocase [ServerType] "core"]

}

# Additional option processing

if {[string equal -nocase $option "local"] || [string equal -nocase
$option "both"]} {

 return true

}

return false

}
```

4. Modify the `Overrides Config` section as follows:

```
Overrides Config {

CORE.ODBC local

PATCH.ODBC local

USAGE.ODBC core

RMP auto

DTM auto

OPE none

DIAG none

USAGE satellite
```

```
RRS core

}
```

5. Delete the following section:
   ```
   if { [ServerType] != "core" } {

   #-------------------------------------------------------------

   # Satellite RMS Configuration - forward everything

   #-------------------------------------------------------------

   msg::router::add router {

   TO *

   USE forward

   }

   }
   ```
6. Replace `serverEnabled` with `LocalEnabled` in the `DIAG` section as follows:
   ```
   if { [ServerEnabled $Config(DIAG)] } {
   ```
   with
   ```
   if { [LocalEnabled $Config(DIAG)] } {
   ```
7. Add the `ForwardEnabled` section in the DIAG section as follows:
   ```
   if { [ForwardEnabled $Config(DIAG)] } {

   #-------------------------------------------------------------

   # Forwarding Upstream

   #-------------------------------------------------------------

   msg::router::add router {

   TO *

   USE forward

   }

   }
   ```
8. Replace `serverEnabled` with `LocalEnabled` in the RMP section as follows:
   ```
   if { [ServerEnabled $Config(RMP)] } {
   ```
   with
   ```
   if { [LocalEnabled $Config(RMP)] } {
   ```
9. Add the `ForwardEnabled` section to the RMP section as follows:
   ```
   if { [ForwardEnabled $Config(RMP)] } {

   #-------------------------------------------------------------

   # Forwarding Upstream

   #-------------------------------------------------------------
   ```

```
msg::router::add router {

TO CORE.RMP

USE forward

}

}
```

10. Replace `serverEnabled` to `LocalEnabled` in the DTM section as follows:
    `if { [ServerEnabled $Config(DTM)] } {`

    with

    `if { [LocalEnabled $Config(DTM)] } {`

11. Add the `ForwardEnabled` section in the DTM section as follows:

```
if { [ForwardEnabled $Config(DTM)] } {

#-------------------------------------------------------------

# Forwarding Upstream

#-------------------------------------------------------------

msg::router::add router {

TO DTM

USE forward

}

}
```

12. Replace `serverEnabled` with `LocalEnabled` in the OPE section as follows.
    `if { [ServerEnabled $Config(OPE)] } {`

    with

    `if { [LocalEnabled $Config(OPE)] } {`

13. Add the `ForwardEnabled` section in the OPE section as follows:

```
if { [ForwardEnabled $Config(OPE)] && ![ForwardEnabled
$Config(RMP)] } {

#-------------------------------------------------------------

# Forwarding Upstream

#-------------------------------------------------------------

msg::router::add router {

TO CORE.RMP

USE forward

}

}
```

14. Replace `serverEnabled` to `LocalEnabled` in the `CORE.ODBC` section as follows:
    ```
    if { [ServerEnabled $Config(CORE.ODBC)] } {
    ```
    with
    ```
    if { [LocalEnabled $Config(CORE.ODBC)] } {
    ```
15. Add the `ForwardEnabled` section to the `CORE.ODBC` section as follows:
    ```
    if { [ForwardEnabled $Config(CORE.ODBC)] } {

    #-------------------------------------------------------------

    # Forwarding Upstream

    #-------------------------------------------------------------

    msg::router::add router {

    TO {CORE.RIM CORE.ODBC WBEM.ODBC INVENTORY.ODBC SECURITY VM}

    USE forward

    }

    }
    ```
16. Replace `serverEnabled` with `LocalEnabled` for `PATCH.ODBC` section as follows:
    ```
    if { [ServerEnabled $Config(PATCH.ODBC)] } {
    ```
    with
    ```
    if { [LocalEnabled $Config(PATCH.ODBC)] } {
    ```
17. Add the `ForwardEnabled` section to the `PATCH.ODBC` section as follows:
    ```
    if { [ForwardEnabled $Config(PATCH.ODBC)] } {

    #-------------------------------------------------------------

    # Forwarding Upstream

    #-------------------------------------------------------------

    msg::router::add router {

    TO {PATCH PATCH5}

    USE forward

    }

    }
    ```
18. Add your DSN information created in step 1 in the `Core.DDA.cfg` file as follows:
    ```
    msg::register core.odbc {

    TYPE SQL

    DSN "Core_Prod"

    SERVER ""

    USER "hpcacore_prod"

    PASS "{AES256}UtmWvG+rnMl//K+bSCpbdg=="
    ```

```
USE ""
AUTOCOMMIT off
DSN_DELAY 30
DSN_PING 120
ENABLE-CORE true
ENABLE-WBEM true
ENABLE-INVENTORY true
ENABLE-VM true
AUTOCREATE true
AUTOLOAD true
STARTUPLOAD true
REJECTS rejects
}
```

19. Apply the DSN information in `PATCH.DDA.cfg` file.

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: User Guide

Feedback: