HP OpenView Management Portal Using Radia

Radia Management Portal Guide

Software Version: 2.0.1

for the Windows operating system

Manufacturing Part Number: T3424-90042

February 2005

Legal Notices

Warranty

Hewlett-Packard makes no warranty of any kind with regard to this document, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. Hewlett-Packard shall not be held liable for errors contained herein or direct, indirect, special, incidental or consequential damages in connection with the furnishing, performance, or use of this material.

A copy of the specific warranty terms applicable to your Hewlett-Packard product can be obtained from your local Sales and Service Office.

Restricted Rights Legend

Use, duplication, or disclosure by the U.S. Government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause in DFARS 252.227-7013.

Hewlett-Packard Company
United States of America

Rights for non-DOD U.S. Government Departments and Agencies are as set forth in FAR 52.227-19(c)(1,2).

Copyright Notices

Trademark Notices

Linux is a registered trademark of Linus Torvalds.

OpenLDAP is a registered trademark of the OpenLDAP Foundation.

Acknowledgements

PREBOOT EXECUTION ENVIRONMENT (PXE) SERVER
Copyright © 1996-1999 Intel Corporation.

TFTP SERVER
Copyright © 1983, 1993
The Regents of the University of California.

Technical Support

Please select Support & Services from the following web site:

<http://www.hp.com/managementsoftware/services>

There you will find contact information and details about the products, services, and support that HP OpenView offers.

The support site includes:

- Downloadable documentation
- Troubleshooting information
- Patches and updates
- Problem reporting
- Training information
- Support program information

About this Guide

Who this Guide is for

This Radia Management Portal Guide for version 2.0 is the first verson to introduce Radia Management Portal Z*ones*, and the related features that accommodate very large enterprises that require multiple Radia Management Portal sites. This version of the Radia Management Portal offers access to directory structures that already exist in your enterprise, including the Radia Database on the Radia Configuration Server, an external policy store, and your enterprise networks.

Using Radia Management Portal 2.0, Radia Administrators can:

- Use one of the self-managed, cross reference groups to perform an operation on all devices that have the same hardware, operating system level, managed service, or Radia Infrastructure on them. For example, Administrators can Notify all Windows XP Servers of an update.

- Centrally schedule and manage jobs on any Radia Management Portal Zone from a single, master portal.

- Define and connect to non-Radia Management Portal directories in your enterprise, such as Microsoft Active Directory, and network directories, such as Microsoft Windows Network.

- Connect to a Radia Database on the Radia Configuration Server and perform instance-level tasks on your enterprise distribution model.

- Connect to any LDAP Directory Service being used with Radia Policy Manager, such as Active Directory, and use Policy tasks in the Radia Management Portal to administer policy for Radia services.

To use the features relating to the Radia Database, RCS Administration, and Policy Administration, you should have a comprehensive understanding of the Radia Configuration Server, Radia Database administration, the Policy Server, and assigning Policy.

What this Guide is about

The *Radia Management Portal 2.0 New Features Guide* describes:

- The new zone-based architecture and Radia Management Portal directory structure.
- How to install the Radia Management Portal 2.0 for Windows. After installing the first RMP zone, you can use the **Install RMP** task to install additional Radia Management Portal zones remotely.
- The user interface and navigational changes.
- The new tasks and task groups that have been added for this release, including:
  - Help Desk Notify
  - Device Management, Grouping, and Import Tasks
  - Radia Management Portal Zone Configuration Tasks
  - RCS Administration Tasks
  - Software and Service Administration Tasks
  - Policy Administration Tasks
- How to create and use Zone Access Points to connect to and browse existing LDAP directory services in your network.
- The various ways of adding devices to your RMP zone, bringing them under RMP management, and establishing device Groups.
- The tasks that you can use in the Radia Management Portal to schedule and sequence jobs across all Radia Management Portal zones in your infrastructure.
- How to add and use multiple profiles for the Install Client task.
- How to add and use modified rps.cfg files to install pre-configured Radia Proxy Servers in your enterprise.

Summary of Changes

The RMP 2.0 features and documentation changes from the 1.x release are extensive.

2.0.1 This icon indicates features or documentation changes related to the RMP 2.0 Service Pack 1.

New Topics

2.0 Table P.1 lists the topics that are new for Radia Management Portal 2.0.

Table P.1 ~ New Topics for RMP 2.0	
Chapter	**Page and Topic**
1. Introduction	Page 25, What is a Zone? Page 25, The Zone Directory Structure Page 26, About Object Names in a Zone
2. Installing the Radia Management Portal	Page 32, Radia Prerequisites Page 33, Directory Size of a Single Zone Page 49, Updating RMP Zones with a New Build
3. Using the Radia Management Portal	Page 68, Navigation Modes: History and Location Page 69, Sample Navigation Session: Viewing Network Objects Page 71, Accessing and Returning to Your Desktop Page 74, Removing Shortcuts from Your Desktop Page 76, Navigating the Portal Directory and the Zone Containers Page 84, Infrastructure Task Group Page 91, Policy (Advanced) Task Group Page 91, Policy Task Group Page 92, RCS Administration Task Group Page 93, Toolbar Tasks Page 96, Radia Directory and Zone Objects Page 97, About the Zone Containers Page 102, Using the RCS Administration Tasks Page 111, Using RMP to Assign Policy through an LDAP Directory Page 118, Resolving Policy Page 123, Customizing Domain Filters (DNAMEs) in the Resolve Policy Task
4. Administrative Functions	Page 142, Setting Additional Configuration Parameters Page 143, Configuring Directory Services Page 159, Configuring for External LDAP Authentication Page 165, Configuring for a Custom LDAP Policy Extension Prefix Page 165, Establishing Devices and Device Groups Page 166, Basic Procedures for Modifying Groups Page 182, Adding a Single Device Page 189, Adding Groups Page 191, Adding Devices to a New Group Page 195, Moving or Copying Devices into a Group Page 201, Removing Groups of Devices Page 202, Importing Devices

Removed Topics

■ The *Novadigm Services* chapter was removed.

Chapter 2:
Installing the Radia Management Portal

2.0.1 Page 48, *Updating Tasks*, modified steps to accommodate selective task updates, and added the following caution: "HP recommends that you do **not** update a task that has been intentionally customized, such as a Notify task. Doing so will overwrite any customizations. The unaccepted task changes remain available for update at a later time."

2.0.1 Page 49, *Updating RMP Zones with a New Build*, new topic explains how to update the Master and Subordinate Zones in your enterprise with a new build.

2.0.1 Page 59, *Changing Passwords*, Step 5: inserted text to define new password support:

"Passwords may include alphanumeric characters as well as spaces and special characters, such as #, $, and \."

Chapter 3:
Using the Radia Management Portal

2.0 All procedures have been modified to show the new starting point and navigation path needed to perform the tasks.

Page 82, *Taskbar and Task Summary*: use the hyperlinks within a task description to quickly locate the procedure for that task.

2.0 Page 82, *Taskbar and Task Summary*: identifies all new task groups and tasks for this release with a **2.0** bullet or a **2.0.1** bullet.

2.0 Page 84, *Model Administration Task Group*: the following tasks have been removed from the **Model Administration** Task Group: Add Container, Add Organization, Add Groups of Devices, Move Device.

The previous **Inventory Management Task Group** and **Notify via Inventory** task have been removed. See the *Radia Reporting Guide* for alternative methods of notifying device groups from inventory reports.

2.0 Page 87, Operations Task Group: the following tasks have been removed from the **Operations** Task Group: **Notify by Audience** and **Notify by Subscription**. These tasks are no longer necessary because of the ability to use the Notify command with the audience groups that are automatically created and maintained in the Cross References container. For details, see *Notifying an Audience* on page 291.

2.0.1 Page 87, Operations Task Group: added **Update RMP** task which allows you to apply a new version of the Radia Management Portal to the subordinate Zones in your enterprise. For procedures, see *Updating Subordinate RMP Zones* on page 349.

2.0.1 Page 89, *Operations Task Group*, added a new task, **Update RMP**.

2.0.1 Page 90, Policy Task Group: added **Resolve Policy** task definition (Figure updated). For procedures, see *Resolving Policy* on page 118.

2.0.1 Page 99, *Cross-References (cn=xref) Self Managed,* added Subnets Container.

2.0.1 Page 118*, Resolving Policy*, this task allows you to view the resulting policies for a selected object. For objects in an LDAP directory, you can also limit the resolution to a specific domain filter as defined in your Policy configuration (DNAME), and insert values for host, operating system, UserID, Zcontext, or another attribute normally available to the LDAP Policy Adaptor at resolution time.

Procedures for configuring *Customizing Domain Filters (DNAMEs) in the Resolve Policy Task* begin on page 123.

Chapter 4:
Administrative Functions

2.0.1 Page 145, *Specifying LDAP Directory Service Properties*, modified the definitions for **Common Name** and **Use** in *Table 4.4 ~ Directory Service Properties for Type = ds-ldap*.

■ Page 148, *Table 4.5 ~ Directory Service Properties for Type = ds-rcs,* added information for Common Name and DS Prefix.

■ Page 161, *Modifying the Default LDAP Authentication for Specific Users*, topic heading used to be "Disabling LDAP Authenticaiton for Specific Users." Modified text before Figure 4.17.

2.0.1 Page 165, *Establishing Devices and Device Groups*, you can now perform installation tasks in the Operations task group directly from a discovered Network or LDAP directory location.

2.0.1 Page 165, *Adding Devices to an RMP Zone*, devices can be automatically added to the Devices container as part of an install task.

2.0.1 Page 195, *Moving or Copying Devices into a Group*, Using any of the install tasks from the Operations task group against devices in the Network container or devices in an LDAP directory automatically creates entries for the devices in the Zone, Devices container and makes them members of the Default Group.

2.0.1 Page 232, *Adding Users*, you must specify the password associated with the External User ID if external authentication is turned on for this user.

Chapter 5:
Operations Functions

2.0.1 Page 277, *Operations Functions,* modified descriptions of the Manage Computer task and the Update RMP task.

2.0.1 Page 285, *Selecting a Starting Zone, Network, or Directory Location*, Install operations can also be started from locations in a **Zone, Network** container or from an **LDAP Directory Services** location.

■ Page 291, Notifying an Audience by Device Characteristics, removed this section.

■ Page 291, Notifying an Audience by Subscription, removed this section.

2.0.1 Page 309, *To install the Radia Management Agent*, you can select a location in your Zone, Networks container or a currently connected LDAP directory location that contains computers on which you want to install the Radia Management Agent.

2.0.1 Page 315, *To install the Radia 4.x Clients with the Radia Management Portal*, you can select a location in your Zone, Networks container or a currently connected LDAP directory location that contains computers on which you want to install the Radia Management Agent.

■ Page 327, *Discovering Radia Subscriber Information using Managed* Services, modified topic title, deleted three images, and replaced the procedure.

2.0.1 Page 329, *To install the Radia Proxy Server*, you can select a location in your Zone, Networks container or a currently connected LDAP directory location that contains computers on which you want to install the Radia Management Agent.

Conventions

You should be aware of the following conventions used in this book.

Table P.1 ~ Styles

Element	Style	Example
References	*Italic*	See the *Publishing Applications and Content* chapter in this book.
Dialog boxes and windows	**Bold**	The **Radia System Explorer Security Information** dialog box opens.
Code	Andale Mono	radia_am.exe
Selections	**Bold**	Open the **\Admin** directory on the installation CD-ROM.

Table P.2 ~ Usage

Element	Style	Example
Drives (system, mapped, CD)	Italicized placeholder	*SystemDrive*:\Program Files\Novadigm might refer to C:\Program Files\Novadigm on your computer. *CDDrive*:\client\radia_am.exe might refer to D:\client\radia_am.exe on your computer.
Files (in the Radia Database)	All uppercase	PRIMARY
Domains (in the Radia Database)	All uppercase	PRIMARY.SOFTWARE. May also be referred to as the SOFTWARE domain in the PRIMARY file.
Classes (in the Radia Database)	All uppercase	PRIMARY.SOFTWARE.ZSERVICE, May also be referred to as the ZSERVICE class in the SOFTWARE domain in the PRIMARY file.

The table below describes terms that may be used interchangeably throughout this book.

Table P.3 ~ Terminology[*]

*Depends on the context. May not always be able to substitute.

Term	May also be called
Application	software, service
Client	Radia Application Manager and/or Radia Inventory Manager
Computer	workstation, server
NOVADIGM domain	PRDMAINT domain **Note**: As of the 4.0 release of the database, the NOVADIGM domain is being renamed the PRDMAINT domain. Therefore, if you are using an earlier version, you will see the NOVADIGM domain in the database.
Radia Configuration Server	Manager, Active Component Server
Radia Database	Radia Configuration Server Database

Contents

3 Using the Radia Management Portal 63

Contents

1

Introduction

At the end of this chapter, you will:

■ Understand the benefits and core capabilities of Radia Management Portal 2.0.

■ Understand the architecture and Directory Structure of any Radia Management Portal Zone.

■ Be familiar with new terminology for this release.

■ Understand the process of adding devices to your Radia Management Portal zone and grouping them for operational purposes. Almost all Operations in RMP 2.0 are performed against device groups.

Introduction

The Radia Management Portal (RMP) is a friendly, Web-based interface that you can use to manage your entire Radia infrastructure, regardless of how small or large your enterprise. Whether you are already using Radia, or are just beginning, you can use the Radia Management Portal to view and manage your existing infrastructure, and remotely install new Radia infrastructure products and applications.

The Radia Management Portal provides the following benefits:

■ **Consistency**
A simple, consistent user experience reduces the learning curve for your administrators. When using the Radia Management Portal, administrators select tasks to manage the infrastructure. Each task follows the same general procedure. Therefore, even if an administrator's role changes, the overall procedure remains the same.

■ **Web-based administration**
Use a browser from anywhere to administer your Radia infrastructure.

■ **A single view into a complex environment**
View and manage your Radia infrastructure, applications, and policy from a single administrative environment.

■ **Role-based entitlement**
Administrators can view and manage only those objects in the infrastructure for which they are responsible.

■ **Security**
Administrators are authenticated against the Radia Management Portal Directory.

■ **Extensibility**
Access any Radia Configuration Server, Radia Database, Active Directory, or other LDAP Directory in your enterprise from within the Radia Management Portal's interface. Administer policy, services, users, and machines directly from the Portal's friendly interface.

■ **Enterprise-Wide Solutions**
Create multiple Radia Management Portal Zones, if desired, to administer the infrastructure at different sites in your enterprise. From any Radia Management Portal, you can access any Zone in your enterprise and perform operations across multiple-zones.

About the Core Capabilities

After installing the Radia Management Portal, you can perform administrative and operational tasks on any piece of your Radia infrastructure. The core capabilities of the Radia Management Portal are:

- **Network Discovery**
  The Radia Management Portal automatically discovers the objects in your networks.

- **Authentication**
  Use the Radia Management Portal Directory to authenticate administrators.

- **Delegated Administration**
  Create roles in the Radia Management Portal so that your administrators have access only to the tasks that are relevant to them and their roles.

- **Remote Installations of Radia Infrastructure Components and RMP Zones**
  Use the Radia Management Portal to install Radia infrastructure products to remote devices running Windows NT, 2000, XP and Server 2003, as well as HP-UX and Solaris. This includes the remote installation of additional Radia Management Portal *Zones* at other sites in your enterprise. Each Zone manages the infrastructure for a given site, but you can access, open, and run jobs against any Zone in your enterprise from a single Radia Management Portal.

- **Remote Infrastructure Administration**
  Use the Radia Management Portal to manage Radia Management Infrastructure products. For example, you can start or stop services on your remote devices or browse client logs from a central location.

- **Remote Radia Configuration Server and Policy Administration**
  Use the Radia Management Portal to access the Radia Database on any Radia Configuration Server in your enterprise, perform instance-level tasks, and assign and manage Policy through Active Directory.

- **Cross Referenced Device Groups**
  The Radia Management Portal captures detailed information regarding device hardware, operating system, Radia infrastructure and managed services and stores it in the Radia Management Portal Directory in self-managed cross reference groups. This simplifies notification of all devices for a given classification in a single step.

- **Notify**
  Use the Notify task to perform an action on the target devices that you select. Notify all devices of a given type in one or all zones in your enterprise.

- **Scheduling**
  Use the scheduling feature to execute and track the progress of any task.

- **Querying**
  Use the query feature to extract information from the Radia Management Portal Directory.

- **Auditing/Logging**
  Use the auditing and logging features to view information about administrators and the activities they performed within the Radia Management Portal. All audit events will be stored in the log generated by the Radia Management Portal.

About the Product Architecture

Although you will be working with the Radia Management Portal in your Web browser, you may want to be familiar with the base architecture for this product.

The Radia Management Portal is made up of the following:

■ The **Portal Run-time** is the run-time technology that integrates Radia infrastructure services. This is made up of the Radia Integration Server (RIS) and the RMP.TKD (in the Radia Integration Server's **\modules** directory).

■ The **Portal Zone Directory**, zone.mk (in the Radia Integration Server's **\etc** directory), is an LDAP directory service. When it starts, it loads the set of objects that represent a given instance of the Radia Management Portal, or *Zone*. The objects stored in the **\etc\zone** directory and loaded at startup include all the information needed to manage a given set of infrastructure at a given location:

- **Managed devices** (device.mk)

- **Device group memberships** (group.mk)

- **Cross Referenced Device Groups** (xref.mk)

- **Job Status and Job History** (job.ckpt and history.mk)

- **Users** (user.mk)

- **Configurations** for **Entitlements, Tasks,** and **Services** (entitlement.mk, task.mk, and msg.mk)

- **Networks** (dns.mk and lanmanredirector.mk)

Whether you have one or many Radia Management Portal Zones in your enterprise, all zones load the same-named set of directories at startup.

■ The **Radia Management Agent (RMA)**, installed on the remote device, performs tasks on behalf of the Radia Management Portal. See *Installing the Radia Management Agent* on page 307 for more information.

Radia Management Portal Zones Overview

Very large enterprises often find it necessary to use multiple Radia Management Portals to effectively view and manage their existing infrastructure. With multiple portal sites, it becomes desirable to be able to perform operations across all sites from one central location. This release extends the scalability of the Radia Management Portal by defining a Zone and a specific Zone Directory Structure for each Radia Management Portal in your enterprise.

What is a Zone?

A *zone* is a logical set of devices, infrastructure, and software that is represented and managed in directory services and administered by the Radia Management Portal.

A zone is created whenever the Radia Management Portal is installed, and all objects in the zone include the high-level qualifier of the zone name. The first installed zone is called the master zone and others are called subordinate zones. The properties for the Zone object, itself, include the URL information needed to access the zone.

The Zone Directory Structure

Every Radia Management Portal Zone has the same directory structure and same-named containers at the highest levels.

Figure 1.1 illustrates the Zone Directory Structure and Containers. See *About the Zone Containers* on page 97 for a description of each container and how they are used.

Figure 1.1 ~ Radia Management Portal Directory of a Zone

About Object Names in a Zone

The Radia Management Portal, itself, is a Directory Service containing objects of various object classes. Each object is assigned a Common Name (cn=*name*). The common name given to an object must be unique among all objects in that class. For example, all Zone names in your enterprise must be unique. Within a given Zone, all common names of objects of the same class must be unique. The common names of the Zone containers are pre-assigned and the same across all Zones in your enterprise.

Each entry within a zone may be identified by its location. For example, the location of the **Devices** container entry in Figure 1.1 is **cn=device,cn=Mahwah** and the location of the **PRIMARY** file on the RCS is **cn=Primary,cn=Mahwah.**

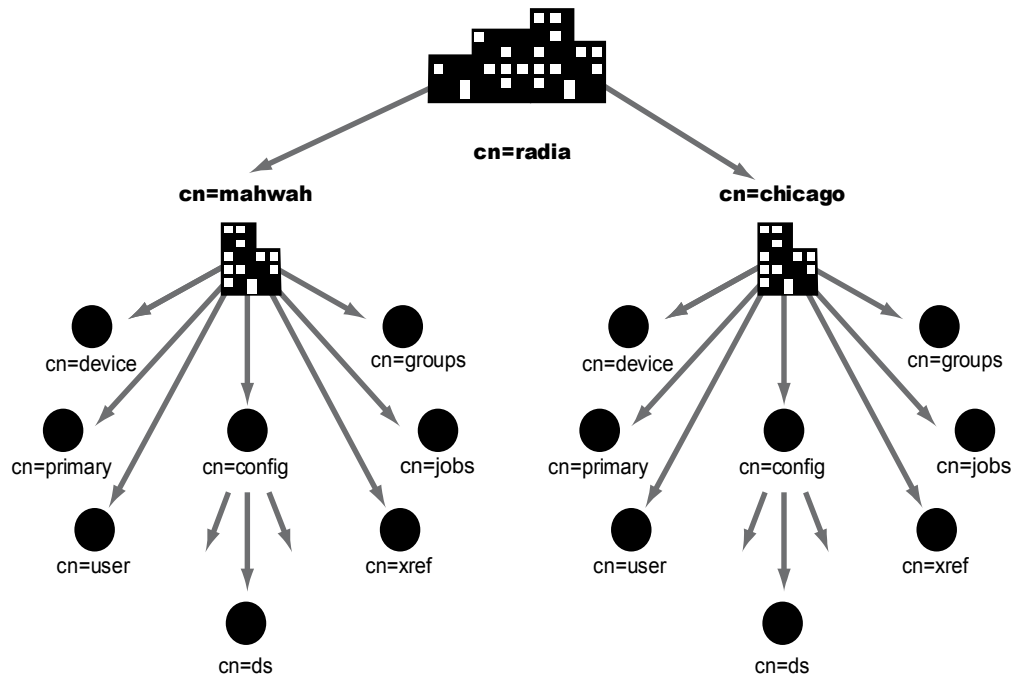*Figure 1.2 ~ Multiple Zones of the Radia Management Portal.*

This naming convention serves to ensure that distinct names exist among devices and other objects across all zones in your enterprise. For example, in Figure 1.2, the location of the **Devices** container in the Mahwah Zone is: **cn=device,cn=Mahwah,cn=radia** and the location of the **Devices** container in the Chicago Zone is **cn=device,cn=Chicago,cn=radia**.

> **Note**
>
> The Common Name for any object can be viewed by hovering the mouse over the object's icon or label in the Radia Management Portal.

The Directory Structure and naming context permit name distinction among all objects in all Zones in your enterprise. This allows the Radia Administrators to schedule operations across devices in the entire enterprise from a single, central site.

New Terminology

The following terms are new to this release. They are often used throughout this guide. It may be helpful to become familiar with them before using this guide.

For a complete Glossary of Terms, see the Glossary at the end of this guide.

Directory Service

A Directory Service in this guide refers to any of the directory service types that can be accessed from the Radia Management Portal. These include any Lightweight Directory Access Protocol (LDAP) directory, the Radia Configuration Server, DSML (allowing access to another Radia Management Portal zone), and metakit (*.MK) files. Metakit files allow access to a customized Radia Management Portal container.

A Radia Management Portal user can connect to other LDAP Directory Services (given proper authority) that have been defined in the Directory Services container.

managed device

A computer or other hardware device in your network, such as a PDA or printer, that has been added to a Radia Management Portal Zone Device container.

Mount Point

The location in a directory structure to which a connection is made. The mount point becomes the root node of the mounted directory, and thus you can only navigate to nodes at or below the mount point.

Master Zone

The initial Radia Management Portal zone installed at an enterprise. Additional Radia Management Portals are installed as subordinate zones to the Radia Management Portal Master Zone, also called the Master Portal.

Schedule Zone Operation

The Portal task used to attach a schedule and launch predefined tasks against a device Group in the selected zone or set of zones. The job finds all devices currently in the named Group in all zones that have been selected as the audience of the operation.

subordinate zone

The secondary Radia Management Portal zones installed at an enterprise, usually from the initial Radia Management Portal master zone. All zones across your enterprise must have unique names to allow for unique distinguished names for all objects across all zones in your enterprise.

Zone

A zone is a logical set of devices, infrastructure, and software that is represented and managed in directory services and administered by the Radia Management Portal.

A zone is created whenever the Radia Management Portal is installed, and all objects in the zone include the high-level qualifier of the zone name. The first installed zone is called the Master Zone and others are called Subordinate Zones. The properties of the Zone object specify the URL needed to access that zone.

Zone Access Points

The Zones Access Points container defines all Radia Management Portal zones in your enterprise. Go to the Zone Access Points container to open another zone's Radia Management Portal, as well as schedule zone operations on devices that exist in any zone in your enterprise. See *ZoneJob*.

ZoneJob

A job group scheduled for devices in a named Group across one or more Radia Management Portal zones. Scheduling a ZoneJob requires a predefined Task Template that defines the job, such as the specific notify command, and Group names in each target zone to be the same.

Summary

■ The Radia Management Portal is a Web-based interface used to manage your Radia infrastructure across your entire enterprise.

■ You can perform administrative and operational tasks on objects in your infrastructure, administer instances in the RCS database, and assign Policy using Active Directory.

■ The Radia Management Portal consists of the Portal Run-time, the Radia Management Portal Zone Directory, and the Radia Management Agent (RMA). The set of container objects in a Zone Directory are loaded at startup.

■ A *zone* is a logical set of devices, infrastructure, and software that is represented and managed in directory services and administered by the Radia Management Portal. Each Zone Directory contains the same set of containers.

■ Multiple Zones allow for management of unlimited numbers of devices at different device locations. Zone names must be unique. Object names in the same class must be unique in a zone.

■ Additional functionality is available via Radia services.

2

Installing the Radia Management Portal

At the end of this chapter, you will:

■ Be able to install the Radia Management Portal.

■ Modify the \media folders to include a \default directory for client installs.

■ Be able to log on to the Radia Management Portal.

■ Be able to change your password.

Preparing for Installation

Before installing the Radia Management Portal, locate your Hewlett-Packard license file.

If you need assistance, contact HP Technical Support (see page 4).

Assemble the following set of Radia CD-ROMs that are used during a complete Radia Management Portal install:

- Management Infrastructure CD-ROMs
- Management Applications CD-ROM
- Publications CD-ROM

Review the README file delivered with the product for the latest information.

Installing the Radia Management Portal

You can use the Radia Management Portal to view and manage your existing Windows infrastructure, add new Radia infrastructure products and applications, as well as perform service and policy administration on your Radia database, using Active Directory if needed.

This release supports environments with multiple Radia Management Portal (RMP) sites using the new *zone* architecture and features. Each Radia Management Portal site being managed from the master portal site needs to have version 2.0 installed.

Radia Prerequisites

Radia Management Portal 2.0 has been optimized to work with the REXX method ZTASKEND Version 1.8, which is installed automatically when you upgrade to Radia Configuration Server 4.5.4 SP3.

To improve the information process flow between the Radia Configuration Server and the Radia Management Portal, we recommend using the Radia Management Portal with this ZSTASKEND (version 1.8 or above) together with the Radia Messaging Server 2.0.

For details on upgrading your Radia Configuration Server to 4.5.4 SV3, see *Radia_RCS_Migrate.PDF* located in the **migrate_RCS** folder of the Radia 4 RCS media location.

For details on installing the Radia Messaging Server, see the *Radia Messaging Server Guide.*

System Requirements

- **Server**
  - Windows 2000 w/ SP3, NT, XP, Server 2003.
  - Installation of the Radia Management Portal requires Administrator authority.
- **Client**

● Any platform that supports a Web browser.

● Microsoft Internet Explorer 4.0 or higher or Netscape 4.0 or higher *with cookies enabled*.

Directory Size of a Single Zone

The **Portal Directory**, zone.mk (in the Radia Integration Server's **\etc** directory), loads all configuration and entitlement information for the Radia Management Portal as well as devices, groups, managed infrastructure, job status, network and mounted services information.

A single Radia Mangement Portal zone has an absolute limit of 10,000 devices. We recommend limiting the number of devices managed by a single zone to the following:

■ Recommended: 1,000 to 2,000 devices

■ Maximum: 5000 devices

Multiple Radia Management Portal Zones can be installed to meet the needs of enterprises of any size. To create additional zones in your enterprise, see *Installing Additional RMP Zones (Subordinate Zones)* on page 344.

Installation Procedures

ImportantNote
This version of the Radia Mangement Portal must be installed to a clean (empty) directory. Do not install it on a machine running an earlier version of the Radia Management Portal.

Use the following procedure to install the first Radia Management Portal Zone in your enterprise.

■ To install additional Radia Management Portal Zones in your enterprise, use the **Install RMP** task in the Operations task group. For details, see *Installing Additional RMP Zones (Subordinate Zones)* on page 344.

To install the Radia Management Portal 2.x

Note
Stop the service for the Radia Integration Server (httpd) if it is installed and running on the machine on which you are installing the Radia Management Portal.

On the Management Infrastructure CD-ROM, go to **extended_infrastructure \management_portal\win32** and double-click **setup.exe**.

The **Radia Management Portal Install** window opens.

Figure 2.1 ~ Radia Management Portal Welcome window.

Click **Next**.

The **End-User License Agreement** window opens for you to read the licensing terms for this product. You must accept the terms before the Radia Proxy Server can be installed.
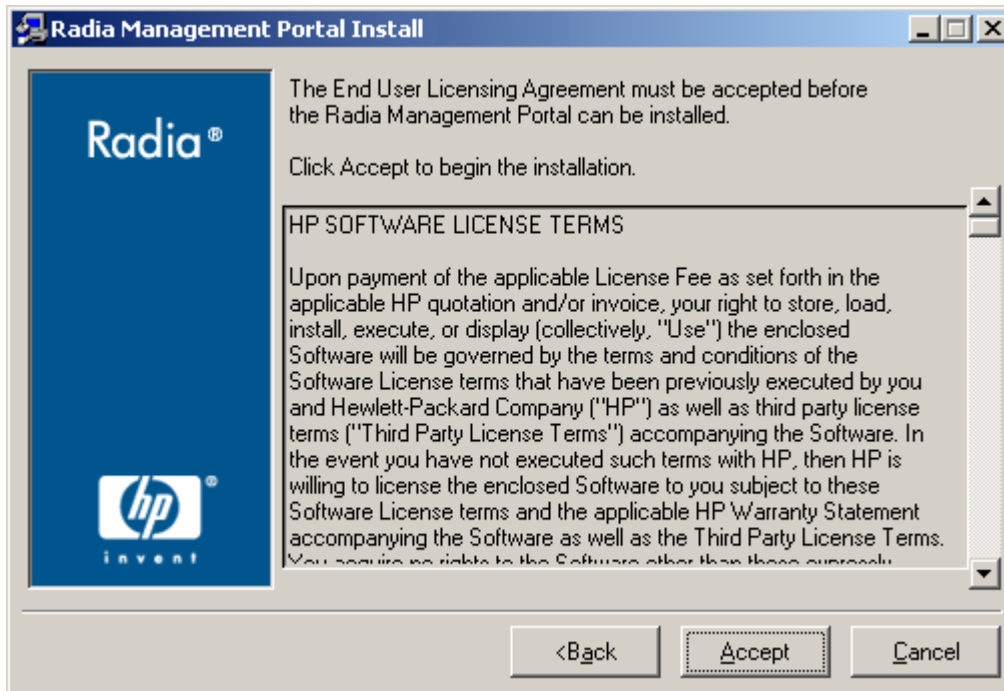
Figure 2.2 ~ End User Licensing Agreement.

Click **Accept** to agree to the terms of the software license and continue with the installation.
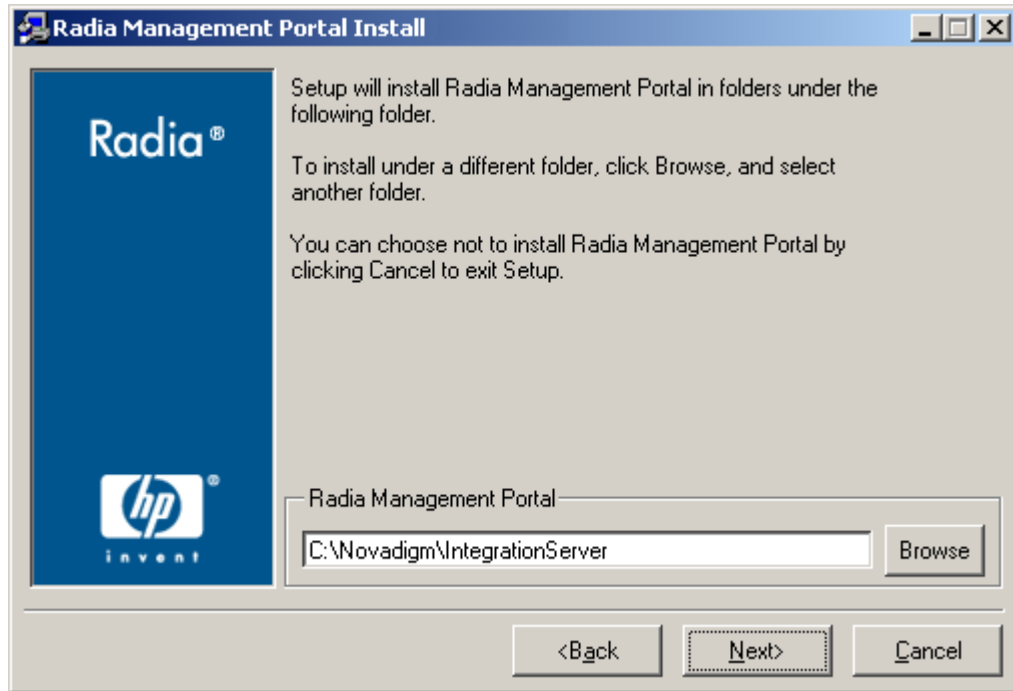
The **Radia Management Portal Location** window opens.

Figure 2.3 ~ Radia Management Portal location window.

Use this window to select the folder where you want to install the Radia Management Portal.

Note
If the Radia Inventory Manager is already installed on the computer, the Radia Management Portal will be installed in the same directory, and the prompt for an install location is skipped.

Click **Next** to accept the default installation folder specified in the window, or click **Browse** to navigate to and select a different folder, and then click **Next**.

The **License File** window opens.

Figure 2.4 ~ License File window.

Click **Browse** to navigate to the location of your license file. If necessary, the installation will rename the license file to **license.nvd**. Then, it will copy the license file into the Radia Integration Server's **\modules** directory.

The **Enable Network Discovery** window opens.

Figure 2.5 ~ Enable Network Discovery window.

Click **Yes** to enable Network Discovery (*recommended*). This option enables the Radia Management Portal to automatically discover all devices in your Windows environment that you can manage.

OR

Click **No** to disable Network Discovery. This option is best used if you are testing the Radia Management Portal and want to prevent the automatic discovery of all machines in your environment from occurring.

Click **Next**.

The **Network Discovery Interval** window opens.

Figure 2.6 ~ Network Discovery Interval window.

In the **Discovery Interval** text box, type how often (in hours) you want the network discovery job to run. Valid entries are **1** to **24**. The default is **24** hours.

To modify this Network Discovery Interval after installation, edit the **NETSCAN_POLL** parameter of the configuration file. For details, see *Configuring Network Discovery* on page 138.

Click **Next**.

The **Discovery Start Delay** window opens.

Figure 2.7 ~ Discovery Start Delay window.

In the **Discovery Start Delay** text box, type how long you want to wait (in hours) after the Radia Management Portal starts before starting the network discovery. The delay applies each time the Radia Management Portal is started. Valid entries are 0 to 24 hours. By default, Network Discovery starts when you start the Radia Management Portal.

To modify the Discovery Start Delay after installation, use the **NETSCAN_START_DELAY** parameter in the configuration file. For details, see *Configuring Network Discovery* on page 138.

Click **Next**.

The first **Zone information** window opens.

Figure 2.8 ~ Management Portal Zone Name information window.

In the **Management Portal Zone Name Name** text box, type a zone name to represent this instance of the Radia Management Portal. **Each instance of the Radia Management Portal in your enterprise must have a unique zone name**.

Enter a name up to 64 characters long. Use only letters (a-z and A-Z), numbers (0-9) and the space character. Do not use special characters, such as an underscores, commas, or periods.

Typically, the initial zone name identifies the entire infrastructure being managed, such as **ACMECorp**. Later installations of subordinate zones are named for the division or location of infrastructure being managed under that zone, such as **NorthAmerica** or **Chicago**.

See *What is a Zone?* on page 25 for more information about Zones.

Click **Next**.

The second **Zone information** window opens.

Figure 2.9 ~ Friendly Zone Name information window.

In the **Management Portal Zone Friendly Name** text box, type a friendly name for this Radia Management Portal Zone. Optional. If omitted, will default to the Zone Name.

The friendly name is the display name for the Zone in the Radia Management Portal user interface.

Click **Next**.

A summary of the installation information opens.

Figure 2.10 ~ Installation Settings window.

Click **Install** to begin the installation.

A message box prompts you to copy the modules used to perform remote installations of the Radia infrastructure components.

Figure 2.11 ~ Prompt to copy modules for infrastructure components.

Click **Yes**.

The **Remotely Installable Components Location** window opens.

Figure 2.12 ~ Remotely Installable Components Location window.

If necessary, click **Browse** to navigate to the location of the Management Infrastructure CD-ROM.

Click **Next**. The modules are copied to the Radia Integration Server's **\media** directory.

A message box prompts you to copy the Radia Client modules to be used for remote installations.

Figure 2.13 ~ Prompt to copy the Radia Client modules for remote installations.

Click **Yes**.

The **Client Modules Location** window opens.

Figure 2.14 ~ Client Modules Location window.

If necessary, remove the Management Infrastructure CD-ROM and insert the Management Applications CD-ROM.

Click **Browse** to navigate to the location of the Management Applications CD-ROM for the Radia Client modules.

Click **Next**.

The Radia Client modules are copied to the Radia Integration Server's **\media** directory. Then, a message box prompts you to install the Documentation (Radia Publications Library).

Figure 2.15 ~ Prompt to install the Radia Publications Library.

Click **Yes**.

The **Publications Location** window opens.

Figure 2.16 ~ Publications Location window.

If necessary, remove the Management Applications CD-ROM and insert the Publications CD-ROM.

In the **Publications Location** window, select the location where the documentation source is stored.

Click **Next**.

The Radia Publications Library is installed to the Radia Management Portal.

Click **Finish** when the installation is complete.

The Radia Management Portal opens.

Logon as **Admin** (*the password is* **secret**).

Updating Tasks

Note

This task is not required the first time you install Radia Management Portal 2.x.

Use **Update Tasks** to update the tasks available to you when you receive a new build of the Radia Management Portal. Any tasks not selected for update remain available for selection at a later time.

Tip

The list of tasks to be added or updated when you run Update Tasks automatically tells you "What's New" in any Radia Management Portal release.

1. If necessary, restart the Radia Management Portal, (the Radia Integration Server [httpd] service).

2. Logon as **Admin** (the password is **secret**) and run **Update Tasks**. Details for running Update Tasks follow.

3. Use the **Navigation aid** to select **Directory, Zone, Configuration, Tasks**.

4. In the **Directory Management** task group, click **Update Tasks**.

5. The **Submit Updates** dialog box opens.

6. Review the task changes in the Differences list and select those that you wish to update.

   ● To select all task changes, click **Select All.**

   ● To select individual task changes, double-click the item.

Caution

HP recommends that you do **not** update a task that has been intentionally customized, such as a Notify task. Doing so will overwrite any customizations. The unaccepted task changes remain available for update at a later time.

Figure 2.17 ~ Run Update Tasks to commit new tasks for RMP 2.x.

7. Click **Commit**.

The new and revised tasks that you selected for the latest release are now available.

To log off the Radia Management Portal

■ In the banner area, click **Logout**.

Updating RMP Zones with a New Build

Refer to the Release Notes that accompany a new build of the Radia Management Portal for details on how to apply the updates. Generally, the same procedure used to install the initial RMP Zone in your enterprise can also be used to apply updates.

To update the subordinate Zones in your enterprise with a new build, the Radia Management Portal includes an **Update RMP** task that is available as of 2.0.1. For details, see *Updating Subordinate RMP Zones* on page 349.

If the new build also includes modifications to the Radia Management Agent (RMA.TKD), use the **Install Management Agent** task to update the Radia Management Agent on the device hosting the Radia Management Portal Zone as well all devices being managed by that Zone.

Specifying the IP Address for a Remote Radia Management Portal

If you are installing the Radia Management Portal on a different computer than where your Radia Configuration Server is installed, you must verify that ZTASKEND contains required lines for the Radia Management Portal, and you must modify the EDMPROF.DAT file on the Radia Configuration Server to specify the IP address and port for the Radia Management Portal.

Complete the tasks below for verifying the contents of ZTASKEND and configuring EDMPROF.DAT.

Verifying the Contents of ZTASKEND

Important Notes
1. This verification step is only required if you are using a ZTASKEND that makes calls to the **RADISH** executable. Customers who have implemented the Radia Messaging Service do not need to perform this task. The ZTASKEND used with the Radia Messaging Service makes calls to QMSG instead of RADISH.
2. If your ZTASKEND calls **radish.exe**, this modification also requires Build 37 or higher of the **radish.exe** on the Radia Configuration Server. To check the build number of the radish program, see *Gathering Version Information for RADISH.EXE* on page 385.

To verify ZTASKEND contains required lines for the Radia Management Portal

On the computer running the Radia Configuration Server, locate **ZTASKEND** in the **\rexx\Novadigm** folder of where the Radia Configuration Server is installed.

By default, **ZTASKEND** is located in: ***SystemDrive*:\Novadigm\ConfigurationServer \rexx\Novadigm**

This directory stores all Radia REXX scripts.

Figure 2.18 ~ ZTASKEND, located in the /rexx/Novadigm folder on the Radia Configuration Server.

Copy **ZTASKEND** and paste it into the **\rexx** directory.

Caution
If you do not copy the ZTASKEND REXX script to this directory, it may be overwritten if you update your Radia Database.

Open **ZTASKEND** (in the **\rexx** directory) with a text editor, such as WordPad.

When the Manager has the Radia Management Portal installed, the lines shown in *Figure 2.19 ~ Lines added to ZTASKEND when the Manager is installed for the Radia Management Portal* below are added to ZTASKEND:

```
/* Object post to Radia Management Portal */
IF  ZCVT.RMP = "ENABLED" THEN DO;
    SAY "**<>** RADIA MANAGEMENT PORTAL ENABLED CALLING RADISH POST: ROUTINE "
    SESSION.REASON = SUBWORD(MYPARM, 2, 1);
    ADDRESS EDMLINK "radish post: -section MGR_RMP /proc/rcs SESSION ZCONFIG
        ZMASTER APPEVENT ZSTATUS";
END;
```

Figure 2.19 ~ Lines added to ZTASKEND when the Manager is installed for the Radia Management Portal.

Verify the lines in Figure 2.19 exist in your ZTASKEND.

If necessary, modify the **ADDRESS EDMLINK** line so that the order of the parameters matches the order shown in Figure 2.19, and below.

```
ADDRESS EDMLINK "radish post: -section MGR_RMP /proc/rcs SESSION ZCONFIG
    ZMASTER APPEVENT ZSTATUS";
```

Close the file and save any changes.

> **Note**
>
> Do not save the ZTASKEND as a text file. Be sure to save this file without an extension.

Configuring **EDMPROF.DAT**

The [MGR_RMP] section of the EDMPROF.DAT file specifies the HTTP HOST for the Radia Management Portal. As shipped from HP, the EDMPROF.DAT file is set up to have the Radia Management Portal and the Radia Configuration Server running on the same computer.

If the Radia Management Portal is running on a different computer than the one running the Radia Configuration Server, you must edit the [MGR_RMP] section of the EDMPROF.DAT file to direct the HOST and PORT to the proper URL.

The default settings are:

HTTP_HOST = Localhost
HTTP_PORT = 3466

The format for this edit is:

HTTP_HOST= HOST NAME
HTTP_PORT= 3466

OR

HTTP_HOST= IPADDRESS
HTTP_PORT= 3466

To edit the EDMPROF.DAT file, use the procedures below.

To edit the EDMPROF.DAT file

Locate the **edmprof.dat** file in the **bin** folder of your Radia Configuration Server. The default location is: *SystemDrive***:\Novadigm\ConfigurationServer\bin.**

As a routine precaution, make a backup copy of **edmprof.dat** before you edit it.

Using a text editor of your choice, open the **edmprof.dat** file, and locate the [MGR_RMP] section, which is shown in *Figure 2.20 ~ [MGR_RMP] section of the edmprof.dat file* below.

```
*--------------------------------------------------------------------------------*
* Manager Radia Management Portal Section                                        *
*  HTTP_HOST       = Host name of Radia Management Portal (RMO)                   *
*          Multiple hosts may be specified (space or comma separated)            *
*          for fail over                                                         *
*  HTTP_PORT       = IP Port number of RMP                                       *
*                    NO restart required                                         *
*--------------------------------------------------------------------------------*
[MGR_RMP]
HTTP_HOST = localhost
HTTP_PORT = 3466
```

Figure 2.20 ~ [MGR_RMP] section of the edmprof.dat file.

Replace the **localhost** entry for HTTP_HOST with the host name or the IP address of the Radia Management Portal host machine.

For example, Figure 2.21 below specifies the Radia Management Portal **host** using an **IP address** of 11.11.11.11. The **port** number of 3466 is the default port number attended by the Radia Management Portal.

```
[MGR_RMP]
HTTP_HOST = 11.11.11.11
HTTP_PORT = 3466
```

Figure 2.21 ~ Specify the IP address or the host name of the Radia Management Portal as the HTTP_Host entry in the [MGR_RMP] section.

Save your changes and exit the text editor.

The Radia Configuration Server is now configured to use the remotely installed Radia Management Portal, as specified in edmprof.dat.

Note

To verify that the Radia Configuration Server is using the specified Radia Management Portal, you can either monitor the posts in the RCS log or check the clients in the Radia Management Portal (since each client will show the services that you deployed under the Radia Subscribers section).

Starting and Stopping the Radia Management Portal

To start the Radia Management Portal

1. If necessary, go to the Windows Services. For example, in Windows 2000, right-click the **My Computer** icon on your desktop. Then, select **Manage**. Expand **Services and Applications**, and then click **Services**.

2. Right-click the Radia Integration Server and select **Start**.

To stop the Radia Management Portal

1. If necessary, go to the Windows Services. For example, in Windows 2000, right-click the **My Computer** icon on your desktop. Then, select **Manage**. Expand **Services and Applications**, and then click **Services**.

2. Right-click the Radia Integration Server and select **Stop**.

Accessing the Radia Management Portal

To access the Radia Management Portal

1. Open your Web browser.

2. In the Address bar, type http://<*IP_Address or host name*>:3466.

    ●   *IP_Address* is the IP address of the computer where the Portal Zone Directory is installed.

    ●   *Host name* is the host name of the computer where the Portal Zone Directory is installed.

Figure 2.22 ~ Radia Management Portal Login page.

Note

If the Radia Inventory Manager, Radia Policy Manager, or Publications Library is installed on the same computer as the Radia Management Portal, links will be available in the top-right banner area, next to the link for HOME.

For example, if INVENTORY displays in the banner area of the Radia Management Portal, click on that link to access the Radia Inventory Manager.

Logging On

To log on to the Radia Management Portal

1. In the **User Name** text box, type a user name.

    ● **Admin**
       Type **Admin** to log on with complete access to the Radia Management Portal. We recommend that you do not modify this ID.

    The password is *secret*.

Caution
Be sure to change your password before moving the Radia Management Portal into your production environment. See *Changing Passwords* on page 58 for more information.

- **Guest**
  Type **Guest** to log on as an unauthenticated user without access to tasks.

  No password is necessary.

- **Operator**
  Type **Operator** to log on as a user with access to basic operations.

  No password is necessary.

- **Test**
  Type **Test** to log on as a test user with very limited access. You can log on as the Portal Administrator and modify the entitlement options for the Test User. Then, log on as Test to view the results of your changes.

  No password is necessary.

Figure 2.23 ~ Login page for the Radia Management Portal.

2. If necessary, in the **Password** text box, type a password. The password is case-sensitive.

The password for the Admin ID is *secret*. No password is necessary for the other IDs.

3. Click **Login**.

OR

Press ENTER.

Your User ID appears in the banner area (the top, left area of the interface) and the highest-level representation of your Radia Zone Directory appears in the workspace. See *Performing Any Task in the Radia Management Portal* on page 64 for more information.

To log off the Radia Management Portal

■ In the banner area, click **Logout**.

Changing Passwords

Changing your password requires familiarity with the user interface and the basics of performing a task. It is performed in the **Modify Person** dialog box for the specific user.

For information about the Radia Management Portal user interface, see page 65.

■ For information about performing tasks, see *Performing Any Task in the Radia Management Portal* on page 64.

To change your password

1. Use the Navigation aid to go to the **Directory, Zone** location. From the initial logon location of your Desktop, click **Directory** in the workspace, and then click **Zone**.

2. In the workspace, click **Administrators & Operators**.

3. In the workspace, select the person whose password you want to change, such as the **Portal Administrator**.

The workspace displays the Desktop and Sessions container for the Person.

> **Note**
>
> The **User Password** field is not displayed in the **Properties** dialog box, but is changed on the **Modify Properties** dialog box for that user.

---

4. In the **Model Administration** task group, click **Modify**.

The **Modify Person** dialog box opens.

Figure 2.24 ~ Modify Person dialog box.

5. In the **User Password** text box, select all asterisks masking the old entry, and then type the new password. Passwords may include alphanumeric characters as well as spaces and special characters, such as #, $, and \.

6. Click **Modify**.

The Modify Person dialog closes and the workspace displays the Desktop and Session containers for the **Portal Administrator**.

Figure 2.25 ~ Navigation location after changing Portal Administrator password.

The password is changed, but is not displayed for security purposes.

> **Note**
>
> To display the properties for any user, navigate to the user object in the **Administrators and Operators** container of the Zone, and then click the View Properties Toolbar icon 🔍.

Summary

■ Install an initial Radia Management Portal 2.0, giving it a zone name. This installation becomes your enterprise's Master Zone.

■ To install additional Radia Management Portal zones, use the **Install RMP** task in the Operations task group. This task installs subordinate zones remotely. All zones in your enterprise must be unique.

■ Click **Logout** in the banner area to log off the Radia Management Portal.

■ Change passwords from the **Zone, Administrators, and Operators** container. Select the user and click **Modify** from the Model Administration task group.

■ Run **Update Tasks** after obtaining a new build of the Radia Management Portal to update the tasks available to you.

■ Run **Update RMP** to update subordinate Zones in your enterprise with a new build, such as a Radia Management Portal Service Pack.

3

Using the Radia Management Portal

At the end of this chapter, you will:

■ Be familiar with the Radia Management Portal user interface for 2.x, including how to use the Navigation aid in location and history mode, how to use the Desktop and shortcuts, and how to use the Toolbar icons.

■ Be familiar with the task groups and tasks available in the Radia Management Portal 2.0.

■ Be familiar with the new icons that represent the objects in your infrastructure.

■ Be familiar with the Zone containers that exist at the highest level of the directory.

■ Know how to navigate to any location in the Radia Management Portal Zone.

■ Know how to navigate to locations that has been configured for access from the Radia Management Portal, including Networks, the Radia Database on a Radia Configuration Server and an Active Directory or other LDAP Directory in your enterprise.

■ Be able to use the RCS Administration tasks to manipulate *instances* in the Radia Database

■ Be able to use the Policy and Policy (Advanced) tasks to assign and manage policy through an LDAP Directory, including Active Directory.

Performing Any Task in the Radia Management Portal

One of the benefits to using the Radia Management Portal is consistency. Because of this consistency, you can use the same basic procedure whether you are notifying devices in your infrastructure or installing the Radia Proxy Server on remote computers.

To perform any task in the Radia Management Portal

1. Use the Navigation aid to select where, in your infrastructure, you want to perform a task. Your selected location is also called your *authority*.

   The procedures throughout the guide refer you to the appropriate starting locations. See the *Taskbar and Task Summary* on page 82 for a list of all tasks.

2. From the **Group of Tasks** taskbar, select a task.

3. In the workspace, enter the information needed to complete the task, such as the device members you want to perform the task on or information about when the job should execute. See *About the Task Lifecycle* on page 283 for detailed information on completing tasks.

| Select Authority | Select a task | Enter necessary information |

Figure 3.1 ~ Performing tasks in the Radia Management Portal.

> **Note**
>
> For detailed information about the Radia Management Portal user interface, see **About the Radia Management Portal 2.x** Interface on page 65.
>
> For detailed information about specific tasks, see the *Administrative Functions* and *Operations Functions* chapters.
>
> For detailed information about using the RCS and Policy tasks, see the topics beginning with *Using the RCS Administration Tasks* starting on page 102.

About the Radia Management Portal 2.x Interface

The Radia Management Portal user interface contains several distinct areas.

Figure 3.2 ~ Radia Management Portal 2.x user interface.

- **Banner area.** This area is discussed on page 66.

- **Navigation aid (History or Location mode).** The previous Authority navigation aid is renamed the Navigation aid. The new Navigation aid has two modes: History (the default) and Location (the mode used in all RMP 1.x releases). Use the icons in the top-right of the Navigation title bar to quickly switch from one mode to the other. For details, see *Navigation Modes: History and Location* on page 68.

- **New Desktop location**. When you log on to the Radia Management Portal, you start at the level of your Desktop, in Navigation (History) mode. This starting location gives you quick access to the Radia Management Portal Directory and the containers and objects in the current Radia Management Portal Zone. As you use this version of the Portal, you can add (and then remove) shortcuts for other locations or devices to your desktop. From the level of the Directory, you can access an external Active Directory that has been configured for access by a Portal Administrator. See *Accessing and Returning to Your Desktop* on page 71 for more information.

- **New Navigation indicators.**
  - *Asterisks* surround the entry in the Navigation aid that is your current location. The objects for this location are displayed in the workspace.

● [Brackets] indicate an object has children.

■ New **Groups of Tasks**. See *Taskbar and Task Summary* on page 82 for a complete list of Task Groups and a summary of all tasks available from the Portal.

■ New **Toolbar** icon buttons. See *Toolbar* on page 94 for more information.

■ New Container objects in your Radia Zone. See *Radia Directory and Zone Objects* on page 96.

Banner

The banner area contains descriptive information about where you are in the Radia Directory, several links, and displays version information for the product.

■ Click **Logout** to log off the Radia Management Portal (RMP).

■ Click **HOME** to return to the RMP home page. This is the Directory location in Navigation (Location) mode.

■ Rest the mouse pointer on the 🔵 button to display the Radia Management Portal version number. For example, a display of `RMP V2.0` indicates the Radia Management Portal Version 2.0.

■ After logging in, click the 🔵 button to view detailed version and build level information for the Radia Management Portal component modules. This information is helpful when you are contacting HP Technical Support. For more information, see *Viewing the Version Information Window* on page 383.

Figure 3.3 ~ Radia Management Portal Version Information window.

> **Note**
>
> If the Radia Inventory Manager or Radia Policy Manager are installed on the same computer, click the appropriate link (**INVENTORY** or **POLICY**) in the banner of the Radia Management Portal to access them.
>
> If the Radia Publications Library is installed on this computer, click the **PUBS** link in the banner of the Radia Management Portal to access the library.

Using the Navigation Aid

Use the **Navigation aid** to browse and then select the place in the Radia Management Portal Directory where you want to perform a task. It is important that you understand that e*very task you select in the Radia Management Portal is performed within the selected authority.*

When you logon to the Radia Management Portal, you start at the level of your Desktop, in Navigation (History) mode.

Figure 3.4 ~ Initial Desktop location in Navigation (History) mode.

This starting **Desktop** location gives you quick access to the Radia Management Portal Directory and the containers and objects in the current Radia Management Portal Zone.

You can add shortcuts to your desktop to quickly go to objects that you use most often. See *Adding Shortcuts to Your Desktop* on page 72 for more information.

Navigation Modes: History and Location

There are two modes of navigation: Navigation (History) 🗀 and Navigation (Location) 🌑. Click the icon to switch between the modes at any time.

■   **Navigation (History)** 🗀
This is the default mode of navigation when you login to the Radia Management Portal. To toggle to the Navigation (Location) mode, click 🗀.

The Navigation (History) aid provides a record of your navigation path. To quickly return to a previously visited location, just click any entry in the Navigation (History) record.

●   *Asterisks* surround the entry in the Navigation aid that is your current location. The objects for this location are displayed in the workspace.

●   [Brackets] indicate an object has children.

Figure 3.5, below, shows the user's current location is the ACME Corp **Zone** level, but the user previously visited the Microsoft Windows Network within the Zone Networks container.

Use the History mode to jump back and forth among visited locations.

Figure 3.5 ~ Navigation (History) records visited locations. Asterisks show current location.

■   **Navigation (Location)** 🌑
This mode allows you to use the Directory structure to select where in the Directory you want

to perform your task. To toggle to the Navigation (History) mode, click 🌑.

Figure 3.6 shows the Desktop location when viewed in Navigation (Location) mode. The Desktop is under the current Person's entry within the Zone Administrators & Operators container.

Figure 3.6 ~ Desktop location in Navigation (Location) mode.

Sample Navigation Session: Viewing Network Objects

Use the steps in the following procedure to become familiar with navigating the Radia Management Portal Zone containers and viewing the objects automatically discovered in your networks.

To access the Portal Directory and the Microsoft Windows Network

When you first logon, your **Desktop** displays in the Navigation aid. If you aren't at this location, click **HOME** in the banner area and then click on the **Desktop** entry in the Navigation area.

The Radia Management Portal Directory object appears in the workspace.

In the Workspace, click **Zone**.

Figure 3.7 ~ Authority–Zone Containers accessed from the Desktop.

The highest-level objects in the Zone appear in the workspace. See *About the Zone Containers* on page 97 for more information.

> **Note**
>
> New container objects at the Zone level for this release include **Configuration**, **Cross References, Devices, Groups** and **Zone Access Points** containers.

In the workspace, click **Networks**.

Figure 3.8 ~ Authority–Zone Networks container.

Notice that the navigation aid now lists **Desktop**, **Zone**, and **Networks**. This is your selected authority.

Besides the Microsoft Windows Network of discovered objects, there are also entries for DNS, Microsoft Terminal Services, Netware, and Web Client Networks**.** Your list will vary according to your enterprise networks and what networks have been configured as mount points. See *Configuring Directory Services* on page 143.

In the workspace, click **Microsoft Windows Network.**

In large networks, use the filtering and paging options to locate objects by their common name:

● For example, enter ***nt*** in the filter text box and click ⏷ to view only those objects whose names include "nt". To remove the filter, delete the entry and click ⏷ .

● Or, set the maximum number of items per page, and then page through the selections using the Browse buttons or the Page drop-down list box to select a specific page.

> **Note**
>
> The objects in your Microsoft Windows Network will be different from the ones in this example because information about your environment is auto-discovered.

Figure 3.9 ~ Browse options for objects in Microsoft Windows Network.

To return to the Desktop, click **[Desktop]** in the Navigation aid.

Accessing and Returning to Your Desktop

The desktop is the default location you access when you logon. If you want to return to the desktop from any point in your session, do the following:

Click **HOME**. HOME is located at the top-right of the Banner.

HOME returns you to **Navigation (History)** mode, at the Directory level.

Figure 3.10 ~ Use HOME to return to Directory or Desktop.

Click on the **Desktop** entry in the Navigation aid.

Adding Shortcuts to Your Desktop

This version of the Radia Management Portal introduces the ability to add shortcuts to the new desktop location. The Desktop location is unique to each user.

To add a shortcut to the desktop

Start in Navigation (History) mode.

To create a shortcut to a particular device group or location within your infrastructure, navigate to that device or location. For example, the figure shows an example of navigating to the **Default Group** for devices by selecting **Zone, Groups**, and then **Default Group**.

Figure 3.11 ~ Object to be added as a Shortcut to your Desktop.

After navigating to the location where you want shortcut, click the **Add Desktop Shortcut** icon on the **Toolbar**.

The **Add Shortcut to (selected location)** window opens.

Figure 3.12 ~ Add Shortcut to Default Group, Confirmation Window.

Click ✔ to confirm that you want add the shortcut.

OR

Click ✘ to indicate that you do not want to add the shortcut.

If you click ✔, the shortcut is added to the desktop.

Shortcuts remain on the Desktop between sessions until they are removed.

Figure 3.13 ~ Desktop now Includes Shortcut to Default Group.

Removing Shortcuts from Your Desktop

You can remove any shortcuts you have added to the your Desktop using the **Remove Shortcuts from the Desktop** task in the **Model Administration** task group.

To remove shortcuts from the desktop

1. Return to your Desktop location. If you need help, see *Accessing and Returning to Your Desktop* on page 71.

Figure 3.14 ~ Select Remove Shortcuts from Desktop task in Model Administration group.

2. In the **Model Administration** task group, click **Remove Desktop Shortcuts**.

   The **Remove Objects** window opens with all desktop shortcut objects placed in the **Available** column.

Figure 3.15 ~ Remove Objects window for selecting shortcuts to remove from desktop.

3. Move any shortcuts you want removed from your desktop to the **Selected** column. To move the shortcuts between columns, use the **Arrow** icon buttons or double-click on an entry.

4. After moving all shortcuts to be deleted to the **Selected** column, click **Next**.

The **Remove Objects Summary** dialog opens. The Selected Audience area lists each shortcut to be removed from your desktop.

Figure 3.16 ~ Summary Page for Removing Shortcuts from your Desktop.

5. Click **Submit** to remove the shortcuts listed as the Selected Audience from your Desktop.

You are returned to the **Desktop** location. Only the shortcuts that you did not remove will be shown.

Navigating the Portal Directory and the Zone Containers

> **Note**
>
> The term Authority Navigation Aid has been changed to Navigation Aid.

Use the Navigation aid to browse your infrastructure and to select the place where you want to perform a task. It is important that you understand that e*very task you select in the Radia Management Portal is performed within the selected level of authority.*

Below is an example of how to select an authority in the Microsoft Windows Network.

To navigate the Zone Containers

To access the Portal Directory Zone containers when in Navigation (History) mode, click on your **Desktop**.

The Desktop objects appear in the Workspace.

> **Note**
>
> In Navigation (Location) mode, the Desktop is always the top entry in the Navigation aid.

In the Workspace, click the **Zone** icon.

Figure 3.17 ~ Authority–Zone Containers accessed from the Desktop.

The highest-level objects in the Zone Directory appear in the workspace. These are the Zone containers.

> **Note**
>
> New objects at the Zone Directory level for this release include containers for **Configuration**, **Cross References, Devices, Groups,** and **Zone Access Points**.

In the workspace, click **Devices**.

Figure 3.18 ~ Authority–Zone Devices container.

Notice that the navigation aid now lists **Desktop**, **Zone,** and **Devices**. This is your selected authority.

Each device being managed by this Radia Management Portal Zone must have an entry in the Devices container. There are a number of ways to bring devices under management. These are discussed in *Establishing Devices and Device Groups* on page 165.

In general, the Device container is mostly *self-managed*. That means by performing other tasks, the Radia Management Portal automatically creates or updates the Devices container entries for you.

See *About the Zone Containers* on page 97 for detailed information on the Devices container and the other Zone containers.

Now let's return to the **Zone** level containers. You can either:

● Click the toolbar icon to go up one level in the Navigation path.

OR

● Click the **[Zone]** entry in the **Navigation aid.**

The workspace displays the Zone containers, again. However, your Navigation path indicates all visited location.

Figure 3.19 ~ Navigation history reflects visit to Devices container.

Now click the **Groups** container in the Workspace.

The Groups container displays all current groups of devices in the workspace. If you have just installed the Radia Management Portal, only the **Default Group** object appears. If the Radia Management Portal is not newly installed, you will see many user-created groups in this container.

Figure 3.20 ~ Sample Zone Groups container with 3 Groups of Devices.

The Groups container is one of the most important containers in the Radia Management Portal for performing operations. Almost all tasks are performed on Groups of Devices.

Devices from the Device container hold *memberships* in these groups; the device objects do not exist within the Group containers. The group memberships can be added or removed, at will.

See *Configuring the Zone Infrastructure* on page 182 for more information on how to create groups and add or import devices into the groups.

Click the **Default Group** object in the Workspace, and then click **View Properties** icon on the toolbar: .

The **Group Properties** page for the **Default Group** object opens.

Figure 3.21 ~ Default Group properties page with Member links.

Notice that each device in the group is listed under the **Members** entry in the Properties area with a link.

Click on a link in the Members area to go to the device's Properties page.

Figure 3.22 ~ Default Group properties page with Member links.

> **Note**
>
> If you switch to Navigation (location) mode, you see that this page is actually within the Devices container.container.

Notice that the Properties page for a Device lists **Group Memberships**. The sample Device shown in Figure 3.22 is a member of two groups: the **Default Group**, and a user-created group named **doc_dept_machines**.

Click on the **HOME** link in the top-right of the banner area to quickly return to your Desktop.

Notice that using HOME clears all entries in the Navigation (History) area.

This completes the navigational discussion of how to access and navigate the Zone containers. The next topics discuss the taskbar and tasks, and the powerful toolbar entries.

Taskbar and Task Summary

When you use the Navigation aid to access your infrastructure, the Taskbar appears. The Taskbar contains logical groups of tasks (called *task groups*). A *task* is an activity that a person performs to initiate a job. The tasks that are available vary, based on the selected navigation location, as well as your role.

The standard task groups include:

- Directory Management
- Infrastructure
- Inventory Management
- Model Administration
- Operations
- Policy Management
- Policy (Advanced)
- RCS Administration

See *Toolbar Tasks* on page 93 for information about the tasks that can be initiated directly from icons in the Toolbar.

See *Configuring Task Groups* on page 212 for information about adding, modifying, or removing task groups.

Click to maximize or to minimize a group of tasks.

Directory Management Task Group

Use the **Directory Management** task group to manage the Radia Management Portal Directory.

Figure 3.23 ~ Sample Directory Management task group.

■   **Backup Directory**
   Click **Backup Directory** to backup the entire Radia Management Portal Zone Directory.
   See *Creating a Backup of the Portal Zone* Directory on page 245 for more information.

■   **Export**
   Click **Export** to export a subset of your Radia Management Portal Zone Directory to an
   LDIF (LDAP Data Interchange Format) file. See *Exporting Data from the Portal Directory*
   on page 253 for more information.

■   **Import**
   Click **Import** to import an LDIF (LDAP Data Interchange Format) file into your Radia
   Management Portal Zone Directory. See *Importing Data into the Portal Directory* on page
   256 for more information.

■   **Restore Directory**
   Click **Restore Directory** to restore a backup of the entire Portal Zone Directory. See
   Restoring the Portal Directory on page 249 for more information.

■   **Update Tasks**
   Click **Update Tasks** when you receive a new build of the Radia Management Portal to
   update the tasks available to you. Available from the Zone, Configuration, Tasks container.
   See *Updating Tasks* on page 260 for more information.

Infrastructure Task Group

Use the **Infrastructure** task group to connect to or disconnect from external services, such as the Radia Database on a Radia Configuration Server or an Active Directory service. Services are configured for access from the Zone, Configuration, Directory Services container.

2.0 **Connect to Directory Service**
Click **Connect to Directory Service** to connect to the Primary Database on the Radia Configuration Server, or other directory service such as Active Directory. See *Connecting to a Directory Service* on page 154 for more information.

2.0 **Disconnect from Directory Service**
Click **Disconnect from Directory Service** to disconnect an external service, such as the Primary Database on the Radia Configuration Server, or another directory service such as Active Directory. See *Disconnecting from a Directory Service* on page 157.for more information.

Model Administration Task Group

Use the **Model Administration** task group to manage the Radia Management Portal Directory and a Zone.

Figure 3.24 ~ Sample Model Administration task group (for a Group of devices.)

The following is a list of all potential Model Administration tasks available in the Radia Management Portal. Remember, the available tasks vary based on your selected navigation location; therefore, Figure 3.24 does not contain all the tasks described here.

■   **Add *object-type***
Click an Add task to create an object in your selected authority, such as a device, group of devices, server, person, user group, delegated administration, task group, or directory service. New object-types for this release are specified below:

2.0   **Add *Device***
Click **Add Device** to define a new device to the Zone and also give it membership in the Default Group or other group within the Zone Groups container. This task automatically creates an entry for the device in the Zone Device container. See *Adding Devices to an RMP Zone*on page 165 for more information.

2.0   **Add *Directory Service***
Click the new **Add Directory Service** task to configure a connection between the Radia Management Portal zone and another Directory Service, including the Radia Configuration Server ZTOPTASK service. The task is available from the Zone, Configuration, Directory Service container. See *Adding a Directory Service* on page 143 for more information.

2.0   **Add *Group* (of Devices)**
Click **Add Group** from the Devices container to create a new Group of Devices for organizing devices for operations. See *Adding Groups* on page 189 for more information. To move or add members to a group in the same task, or later import devices into a group, refer to the **Import Devices** task.

2.0   **Add *Install Profile***
Click **Add Install Profile** to define a custom profile for selection during the **Install Client** task. Add Install Profile is available from the **Zone, Configuration** container, by browsing to Profiles, Radia Products, and then Client Installs. See *Adding, Modifying, and Deleting Install Profiles* on page 320 for more information.

·   **Disable**
Click **Disable** to prevent a job or job group from being processed. See *Disabling Jobs or Job Groups* on page 271 for more information.

·   **Enable**
Click **Enable** to restart a job or job group the next time it is scheduled to run. See *Enabling Jobs or Job Groups* on page 271 for more information.

2.0   **Import Devices**
Click the **Import Devices** task to add a list of devices with fully qualified DNS names into the Zone Devices container. The devices become members of the Zone Groups container group from which you begin this task. See *Importing Devices* on page 202 for more information.

- **Modify** 🔶
  Click **Modify** to change an object. For example, you might want to change the areas of the Radia Management Portal that an administrator can access, or change a job group's schedule. See *Modifying Objects* on page 209 or *Modifying Job Groups* on page 265 for more information.

2.0 **Move/Copy Device(s)** 📁
  Click the **Move/Copy Device(s)** task to move or copy devices that are members of other groups into the group you have selected from the Zone Groups container. See *Moving or Copying Devices into a Group* on page 195 for more information.

- **Query** 📁
  Click **Query (also available from the Toolbar)** to extract information from the directory tree or to narrow the scope of a job. For example, you might want to search for a specific audience for whom you want to schedule a task. See *Performing Queries* on page 285 for more information.

- **Query Jobs** 📁
  Click **Query Jobs** to locate existing jobs, review their status, and make changes to them. See *Querying Jobs or Job Groups* on page 267 for more information.

- **Query User's Delegated Administration** 📁
  Click **Query User's Delegated Administration** to display information about a user's role. See *Querying a User's Delegated Administration* on page 231 for more information.

- **Remove** ❌
  Click **Remove** to remove an object and all of its children from the Radia Management Portal Directory. See *Removing Objects* on page 209 or *Removing Jobs or Job Groups* on page 272 for more information.

2.0 **Remove Shortcuts from Desktop** ❌
  Click **Remove Shortcuts from Desktop** to remove any previously added shortcuts from your **Desktop** location. See *Removing Shortcuts from Your Desktop* on page 74 for more information.

- **Restart Failed Jobs** 🟢
  Click **Restart Failed Jobs** to restart the failed jobs displayed in the current Job Group. See *Restarting Failed Jobs in a Job Group* on page 269 for more information.

- **Stop** 🛑
  Click **Stop** to stop an active job group from running. See *Stopping Job Groups* on page 270.

- **View Properties** 🔑
  Click **View Properties** from the Model Administration task group or click 🔑 from the Toolbar to display the properties of an object. See *Viewing Properties* on page 274 for more information.

Operations Task Group

Use the **Operations** task group to perform operations on your Radia infrastructure. This release introduces the following new tasks.

Figure 3.25 ~ Sample Operations task group.

The following describes all of the operations available in the Radia Management Portal. Remember, the tasks available to you vary based on your selected authority: therefore, Figure 3.25above may not contain all of the tasks described here.

2.0   **Add Job Sequence**
Use **Add Job Sequence** to define a job sequence. Access the task from the **Jobs** container. Sequencing jobs can be an efficient tool for managing jobs common to many devices across many zones. See *Sequencing Jobs* on page 359 for more information.

2.0   **Add Task Template**
Add Task Template is available from the Task Template container within the Zone, Configuration container. Use **Add Task Template** to preset the options for a Task Type, such as Notify or Install RPS, as a saved Task Template. Task templates can be selected and applied during the Schedule Zone Operations task. See *Managing Task Templates* on page 340 for more information.

■   **Help Desk Notify**
Click the **Help Desk Notify** icon on the toolbar to quickly Notify a single computer, whose name you already know. See *Using Help Desk Notify* on page 295 for more information.

■   **Install Client**

Click **Install Client** to install the Radia Client on remote computers. See *Installing the Radia Client* on page 314 for more information. Multiple Client Install Profiles are supported. For details, see *Supporting Remote Installs Using Multiple Profiles* on page 320.

■   **Install Management Agent**

Click **Install Management Agent** to install the Radia Management Agent on remote computers. See *Installing the Radia Management Agent* on page 307 for more information.

■   **Install Proxy Server**

Click **Install Proxy Server** to install the Radia Proxy Server on remote computers. See *Installing the Radia Proxy Server* on page 329 for more information.

2.0   **Install RMP**

Click **Install RMP** to remotely install another Radia Management Portal Zone in your infrastructure. See *Installing Additional RMP Zones (Subordinate Zones)* on page 344 for more information. Also refer to the tasks for **Update RMP**, **Open Subordinate Zone** and **Schedule Zone Operation**.

2.0   **Open Subordinate Zone**

Click **Open Subordinate Zone** to quickly access the Radia Management Portal of another Zone in your enterprise from the **Zone Access Points** container. See *Opening a Subordinate Zone* on page 356 for more information.

■   **Purge Dynamic Cache**

Click **Purge Dynamic Cache** to purge the dynamic cache of the Radia Proxy Server. See *Purging the Dynamic Cache of the Radia Proxy Server* on page 336 for more information.

■   **Notify**

Use the **Notify** tasks to perform an action on the selected audience. See *Using the Notify Tasks* on page 291 for more information.

■   **Purge Dynamic Cache**

Click **Purge Dynamic Cache** to purge the dynamic cache of the Radia Proxy Server. See *Purging the Dynamic Cache of the Radia Proxy Server* on page 336 for more information.

■   **Refresh Management Agent**

Click **Refresh Management Agent** to have the selected Management Agent immediately update its registered Radia services with the Radia Management Portal. See *Refreshing the Radia Management Agent* on page 314 for more information.

■   **Restart**

Click **Restart** to stop a service and then start it again. See *Managing Services* on page 338 for more information.

■   **Resume**

Click **Resume** to resume execution of a service that has been paused. See *Managing Services* on page 338 for more information.

- **Set Password**
  Click **Set Password** to set the VNC Authentication password prior to the first time you use remote control to access a VNC Server on a Radia client. See *Using Remote Control* on page 363 for more information.

2.0 **Schedule Zone Operation**
  Click **Schedule Zone Operation** from the **Zone Access Points** container to run a Notify or Install RPS job on all devices in each of the selected zones in your enterprise. The job options must be predefined as a Task Template. See *Scheduling Zone Operations* on page 349 for more information.

- **Start**
  Click **Start** to run a service. See *Managing Services* on page 338 for more information.

- **Start Viewer**
  Click **Start Viewer** to start a VNC session on a remote Radia client. See *Using Remote Control* on page 363 for more information.

- **Stop**
  Click **Stop** to stop a service. See *Managing Services* on page 338 for more information.

- **Synchronize Proxy Server**
  Click **Synchronize Proxy Server** to force the Radia Proxy Server to connect to the Radia Configuration Server to preload the files to the static cache on the Radia Proxy Server. See *Synchronizing the Radia Proxy Server* on page 335 for more information.

2.0.1 **Update RMP**
  Click **Update RMP** to remotely update the code delivered with a new build to the subordinate Radia Management Portal Zones in your infrastructure. See *Updating Subordinate RMP Zones* on page 349 for more information.

Policy Task Group

Use the **Policy** task group to assign policy using an LDAP Directory, such as Active Directory.

Figure 3.26 ~ Policy task group.

The following is a list of the available Policy tasks. Remember, the available tasks vary based on your selected authority.

2.0   **Add Policy Object**
Click **Add Policy Object** to create a new group or organizational unit in an LDAP Directory. See on page for more information. See *Adding a Policy Object* on page 112 for more information.

2.0   **Modify Policies**
Click **Modify Policies** to assign services to the selected policy object. See on page for more information. See *Modifying Policies* on page 115 for more information.

2.0   **Modify Targets**
Click **Modify Targets** to specify members of a group to be targeted based on the policy assignments. See *Modifying Targets* on page 116 for more information.

2.0   **Remove Policy Object**
Click **Remove Policy Object** to remove a group or organizational unit from an LDAP Directory. See on page for more information. See *Removing a Policy Object* on page 114 for more information.

2.0   **Refresh Managed Services Cache**
Click **Refresh Managed Services Cache** to refresh the list of services displayed in the Radia Management Portal. This list is created from information in the Radia Database. See on page for more information. See Refreshing the Managed Services Cache on page 124 for more information.

2.0.1 **Resolve Policy**

Click **Resolve Policy** to resolve the service entitlements for an object. The list is grouped by product type and then policy source, and may be viewed for a specific domain filter (DNAME). For LDAP objects, you can specify values for attributes, such as Hostname, OS, UserID, and Context, which are normally available at the time of resolution. See *Resolving Policy* on page 118 for more information.

Policy (Advanced) Task Group

Use the **Policy (Advanced)** task group to modify the Radia Policy attributes as described in the *Policy Server Guide*. These attributes are used to manage policy scope, relationships, and assignments.

Caution
Make sure that you have a good understanding of the Policy Server and the Radia Policy attributes before using these tasks.

The tasks available are:

2.0 **Modify Defaults**

Click Modify Defaults to set the defaults for the attributes in a service. Using this task modifies edmPolicyDefault. See the *Policy Server Guide* for details. See *Modifying Defaults* on page 130 for more information.

2.0 **Modify Dependencies**

Click **Modify Dependencies** to modify policy links. Using this task modifies the edmLink attribute. See the *Policy Server Guide* for details. See *Modifying Dependencies* on page 126 for more information.

2.0 **Modify Flags**

Click **Modify Flags** to limit the scope of policy resolution for specific objects. Using this task modifies the edmFlags attribute. See the *Policy Server Guide* for details. See *Modifying Flags* on page 129 for more information.

2.0 **Modify Overrides**

Click **Modify Overrides** to bypass the pre-set values of one or more attributes for a service and specify alternate values. Using this task modifies the edmPolicyOverride attribute. See the *Policy Server Guide* for details. See *Modifying Overrides* on page 131 for more information.

RCS Administration Task Group

Use the **RCS Administration** task group to manage instances in the Radia Database.

Figure 3.27 ~ RCS Administration task group.

The following is a list of the RCS Administration tasks. Remember, the available tasks vary based on what you have selected in the navigation aid.

2.0   **Add Connections**
Click **Add Connections** to add connections to the selected instance. See *Adding Connections* on page 104 for more information.

2.0   **Copy**
Click **Copy** to create a copy of the selected instance. See *Copying Instances* on page 106 for more information.

2.0   **Create**
Click **Create** to add a new instance to the current class. After adding the new instance, use the Modify and Add Connections tasks to set the attributes and make connections for the instance. See *Creating Instances* on page 103 for more information.

2.0   **Delete**
Click **Delete** to remove the selected instance from the Radia Database. See *Deleting Instances* on page 107 for more information.

2.0   **Modify**
Click **Modify** to modify the selected instance. Use the Advanced View in the Modify window to modify any attributes that you can modify from the System Explorer. See *Modifying Instances* on page 108 for more information.

2.0 **Remove Connections**
Click **Remove Connections** to remove connection(s) from the selected instance. See *Removing Connections* on page 109 for more information.

Toolbar Tasks

2.0 **Add Shortcut to Desktop**
Click **Add Shortcut to Desktop** to add a shortcut icon to the **Desktop** location within the Radia Management Portal for easy access to frequently visited locations. The desktop location is unique for your Username, and is your initial logon location. See *Adding Shortcuts to Your Desktop* on page 72 for more information.

2.0 **Help Desk Notify**
This release introduces a streamlined task to Notify a computer from the new Help Desk Notify icon. Use the toolbar icon for **Help Desk Notify** to quickly Notify a single computer. Typically, this is used by Help Desk staff working on an issue. Available from any location within the Desktop or Zone. A computer DNS name must be entered and cannot be selected from a list. See *Using Help Desk Notify* on page 295 for more information.

2.0 **View Properties**
Click **View Properties** from the Toolbar to display the properties of an object. See *Viewing Properties* on page 274 for more information.

Toolbar

The Toolbar appears at the top of the workspace when you are viewing objects in your Radia Directory, such as a list of all computers in your network. This toolbar appears if you are browsing your infrastructure or viewing the results from a query.

Figure 3.28 ~ Sample Radia Management Portal Toolbar.

Note
Some Figures throughout this book show an earlier version of the toolbar. Please discregard these earlier images and refer to this topic for toolbar usage information.

Navigation Icons

■   Click ⬅ t to Back one page.

■   Click ➡ t to go Forward one page.

■   Click 📁 to go up one level in the Radia Management Portal Directory.

■   Click 🔄 to refresh the information displayed in the workspace.

Task Icons

See *Toolbar Tasks* on page 93 for more information on these tasks.

■   Click 🔍 to **View the Properties** for the *****current***** object in the navigation aid.

■   Click 🔲 to **Add a Shortcut** to your desktop for the *current***** Navigation location.

■   Click 🔍 to **Query the Directory** for objects at the current level or below.

■   Click 📋 to open the Help Desk Notify dialog to notify a single computer whose name you know.

Print and Status Icons

■   Click ![printer icon] from the Jobs container to obtain a printable view of the job list.

Several formats are available for viewing most objects.

Use the **Status** drop-down list box to view only jobs that meet the selected status. Job status options include:

■   All
■   Waiting to Start
■   Successful
■   Failed
■   Active
■   Disabled

View Icons

■   Click ![large icons icon] to show the potential targets with large icons.

■   Click ![small icons icon] to show the potential targets in a list view (small icons).

■   Click ![detailed view icon] to show the potential targets in a detailed view.

Paging and Filtering Icons

The following icons assist in browsing and selecting from large numbers of items.

■   Use the drop-down list box to set the maximum number of items for a given page:

    | 100 Items ▼ |

■   In the filter text box, type a filter value and click ![filter icon] to filter the items on the current page according to their display names, common names, and cn= values.

    | | ▼ |

    Valid filter entries include text, asterisk (*) and question mark (?) wildcards, cn= values, as well as LDAP attribute values (attribute=*value*).

■   To remove a filter, clear the text box and click ![filter icon] . Use the drop-down list box or the arrows to page through multiple pages of objects.

    ●   Open and select a specific page from the drop-down list box:

```
BEHEMOTH...  1-20/45  ▼
BEHEMOTH...  1-20/45
QA-TCL...  21-40/45
TS1-HP37...  41-45/45
```

- ● Click ◀ to go to the beginning of the list of objects.
- ● Click ◀ to go to the previous page in the list of objects.
- ● Click ▶ to go to the next page in the list of objects.
- ● Click ▶ to go to the last page in the list of objects.

■ Use the scroll bar to scroll to items not currently in view.

Workspace

The workspace is the main work area and will change based on your actions.

Radia Directory and Zone Objects

Once you are familiar with the Radia Management Portal user interface, you need to understand how to access the key areas of the infrastructure that you want to manage. However, first you must be familiar with the objects represented in a Radia Directory and Zone in the Radia Management Portal.

A tree view is used to organize these objects. The tree consists of the following icons, which represent the Zone Directory objects.

■ **Zone**
The Zone Directory contains all devices, infrastructure, and software that is managed and administered by the Radia Management Portal at this location. Other Radia Management Portal Zones are accessed from the connections available from the Zone Access Points container.

■ **Active Directory**
An Active Directory configured for access by a Radia Management Portal Administrator appears at the Directory level in the Workspace.

■ **Primary file**
The Primary file is a Primary file on a Radia Database on a Radia Configuration Server, whose Common Name has been assigned cn=primary. Use the RCS Administration Tasks from the Radia Management Portal to perform instance-level tasks on the Radia Database. To configure the Primary file, see *Adding a Directory Service* on page 143.

■ **Containers**
A **container** is a grouping of objects used to select a particular object type, or to limit the

scope of influence that an administrator can have over the entire infrastructure. The containers at the highest level of a Radia Zone are discussed in *About the Zone Containers* on page 97. All Zones include the same containers and container names. The procedures throughout the guide identify which containers to start from when performing any task.

- **Computer, Servers and Devices**

  A **server** is a physical device that is running a piece of the infrastructure (service) that you want to manage via the Radia Management Portal. A server must be addressable by an IP address. An example of a server would be an NT Server that is running a Radia Configuration Server.

  A **computer** is a physical device that exists in your infrastructure. If you want it managed by this Radia Management Portal Zone, you must specify **Manage Computer** to add it to the **Zone, Devices** container.

  A **Device** is a physical device that exists in the Devices container of the Zone, and is being managed from this Zone. **Devices** also have memberships in groups in the **Groups** container and the **Cross References** container.

- **Network**

  A network, such as Microsoft Windows Network, represents an external network directory that has been discovered by the Radia Management Portal. Objects in a network can be selected for management by this Radia Management Portal Zone.

- **Directory Service**

  External Services are defined to the Radia Management Portal Zone to enable a connection to that service from within the Radia Management Portal. An Active Directory, the Radia Database on the Radia Configuration Server, and other LDAP directories can be configured for access from the **Directory Service** container.

- **Services**

  A **service** is an application running on a server such as a Radia Configuration Server or Radia Proxy Server.

About the Zone Containers

This topic defines the Radia Management Portal Zone Containers that are directly beneath the Zone node. Containers designated as *self managed* are directory areas where no administrative operations are performed.

Figure 3.29 ~ Zone Containers.

> **Note**
>
> Numerous containers and objects are new to this release to enable users to do the following:
>
> - Perform operations against groups that are automatically created and managed by the Radia Management Portal (based on known hardware, software, and managed service information for the devices)
>
> - Establish multiple zones in an enterprise, with the ability to access remote zones and perform operations against remote zone device groups.
>
> - Access the Radia Configuration Server and administer services and policy at the instance-level. Apply Policy using an LDAP directory, such as Active Directory.
>
> - Connect to and browse entries in an external LDAP directory, such as Active Directory.
>
> - Connect to and browse your existing network directories.

- **Administrators and Operators Container (cn=USER)**
  The Administrators and Operators Container is the default, built-in source for authenticating users of the Radia Management Portal and specifying which tasks they are entitled to perform. There are separate user groups for Operators and Auditors, as well as Administrators of the Radia Management Portal, Accounts, Infrastructure, the Network, Packages, Policy, Services, and the Radia Configuration Server.

- **Configuration Container (cn=config)**
  The Configuration container holds the start-up configuration of the Radia Management Portal zone for both internal and external objects and mount points. All objects in the previous containers are "mounted" as directories when the zone is started.

  Directory objects that are defined and mounted from the Configuration container include:

  ● Entitlements for Delegated Administrators

  ● Radia Management Portal Task Groups and Tasks

- Radia Products, Client Installs, and Profiles
- Directory Services
- Primary file in the RCS database (cn=primary,cn=config)

■ **Directory Services Container** (cn=ds, cn=config)
The Directory Services container is one of the Configuration containers. It defines the external directory services and mount points the zone is to connect with automatically at startup, or make available for connection during operation. Use this container to define access to other LDAP directory services in your enterprise, such as Active Directory, as well as access to the Primary file on the Radia Configuration Server database. Additional Radia Databases can also be defined for access from this container.

The delivered zone template automatically defines configurations for the following mount points:

- Domain Name System (DNS)
- Windows Networking
- Radia Messaging

■ **Cross-References (cn=xref)** *Self Managed*
The Cross References container is a self-managed container of automatically-generated device groups. The groups are created once the Radia Management Agent is installed on the computers in your Devices container. The Cross References container creates and maintains the memberships for all devices according to the following classifications, using information passed from the Radia Management Agent to the Radia Management Portal for all devices under a zone's management:

- **Device Manufacturers** – For example, Hewlett-Packard, Dell, and Gateway device groups.
- **Infrastructure Services** – For example, Radia Proxy Server, Radia Management Agent, and Radia Configuration Server device groups.
- **Managed Services** – For example, groups for each service being managed on devices through the Radia Application Manager or Radia Software Manager.
- **Operating Systems** – For example, Windows XP. Within a specific operating system group are sub-groups for Service Pack levels, as shown in the following figure:

Figure 3.30 ~ Location of Group for Windows XP, SP1 devices in Cross-Reference Container.

- **Subnets** – For example, Subnet 16 groups all devices whose IP addresses are on that subnet.

■ **Devices Container (cn=device)** *Self Managed*
The Devices container holds the object properties for all devices being managed by this Radia Management Portal Zone. Entries are automatically created in this container when other operations are performed, such as adding a device to a group in the Ggroups container or selecting Manage Computer from a computer object in your network.

Devices in this container have *memberships* in other containers. For example, each device must have membership in at least one group in the **Group** container to facilitate operations. In addition, devices have *automatic membership* in various **Cross-Reference** container entries, based on what hardware, software, managed services, and Radia Infrastructure they contain.

■ **Groups Container (cn=group)**
Most Radia Management Portal Operations are performed against groups of devices, as opposed to individual devices. The Group container holds the provided Default Group, as well as any groups you create. Devices hold memberships in at least one group, but as many as you choose. Operations scheduled against a specified target group will include the members of that group at the time the job runs. Groups can be defined with a hierarchy, such that Group A includes a set of devices as well as all devices that are members of GroupAA.

To schedule jobs against groups in more than one zone, you can establish same-named groups in the Groups container of each Zone, and then select the group for the operation.

■ **Jobs Container (cn=jobs)**
Holds the objects for jobs and job groups scheduled or recently run by the Radia Management Portal. Within the Jobs Container is the History container, holding daily records of completed jobs.

■ **Networks Container (cn=network)**
Container used to access the enterprise networks that have been configured as mount points from the Directory Services container, including DNS and Microsoft Windows Network. Networks are often used to access computers that need to be brought under management in the Radia Management Portal Zone.

■ **Zone Access Points Container (cn=zone-sap)**
Holds an entry for the current Zone and any remote zones in your enterprise that have been configured for access. From this container, you can use the Operations task to open a subordinate zone's Radia Management Portal, or schedule zone operations to launch jobs across multiple zones in your enterprise, at once.

Obtaining Descriptions using Details View

One of the easiest ways to become familiar with the Portal objects is to switch to **Details** view whenever you come across a new object. **Details** view includes a one-line **Description** of each object.

For example, Figure 3.31 on page 101 shows the descriptions available for the objects at the highest level of the **Directory**.

Figure 3.31 ~ Details View of *Directory* includes Descriptions.

Now that you are familiar with the Radia Management Portal user interface and the key containers in a Radia Zone, you are ready to begin managing your infrastructure.

■ To configure your Radia Management Portal Zone and bring devices under management, go to *Chapter 4: Administrative Functions*.

■ To perform operations on devices in your Radia Management Portal Zone, go to *Chapter 5: Operations Functions*.

■ To perform RCS Administration Tasks on the instances in the Radia Database, see *Using the RCS Administration Tasks*, on page 102.

■ To perform Policy using an LDAP directory, see *Using RMP to Assign Policy through an LDAP* Directory on page 111.

Using the RCS Administration Tasks

The Radia Management Portal contains several tasks, stored in the RCS Administration task group, that allow you to manipulate *instances* in the Radia Database.

Prerequisites

■ The Radia Configuration Server service must be started on the machine where you want to make changes.

■ A Radia Configuration Server directory service must be defined and the RMP must be connected to that directory service. For details, see the following topics in *Chapter 4: Administrative Functions*: *Adding a Directory Service* on page 143 and *Connecting to a Directory Service* on page 154.

About the RCS Administration Tasks

Use the **RCS Administration** task group to manage instances in the Radia Database.

Figure 3.32 ~ RCS Administration task group.

The following is a list of the RCS Administration tasks. Remember, the available tasks vary based on what you have selected in the navigation aid.

■ **Add Connections**
Click **Add Connections** to add connection(s) to the selected instance.

■ **Create**
Click **Create** to add a new instance to the current class. After adding the new instance, use

the Modify and Add Connections tasks to set the attributes and make connections for the instance.

■ **Copy**
Click **Copy** to create a copy of the selected instance.

■ **Delete**
Click **Delete** to remove the selected instance from the Radia Database.

■ **Modify**
Click **Modify** to modify the selected instance. Use the Advanced View in the Modify window to modify any attributes that you can modify from the System Explorer.

■ **Remove Connections**
Click **Remove Connections** to remove connection(s) from the selected instance.

Creating Instances

Use the **Create** task in the **RCS Administration** task group to add new instances to the selected class.

To add an instance

Use the navigation aid to go to the class where you want to add a new instance. For example, go to the Accounts class.

In the **RCS Administration** task group, click **Create**.

The **Create** window opens.

Figure 3.33 ~ Create window.

In the **Instance** text box, type a name for the new instance.

In the **Friendly Name** text box, type the display name for the instance.

Click **Create**.

The **Properties** window for the new instance opens.

Figure 3.34 ~ Properties window.

Adding Connections

Use the **Add Connections** task to add connections to the selected instance

To add a connection

Use the navigation aid to go to the instance for which you want to create a connection.

In the **RCS Administration** task group, click **Add Connections**.

The **Add Connections - Select** window opens. The fields in this window vary depending on the object that you have selected in the navigation aid.

Figure 3.35 ~ Add Connections window.

If necessary, use the **Type** drop-down list to select the type of connection that you want to make. The type of connection that you select determines which classes you will be able to select from the next drop-down list.

Figure 3.36 ~ Add Connections window – Class area.

From the **Class** drop-down list, select the class that you want to connect to.

The **Connections** area opens.

Figure 3.37 ~ Add connections window - Connections area.

From the **Available** list, select one or more instances.

Click to add the selected instances to the **Selected** list.

Click **Next**.

The **Add Connections - Summary** window opens.

Click **Commit**.

The **Properties** window opens and displays the new connections.

Copying Instances

Use the **Copy** task to create a copy of the selected instance.

To copy an instance

1. Use the navigation aid to go to the instance that you want to copy.

2. In the **RCS Administration** task group, click **Copy**.

The **Copy** window opens.

Figure 3.38 ~ Copy window.

3. In the **Instance** text box, type a name for the new instance.
4. In the **Friendly Name** text box, type the display name for the instance.
5. Click **Copy**.

   The **Properties** window for the new instance opens.

Deleting Instances

Use the **Delete** task to remove the selected instance from the Radia Database.

To delete an instance

1. Use the navigation aid to go to the instance that you want to delete.
2. In the **RCS Administration** task group, click **Delete**.

   The **Delete** window opens.

Figure 3.39 ~ Delete window.

3. Click ✔ to confirm that you want to remove the selected instance.

OR

Click ✖ to indicate that you do not want to remove the selected instance.

Modifying Instances

Use the **Modify** task to modify the selected instance.

To modify an instance

Use the navigation aid to go to the instance that you want to modify.

In the **RCS Administration** task group, click **Modify**.

The **Modify** window opens.

Figure 3.40 ~ Modify window.

Make any necessary changes.

Click **Modify**.

The **Properties** window opens.

Removing Connections

Use the **Remove Connections** task to remove connection(s) from the selected instance.

To remove a connection

Use the navigation aid to go to the instance for which you want to remove a connection.

In the **RCS Administration** task group, click **Remove Connections**.

The **Remove Connections** window opens.

Figure 3.41 ~ Remove Connections window.

From the **Available** list, select one or more instances.

Click ![button] to move the instances to the **Selected** list.

Click **Next**.

The **Summary** window opens.

Click **Commit**.

The **Properties** window opens and the connections are removed.

Using RMP to Assign Policy through an LDAP Directory

The Radia Management Portal contains several tasks used to assign and manage policy through an LDAP directory. Examples of LDAP directories include Active Directory and the Radia Management Portal, itself.

Prerequisites

■   A comprehensive understanding of the Policy Server and assigning policy.

■   A connection to the *primary* Radia Configuration Server service so you can access services.

> ### Note
>
> The *primary* Radia Configuration Server service must be defined in the Zone's Directory Services container with the Common Name of **primary**. See *Specifying RCS Directory Service Properties* on page 147 for more information.

■   A connection to the LDAP Directory service. See *Connecting to a Directory Service* on page 154 for more information.

■   The **Used for Policy** field in the directory service must be set to True. To do this, you must modify the Directory Service. See *Modifying Directory Service Properties* on page 151.

■   If you defined an LDAP Policy Extension with a prefix other than **edm** through the Radia Policy Manager, you must also define the custom policy prefix to the Radia Management Portal. This is done using the PREFIX parameter in the rmp.cfg file. See *Configuring for a Custom LDAP Policy Extension Prefix* on page 162 for more information.

> ### Caution
>
> Please use your discretion when performing Policy Tasks to which you are entitled. Assigning policy to an object in a directory does not guarantee that policy will be applied. For example, if the object containing policy information is not in the scope of your policy search (that is, the search is not going to traverse this object), the policy will not be picked up. See the *Radia Policy Server Guide* for additional information.

About the Policy Tasks

Use the **Policy** task group to assign policy using an LDAP directory, such as Active Directory or another LDAP directory.

Figure 3.42 ~ Policy task group.

The following is a list of the available Policy tasks. Remember, the available tasks vary based on your selected Authority.

■ **Add Policy Object**
Click **Add Policy Object** to create a new group or organizational unit in the LDAP directory.

■ **Modify Policies**
Click **Modify Policies** to assign services to the selected policy object.

■ **Modify Targets**
Click **Modify Targets** to specify members of a group to be targeted based on the policy assignments.

■ **Remove Policy Object**
Click **Remove Policy Object** to remove a group or organizational unit from the LDAP directory.

■ **Refresh Managed Services Cache**
Click **Refresh Managed Services Cache** to refresh the list of services displayed in the Radia Management Portal. This list is created from information in the Radia Database.

■ **Resolve Policy**
Click **Resolve Policy** to resolve the service entitlements for an object. The list is grouped by product type and then policy source, and may be viewed for a given domain filter (DNAME). For LDAP objects, you can add values for the attributes, such as Hostname, OS, UserID, and Context, which are normally available when the LDAP policy is resolved.

Adding a Policy Object

Use the **Add Policy Object** task to add a group or organizational unit.

To add a policy object

1. Use the navigation aid to go to the appropriate container in the directory service where you want to add a policy object.

Figure 3.43 ~ Navigate to the policy object.

2. In the Policy task group, click **Add Policy Object**.

The **Add Policy Object** window opens.

Figure 3.44 ~ Add Policy Object window.

3. From the **Type** drop-down menu, select Group or Organizational Unit.

The **Add Group** window opens.

Figure 3.45 ~ Add Group window.

4. In the **Common Name** text box, type a unique name for the policy object.
5. In the **Display Name** text box, type a name for the policy object that will appear in the RMP.
6. In the **Description** text box, type a description that will appear in the Details view.
   Click **Add**.
   The **Properties** window for the policy object opens.

Removing a Policy Object

Use the **Remove Policy Object** task to delete a group or organizational unit.

To remove a policy object

1. Use the navigation aid to go to the policy object that you want to delete.
2. In the Policy task group, click **Remove Policy Object**.
   The **Remove Group** window opens.

Figure 3.46 ~ Remove Group window.

3. Click ✔ to confirm that you want to remove the object.

   OR

   Click ✘ to indicate that you do not want to remove the object.

Modifying Policies

Use the **Modify Policies** task to assign services to the selected policy object.

To modify policies

Use the navigation aid to go to the policy object that you want to modify.

Figure 3.47 ~ Policy object selected.

In the **Policy** task group, click **Modify Policies**.

The **Modify Policy** window opens.

Figure 3.48 ~ Modify Policy window.

Use the **Modify Policies** window to modify existing policy or to select additional services to be assigned to the policy object. See ***Basic Procedures for Modifying Groups*** on page 166 for information on how to use this window. Within that section, see ***Using the Attribute Editor*** on page 172 for information on how to modify service attributes, and see ***Using the Expression Editor*** on page 176 for information on how to modify the constraints for a service using the expressions editor.

When you are done making changes, click **Commit**.

Modifying Targets

Use the **Modify Targets** task to specify members of a group to be targeted based on the policy assignments.

To modify targets

1. Use the navigation aid to go to the appropriate policy object.

Figure 3.49 ~ Policy object selected.

2. In the **Policy** task group, click **Modify Targets**.

The **Modify Policy Targets** window opens.

Figure 3.50 ~ Modify Policy Targets window.

3. Use the **Modify Policy Targets** window to select the appropriate targets. See *Basic Procedures for Modifying Groups* on page 166 for information on how to use this window.

4. When you are done making changes, click **Commit**.

Resolving Policy

Use the **Resolve Policy** task to view resulting policy entitlements for an object. You can limit the view to an established domain filter group by selecting a DNAME. You can also add values for input attributes that are normally available to the LDAP resolve method during an actual resolution, such as host computer, operating system, userID and Zcontext.

Note
If you customized the set of domain filters (DNAMEs) in the Radia Policy Manager configuration file (pm.cfg), you can also customize the domain filters available in the Resolve Policy task of the Radia Management Portal. See *Customizing Domain Filters (DNAMEs) in the Resolve Policy Task* on page 123 for details.

To resolve policy entitlements

1. Use the navigation aid to go to the appropriate policy object.

Figure 3.51 ~ Policy object selected.

2. In the **Policy** task group, click **Resolve Policy**.

The **Resolve Policy** window opens, displaying all policy entitlements for the object.

Figure 3.52 ~ Resolve Policy page with initial, unfiltered view.

The top area displays all Resultant Policies for the selected target object.

Upon initial display, Resultant Policies are grouped into categories such as Patch Management, OS Management, and Software Management. Within a category, the direct policy entitlements are listed first, followed by indirect policy entitlements attributable to group memberships.

The source of indirect entitlement are listed on the left column. Figure 3.53 shows the direct policies for Patch Management, followed by the indirect policies inherited for three groups. The policies for the 2nd and 3rd groups have been hidden from view.

Figure 3.53 ~ Resultant Policies by type (e.g.Patch Management) list direct and then indirect policies, by source.

- Click the ⊟ icon to hide policies inherited from that group.
- Click the ⊞ icon to view policies inherited from that group.
- Click on a group name to browse that object's properties.

3. Use the Attributes area on the lower half of the page to limit the resolution to a specific domain filter group, or to specify values for attributes normally available at the time of resolution. The attributes correlate to the in.<attribute> value normally passed from Radia to the LDAP Policy Adapter.

> **Note**
>
> If you customized the set of DNAMEs in your pm.cfg file, you can modify the Dname selection list values for the Resolve Policy task. See *Customizing Domain Filters (DNAMEs) in the Resolve Policy Task* on page 123 for more information.

- In the **Dname** drop-down list box, select an entry other than Unfiltered to view policy resolution for a specific domain filter group. Default domain filter groups include *, PATCH and OS, where * represents all domains other than PATCH and OS.

- In the **Host** text box, optionally type a host computer name to specify the value of the ⟨⟨in.host⟩⟩ attribute.

- In the **Uid** text box, optionally type a User ID to specify the value of the ⟨⟨in.uid⟩⟩ attribute.

- In the **Os** text box, optionally type an operating system name, such as Win32, to specify the value of the ⟨⟨in.os⟩⟩ attribute.

- In the **Zcontext** text box, optionally type M for machine or U for user to specify the context of the delivery option for applications configured to accommodate multiple users. This attribute represents the zservice.zcontext value in the Radia database.

4. To reference another input attribute for policy resolution, click the ⊕ on the bottom-right of the page. This adds a text box area for a new attribute name and value to the bottom of the Attributes list.

- In the left text box, type the new attribute name.

- In the right text-box, type the value for the new attribute. Enter quotes around values that include spaces.

Figure 3.54 ~ Specifying a new Attribute for the Policy Resolution.

5. After specifying Attributes for the policy resolution, click **Resolve** on the bottom of the page.

The Resultant Policies area displays the service entitlements for the object, given the selected Dname filter group and any input attribute values entered in the Attributes area.

Figure 3.55 ~ Viewing Policy Resolution for the OS Domain Filter Group and Win98 Operating System.

6. To exit the Resolve Policy page, click an entry in the Navigation area. This returns you to the selected object's properties page.

Customizing Domain Filters (DNAMEs) in the Resolve Policy Task

If you have modified the domain filter settings defined in your Radia Policy Manager pm.cfg file, you can port your modified filter settings to the Radia Management Portal. The modified filter settings will be available from the Dname drop-down list box on the Resolve Policy task page.

Domain filtering is defined in your Radia Policy Manager. Any custom filter settings must be properly defined in the Radia Policy Server configuration file, pm.cfg using the format:

```
DNAME=<DOMAIN NAME>    { rule }
```

> **Note**
>
> See *Appendix C:Domain Filtering* in the *Radia Policy Manager Guide* for details on domain filtering and syntax.

To port your custom domain filter settings to the Radia Management Portal Resolve Policy task you must modify the httpd.rc file, which is located in the etc directory of where the Radia Management Portal is installed. Add the following custom code to the end of the httpd.rc file using the format:

```
namespace eval policy {

    default cfg(DNAME=<DOMAIN NAME>)   { rule }

}
```

where DNAME=<DOMAIN NAME> and { rule } correspond to a custom filter setting in your pm.cfg file. *Figure 3.56 ~ Syntax to configure custom policy filters in the RMP httpd.rc file*, below, shows a sample code at the end of the httpd.rc file configured for custom policy filters. This example shows a modified definition for the default (*) filter as well as a new AUDIT filter.

```
namespace eval policy {

    default cfg(DNAME=*)        { * !PATCHMGR !OS !AUDIT}

    default cfg(DNAME=PATCH)    { PATCHMGR }

    default cfg(DNAME=OS)       { OS }

    default cfg(DNAME=AUDIT)    { AUDIT }

}
```

Figure 3.56 ~ Syntax to configure custom policy filters in the RMP httpd.rc file.

Save the changes to the httpd.rc file and restart the Radia Management Portal service. The modified filter settings will be available from the Dname drop-down list box on the Resolve Policy task.

Refreshing the Managed Services Cache

Use the Refresh Managed Services Cache task to periodically refresh the list of services displayed in the Radia Management Portal. This list is created from information in the Radia Database.

To refresh the managed services cache

1. Use the navigation aid to go to the Configuration container.

Figure 3.57 ~ Configuration container selected.

2. In the **Policy** task group, click **Refresh Managed Services Cache**.

About the Policy (Advanced) Tasks

Use the **Policy (Advanced)** task group to modify the Radia Policy attributes as described in the *Policy Server Guide*. These attributes are used to manage policy scope, relationships, and assignments.

Caution
Make sure that you have a good understanding of the Policy Server and the Radia Policy attributes before using these tasks.

The tasks available are:

■ **Modify Defaults**
Click Modify Defaults to set the defaults for the attributes in a service. Using this task modifies edmPolicyDefault. See the *Policy Server Guide* for details.

■ **Modify Dependencies**
Click **Modify Dependencies** to modify policy links. Using this task modifies the edmLink attribute. See the *Policy Server Guide* for details.

■ **Modify Flags**
Click **Modify Flags** to limit the scope of policy resolution for specific objects. Using this task modifies the edmFlags attribute. See the *Policy Server Guide* for details.

■ **Modify Overrides**
Click **Modify Overrides** to bypass the pre-set values of one or more attributes for a service and specify alternate values. Using this task modifies the edmPolicyOverride attribute. See the *Policy Server Guide* for details.

Modifying Dependencies

Use the **Modify Dependencies** task to modify policy links. Using this task modifies the edmLink attribute. See the *Policy Server Guide* for details.

Caution
This task allows you to create relationships in addition to your parent and group relationships. It is recommended that you use this task sparingly.

Example

Jennifer Blake is part of the Marketing group, which falls under the Sales organization. Jennifer and the rest of the Marketing group use different machines than the rest of the company. Therefore, the Marketing group must receive several services that are specifically for HP Compaq

Notebook nc6000 machines. The following example shows how to create a dependency (also called a link) from the Marketing group to the HP Compaq Notebook nc6000 group.

To modify a dependency

Use the navigation aid to go to the group for which you want to modify a policy link, such as Marketing.

Figure 3.58 ~ Select a group.

In the **Policy (Advanced)** task group, click **Modify Dependencies**.

The **Modify Policy Dependencies** window opens.

Figure 3.59 ~ Modify Policy Dependencies window.

Use this window to select the policy link. See *Basic Procedures for Modifying Groups* on page 166 for information about how to use this window.

Figure 3.60 ~ Modify Policy Dependencies window.

If you want to add any additional constraints use the Expression Editor. See *Using the Expression Editor* on page 176 for more information about how to use this window and the *Policy Server Guide* for more information about expressions.

Click **Commit** to save the changes to the policy dependencies.

Modifying Flags

Use the **Modify Flags** task to limit the scope of policy resolution for specific objects. Using this task modifies the edmFlags attribute. See the *Policy Server Guide* for details.

Example

In your organization, the Marketing group is typically a member of Sales. However, the Marketing group should receive the same software applications as Sales. Therefore, you may want to set up a flag that limits policy resolution for the Marketing group.

To modify flags

Use the navigation aid to go to the policy object for which you want to limit the scope of policy resolution.

In the Policy (Advanced) task group, click **Modify Flags**.

Figure 3.61 ~ Modify Policy Flags window.

Select the appropriate check box.

- **Secede**
  Instructs the Policy Server not to include any parent objects in the outcome.

- **Continue**
  Instructs the Policy Server to ignore all other attributes in this object. The parent object is still processed unless Secede is selected.

- **Break**
  Instructs the Policy Server to abort resolution and return the condition to the client. The client device should not apply policy.

- **Strict**
  Instructs the Policy Server to ignore 'memberOf' attributes and only process edmFlags, edmPolicy and edmLink.

Click ✔ to accept the changes.

Click **Commit**.

Modifying Defaults

Use the **Modify Defaults** task to set the defaults for the attributes, such as version, in a service. Using this task modifies edmPolicyDefault. See the *Policy Server Guide* for details.

Example

If the Sales application does not have a version specified, you can use this task to specify the default version to be deployed to the target machines.

To modify defaults

Use the navigation aid to go to the appropriate policy object.

In the **Policy (Advanced)** task group, click **Modify Defaults**.

The **Modify Policy Defaults** window opens.

Figure 3.62 ~ Modify Policy Defaults window.

Use this window to select the service whose attributes you want to define. See *Basic Procedures for Modifying Groups* on page for information about how to use this window.

Once you have selected a service, use the Attribute Editor to specify the default values. See *Using the Attribute Editor* on page 172 for information about how to use this editor and the *Policy Server Guide* for details about attributes.

Use the Expression Editor to specify any additional constraints. See *Using the Expression Editor* on page 176 for information about how to use this editor and the *Policy Server Guide* for details about expressions.

Modifying Overrides

Use the **Modify Overrides** task to bypass the pre-set values of one or more attributes for a service and specify alternate values. Using this task modifies the edmPolicyOverride attribute. See the *Policy Server Guide* for details.

Example

Bob Smith is entitled to the Sales application, version 1. You can use this task to override the version information for Bob alone, and entitle him to version 2.

To modify overrides

Use the navigation aid to go to the appropriate policy object.

In the **Policy (Advanced)** task group, click **Modify Overrides**.

The **Modify Policy Overrides** window opens.

Figure 3.63 ~ Modify Policy Overrides window.

Use this window to select the service whose overrides you want to define. See *Basic Procedures for Modifying Groups* for information about how to use this window.

Once you have selected a service, use the Attribute Editor to specify the override values. See *Using the Attribute Editor* on page 172 for information about how to use this editor and the *Policy Server Guide* for details about attributes.

Use the Expression Editor to specify any additional constraints. See *Using the Expression Editor* on page 176 for information about how to use this editor and the *Policy Server Guide* for details about expressions.

Summary

- The Radia Management Portal has a consistent user interface, which means that you can follow the same basic procedure to complete any task.

- The Radia Management Portal user interface has a banner area, navigation aid, taskbar, toolbar, and workspace.

- The previous Authority area is now renamed the Navigation area. There are two Navigation modes: Navigation (History) — which traces your Portal navigation path during a session, and Navigation (Location)—which shows the directory path of your current location. You can switch between the two Navigation modes using the icon included in the Navigation title bar.

- Your initial login authority is the Desktop area, which contains links to the Portal Directory and your Radia Zone, by default. You can add or remove Shortcuts to your Desktop that link to frequently used navigation locations.

- The Radia Management Portal tasks are maintained in task groups that reflect their function. The task groups and tasks available at any time vary based on your assigned role as well as your current navigation location.

- The Radia Management Portal Zone is composed of containers. Navigate to the appropriate container and location to perform tasks related to the objects stored in each container.

- The Radia Management Portal contains several tasks, stored in the RCS Administration task group, that allow you to manipulate *instances* in the Radia Database.

- The Radia Management Portal contains several tasks used to assign and manage policy through LDAP directories. These tasks are available from the Policy and Policy (Advanced) task groups.

4

Administrative Functions

At the end of this chapter, you will:

■ Be able to configure the Radia Management Portal Zone for Network Discovery and Directory Services.

■ Be able to connect to and disconnect from a Directory Service or RCS Primary Database, or other object defined in the Directory Services container.

■ Understand the various methods of bringing devices under management by a Radia Management Portal Zone.

■ Be able to create groups of devices for performing operations, and know how to add, move, copy or import devices into the groups.

■ Be able to create and configure delegated administration roles, and add administrators and operators to the Radia Management Portal Directory.

■ Be able to manage the Radia Management Portal Zone Directory using Backup, Restore, Import, and Export tasks.

■ Be able to view and manage active Jobs, and view executed jobs from the Job History container.

■ Be able to view the properties for any object in the Radia Management Portal.

Several administrative functions are available for configuring and managing your organization's infrastructure from the Radia Management Portal. Administrative functions allow you to prepare your Radia Management Portal for use by the administrators and operators in your organization, as well as to handle general administrative functions such as creating a backup of the Radia Management Portal Directory.

New for this release is the configuration of Directory Services to allow users access to the RCS Primary file and your existing LDAP directories, such as Active Directory for Policy administration. For details, see *Configuring Directory Services* on page 143.

Also new for this release are the containers and tasks used to bring devices under management by the Radia Management Portal Zone. For details, see *Establishing Devices and Device Groups* on page 165.

Configuring a Radia Management Portal Zone

Following installation, you need to add the following objects to a zone's infrastructure in order to use various new features.

- **Directory Services**
  Add a Directory Service object for each outside directory to which you want the Radia Management Portal to be able to connect, such as the Primary file on your Radia Configuration Server or an existing LDAP Directory in your enterprise.

- **Network Discovery and Mount Points**
  The Radia Management Portal is configured to connect to a set of network directories in your enterprise through mount points. The definitions are also found in the Directory Services container, where the startup can be changed from automatic to manual, if desired.

- **Groups** (of Devices)
  Almost all operations in this release are performed using device Groups. The devices that are imported or added to a specific Radia Management Portal Zone can be further clustered into different Groups to expedite common operations.

- **Subordinate Zones**
  From the initial Radia Management Portal, run the **Install Zone** task to remotely install subordinate zones in your enterprise, each with a unique name. All zones retain an entry in the Zone Access Points container, which can be used to schedule Zone Operations on devices in all zones in your enterprise.

- **Task Templates**
  Task templates need to be added before scheduling jobs for Zone Operations.

- **Cross Reference Container**
  The groups in the Cross Reference container are self-managed. They are automatically created after the Radia Management Agent is installed on devices in the Device container, and dynamically maintained.

Understanding Network Discovery

The Radia Management Portal runs the network discovery job, NETSCAN, upon startup and at regular intervals to automatically discover the resources on your network. The discovered objects are placed in the appropriate network container in the Zone's **Networks** location, where they can be selected for management by the Radia Management Portal Zone.

To view the network containers of discovered objects in the Radia Management Portal, use the **Navigation Location** aid to go to the **Zone** container, and then click **Networks**.

Figure 4.1 ~ Networks container includes discovered Networks.

To view the objects discovered in a specific network, navigate to the Networks container and then click the network in the Workspace. For example:

■ Click **Microsoft Windows Network (cn=lanmanredirector)** to view the Windows devices that you can manage.

■ Click **Netware or Compatible Networks (cn=nrnwk)** to view Netware devices that you can manage.

Figure 4.2 ~ Objects discovered in a Domain of the Microsoft Windows Network.

Configuring Network Discovery

In some environments, you may want to configure your network discovery so that you have more control over network discovery, especially in environments with large networks.

Each time the network discovery job runs, newly discovered objects are added to the Networks container. Additional Network Discovery jobs will only add objects to previously discovered Networks containers, not remove them.

To configure network discovery

Stop the **Radia Integration Server** service.

Use a text editor to open the Radia Management Portal configuration file, rmp.cfg, located by default in **SystemDrive:\Novadigm\IntegrationServer\etc**.

```
#
# Copyright (C) 1997-2001 HP.  All Rights Reserved.
#
# $Header: /cvs/nvd/rmp/default.rc,v 1.6 2002/02/01 17:56:24 Exp $
#
#
# RMP Module (Radia Management Portal)
#

# This section provides the core configuration for the
# RMP Sub-system. Please take care when hand-editing this.
#
rmp::init {
     URL              /          Insert Network Discovery configuration parameters here.

     }
#
# END OF CONFIG
#
```

Figure 4.3 ~ Sample default rmp.cfg file.

You can insert any of the parameters in *Table 4.1 ~ Parameters to Configure Network Discovery* on page 140 into this file before the finishing curly bracket (}) as shown in *Figure 4.3 ~ Sample default rmp.cfg* file above.

Use a space to separate the parameter and its value.

Table 4.1 ~ Parameters to Configure Network Discovery

Parameters	Explanation
NETSCAN	Enables or disables network discovery. Default is enabled. • Type NETSCAN 0 to disable network discovery. • Type NETSCAN 1 to enable network discovery.
NETSCAN_START_DELAY	The time to wait (in seconds) before starting network discovery when the Radia Management Portal starts up. Default is 15 minutes or 900 seconds. You can specify this value as: NETSCAN_START_DELAY 900 Another way to specify this value is by using a Tcl expression, which would read as follows: NETSCAN_START_DELAY {15*60} where 15 is the number of minutes. When multiplied by 60 seconds, the value becomes 900 seconds.
NETSCAN_POLL	Network Discovery Interval (in seconds). Default setting is 86400 seconds, or 24 hours. Optionally, specify this value using a Tcl expression in curly brackets. For example: to specify 12 hours, enter: NETSCAN_POLL {12*60*60} where 12 is the number of hours, multiplied by 60 minutes, multiplied by 60 seconds.
NETSCAN_INCLUDE	For each object class specified, limits network discovery to only those objects named in the include list. Default is to include all discovered objects in all classes within the network. Use the following syntax: NETSCAN_INCLUDE { *object_class* {*object_list*} object_classn {object_list} } *where:* *object_class* is a class whose discovered objects are to be restricted to the members specified in the following object list. Valid object classes include, but are not limited to: network, tree, domain, computer. Your network may include other classes. Tip: Any object's class is listed when you hover the mouse pointer over its icon. *object_list* is a space-separated list of common names within curly brackets. These are the only objects to be **included** in network discovery for the given object class. Unnamed objects in the specified class are **excluded.** All names are case insensitive. Example: The following limits discovery to all objects found in the 2 listed domains in the Microsoft Windows Network. No other networks will be discovered. NETSCAN_INCLUDE { network {lanmanredirector} ↵ domain {domain1 domain2} } For additional examples, see *Using NETSCAN_INCLUDE to Limit Network Discovery* on page 141.

Save and close the file.

Restart the Radia Integration Server and open the Radia Management Portal.

Using NETSCAN_INCLUDE to Limit Network Discovery

The NETSCAN_INCLUDE {} parameter allows you to restrict network discovery of the objects and object classes in your network. It is very powerful, and can be extremely restrictive.

For general syntax, refer to the NETSCAN_INCLUDE entry in *Table 4.1 ~ Parameters to Configure Network Discovery*.

When using NETSCAN_INCLUDE, be aware of the following implications:

Classes are hierarchical, and the include lists are processed for higher-level classes before lower-level classes. For example, the network class include list is processed before the domain include list.

---

network

domain

computer

Figure 4.4 ~ Sample Microsoft Windows Network object class hierarchy.

For a given class, if a class is not named in a NETWORK_INCLUDE list, all objects are included. (This is subject to limits already processed for a higher-class object, discussed in step 3 below.)

Once you limit objects of a given class in a NETWORK_INCLUDE list, you are also EXCLUDING the unnamed objects of the same class. In addition, you are also EXCLUDING all lower-class objects contained in the excluded branches.

For example, including a domain list by definition EXCLUDES all domains in the network that are not listed. All computers contained in the excluded domains ARE ALSO EXCLUDED.

Examples:

Use the following examples as reference when coding your own NETSCAN_INCLUDE lists.

`NETSCAN_INCLUDE {}`

Discover all objects in the network. **Default.**

`NETSCAN_INCLUDE { network {lanmanredirector}}`

Limits discovery to the lanmanredirector network. (Lanmanredirector is the common name for Microsoft Windows Network.) No other network will be discovered. All the objects under lanmanredirector will be discovered.

```
NETSCAN_INCLUDE { computer {gta02 vhr01 kwo04 jra06} }
```
Limits discovery of computer objects to the four computers in the list: gta02, vhr01, kwo04, and jra06. Discovers all network objects that are not computers.

```
NETSCAN_INCLUDE { domain {Novad} computer {gta02 vhr01 kwo04 jra06} }
```
Discovers all network objects that are not domains or computer objects. Discovers any of the computers listed **if** they exist in the domain Novad. No other computers will be discovered.

Setting Additional Configuration Parameters

Separate topics discuss how to modify the rmp.cfg file for network discovery (see page 138) or LDAP authentication (see page 159).

Table 4.2, below, lists the parameters you can add to the RMP.CFG file for options that are not related to either of these topics. Refer to the procedure *To configure network discovery* on page 138 for detailed steps on how to modify parameters in the rmp.cfg file.

Table 4.2 ~ Additonal RMP Configuration Parameters	
Parameters	**Explanation**
USE_FQDNSHOST_NAME	Specifies that RMP should contact remote hosts using either fully qualified domain names or short names (that is, the left-most portion of a fully qualified domain name). Customers whose DNS tables contain imperfect entries may want to switch to the use of short names. Sample operations that involve contacting a remote host include a Notify, a Proxy preload or purge, stopping or starting services via the RMA, and contacting the RMA. - Type USE_FQDNSHOST_NAME 0 to use short names (that is, the left-most portion of a fully qualified name). Customers whose DNS tables contain imperfect entries may want to switch to the use of short names. - Type USE_FQDNSHOST_NAME 1 to return to the use of fully qualified domain names (the Default).
WOL_MCAST_ADDR	Permits Wake-on-LAN (WOL) support in multicast-enabled environments. Default is no support for multicast WOL. - Type WOL_MCAST_ADDR \<IP_address\> where the \<IP address\> specifies the multicast address to use to revolve a WOL request. - Type WOL_MCAST_ADDR 0 to return to standard WOL support (no multicast WOL support). This is the default.

Configuring Directory Services

The Zone Configuration container includes the Directory Services container. This is where an Administrator can define, configure, and connect to or disconnect from another Directory Service, including the Radia Configuration Server PRIMARY database and an Active Directory service in your enterprise. For details, see the following topic *Adding a Directory Service*.

Figure 4.5 ~ Directory Services Container Location.

Adding a Directory Service

Use the **Add Directory Service** task from the Directory Services container to define a connection from the Radia Management Portal's Zone directory service to another directory service. You can add one of the following types of directory services to your RMP zone:

■   **LDAP**
   Use this type to connect to another LDAP directory, such as Microsoft Active Directory, DNS, or Netscape Iplanet.

■   **RCS**
   Use this type to connect a Radia Configuration Server and access the PRIMARY file in the Radia Database.

■   **DSML**
   Use this type to connect to another Radia Management Portal zone in your enterprise or a Radia Information Base (RIB) service. (Note: If you use the Install RMP task, this entry is created automatically.)

■   **MK**
   Advanced users who have created a custom metakit container for the zone directory service may use this type to extend the capabilities of the Radia Management Portal.

When you define properties for a Directory Service connection, you need to specify:

■   The *mount point*. This is the highest level of the directory structure to which you will be connecting. You can browse to a lower level, but not higher. For example, you can define a

connection to the highest level of an Active Directory, or to a specific organizational unit within the structure.

■   The login credentials for access. These credentials will be passed whenever a connection is made.

■   Whether the connection should be automatic, manual, or disabled upon future Radia Management Portal startups.

   ●   A manual connection requires the user to connect each time they want to access the defined directory. For details, see *To connect to a predefined Directory Service* on page 191.

   ●   A disabled connection requires an administrator to set the connection to manual or automatic before anyone can access the defined directory. For details, see *Modifying Directory Service Properties* on page 191.

To add a directory service

Navigate to the Directory Services container. It is located within the Zone Configuration container, as shown in the following figure.

Figure 4.6 ~ Location for adding a directory service.

Click **Add Directory Service** from the Model Administration task group.

The **Add Directory Service** page opens, where you specify the properties.

Begin by selecting the **Type** of directory service from the **Type** drop-down list.

Table 4.3 ~ Adding a Directory Service by Type

Select Type	Added Directory Service
ds-dsml	DSML: an external Directory Service, such as a RIB or another RMP Zone.
ds-ldap	LDAP: an LDAP Directory Service, including Active Directory.
ds-mk	MK: a custom-built Zone Metakit Container (Advanced Users only).
ds-rcs	RCS: A Radia Configuration Service, which hosts the Radia Database. **Note:** The RCS defined with cn=primary

Once the Type is selected, the Directory Service Properties page shows the set of properties and any defaults specific to that type. For details on specifying the properties, see the following topics:

- *Specifying LDAP Directory Service Properties*
- *Specifying RCS Directory Service Properties*
- *Specifying DSML Directory Service Properties*
- *Specifying Metakit Directory Service Properties*

After entering all properties, click **Submit**.

The Directory Service definition is added to the Directory Services container. To connect to the service, see the topic: *Connecting to a Directory Service.*

Specifying LDAP Directory Service Properties

To complete the Directory Service Properties for a Type of ds-ldap (LDAP and AD), use the following table:

Table 4.4 ~ Directory Service Properties for Type = ds-ldap

Field	Description
Common Name	Common name for the Directory Service. Must be unique among Directory Service objects and follow X500 standards. **Example:** eng.acme.com is assigned to the LDAP Directory Service known as dc=eng,dc=acme,dc=com
Display Name	Display Name of the object in the Directory Service container.
Description	Description of this Directory Service.

Table 4.4 ~ Directory Service Properties for Type = ds-ldap	
Field	**Description**
Startup	Select auto, manual, or disabled.
	Auto
	Specifies the connection to this Directory Service will be automatic when the RMP Zone starts up.
	Manual
	Specifies the connection to this Directory Service requires an Administrator or user to use the "Connect to Directory Service" task to connect during an RMP session.
	Disabled
	Restricts any connection to this Directory Service. The startup must be changed to auto or manual before anyone can connect to this Directory Service during a session.
Type	**ds-ldap**
	Type required for an LDAP directory service.
URL (Web Page Address)	Format:
	ldap://<IP address or qualified computer name>:389/ <qualified_Username>
	Examples:
	ldap://10.10.10.1:389/administrator@eng.acme.com
	ldap://usa.mycompany.com:389/admin@usa.mycompany.com
Password	Password for the username entered in the URL
Used for Policy	Default: false
	False
	indicates this LDAP directory service is not to be used for policy tasks.
	True
	enables the use of this Directory Service for all policy tasks. To set this field, use the **Modify** task.
Use	Specifies a fully-qualified domain at which to mount the directory service. This mount point becomes the highest level of the directory structure that can be accessed from the Radia Management Portal. For example, to mount and limit the use of the eng.acme.com directory to the Computers domain, specify the properties for this Directory Service with a Use value of:
	cn=computers,dc=eng,dc=acme,dc=com
	If left blank, the common name is used to mount the directory service at the highest level.

Click **Submit** to enter this Directory Service definition.

The following figure shows a sample set of directory service properties for accessing an LDAP directory service.

Figure 4.7 ~ Sample Directory Service Properties to add an LDAP Directory Service

> **Notes:**
>
> **1.** To specify an LDAP Directory Service being used for policy, see *Modifying Directory Service Properties* on page 151.
>
> **2.** To specify an LDAP Directory Service being used for Policy but with an LDAP policy extension prefix other than edm, also see *Configuring for a Custom LDAP Policy Extension Prefix* on page 162.

Specifying RCS Directory Service Properties

Refer to the following table to complete the Directory Service Properties for an RCS Directory Service connection.

Table 4.5 ~ Directory Service Properties for Type = ds-rcs

Field	Description
Common Name	Default: **primary**
	If primary exists, default is RCS*n*.
	Required. Must be unique among Directory Service objects and follow X500 naming standards.
	Multiple RCSs may be defined as Directory Service objects. However, only the RCS defined with the Common Name of **primary** has its services made accessible to the Policy and Advanced Policy tasks.
Display Name	Display Name of the object
Description	Description of this Directory Service
Startup	Select auto, manual, or disabled.
	Auto
	Specifies the connection to this Directory Service will be automatic when the RMP Zone starts up.
	Manual
	Specifies the connection to this Directory Service requires an Administrator or user to use the "Connect to Directory Service" task to connect during an RMP session.
	Disabled
	Restricts any connection to this Directory Service. The startup must be changed to auto or manual before anyone can connect to this Directory Service during a session.
Type	**ds-rcs**
	Type required to connect to a Radia Configuration Server directory service.
URL (Web Page Address)	Default entry:
	rcs://localhost:3464/RAD_MAST
	Format:
	rcs://<hostname or IP address>:<port #>/<Username>
	Example:
	rcs://myserver600:3464/RAD_MAST
	Change <localhost> to specify the qualified host name or IP address of your Radia Configuration Server, and if necessary, change the Username from the RAD_MAST default to the one used at your installation. The port number is normally 3464.
Password	Password for the username entered in the URL.
Path (see Modify task)	Optional entry for expediting a connection to the RCS Primary file.
	Specifies the fully qualified path of ZTOPTASK.EXE on the RCS. For example:
	C:/Novadigm/ConfigurationServer/bin/ztoptask.exe

Table 4.5 ~ Directory Service Properties for Type = ds-rcs

Field	Description
DS Prefix	Default for primary: cn=config,cn=<zone name>,cn=radia
	Instructs the Radia Management Portal where to mount the RCS Primary file. Leave the default as is if this RCS is the Primary Database for the Zone and is to be used for LDAP policy assignment.
	When defining an additional, non-primary RCS as a Directory Service, specify a DS Prefix that mounts it under the ZTOPTASK Service object for the Device hosting the RCS. For example:
	cn=ztoptask,cn=<device_of cn>,cn=device,cn=<zone name>,cn=radia
	See *To connect to a service defined for a Device* on page 155 for more information on how to do this automatically.
Timeout	Default: 0
	Leave **0** to never have an RCS connection timeout. To have the RCS connection timeout after a specific period of inactivity, enter the timeout period in seconds in this field.

Click **Submit** to enter this Directory Service definition.

The following figure shows a sample set of directory service properties for accessing the Radia Database Primary file on a Radia Configuration Server.

Figure 4.8 ~ Sample Directory Service Properties for an RCS.

Specifying DSML Directory Service Properties

Directory Service Properties for a DSML connection are specified the same as for LDAP. The only difference is the format of the URL entry, which begins with **dsml:** instead of **ldap:**. DSML connections may be defined to connect to another RMP Zone, or to a Radia Information Base (RIB) directory service.

Specifying Metakit Directory Service Properties

Advanced users can extend the capabilities of their Radia Management Portal Zone by adding another Directory Service container to the Zone. Each container in a Zone is loaded as a directory service upon Zone startup using a template (*.tmpl) file, LDAP data interchange file (*.ldif) file, and metakit (*.mk) file.

If you have a customized directory service, add a Directory Service definition for the *.mk file. Refer to the following table for guidance on specifying Directory Service properties.

Note

Examples of ds-mk directory services include the Radia Management Portal's own directory service mount points. For examples, refer to the Tasks, Jobs, and Users directory service mount points located in the Zone, Configuration, Management Portal container.

Table 4.6 ~ Directory Service Properties for Type = ds-mk

Field	Description
Common Name	Common name for the Directory Service. Must be unique among Directory Service objects and follow X500 standards. **Example:** zone/config/tasks
Display Name	Display Name of the Directory Service object. **Example:** Mount Point: Tasks
Description	Description of this Directory Service or mount point.

Table 4.6 ~ Directory Service Properties for Type = ds-mk	
Field	**Description**
Startup	Select auto, manual, or disabled.
	Auto Specifies the connection to or mounting of this Directory Service will be automatic when the RMP Zone starts up.
	Manual Specifies the connection to or mounting of this Directory Service requires an Administrator or user to use the "Connect to Directory Service" task to connect during an RMP session.
	Disabled Restricts any connection to or mounting of this Directory Service. The startup must be changed to auto or manual before anyone can connect to this Directory Service during a session.
Type	**ds-mk** Type required to connect to a custom metakit directory service.
Use	Overrides the common name.
Template	Specifies the template file needed for the directory service. **Example:** <<module.curpath>>/etc/task.ldif

Click **Submit** to enter this Directory Service definition.

Modifying Directory Service Properties

Use the **Modify** task in the **Model Administration** task group to change the properties of a Directory Service connection defined in your Zone's Directory Services container, such as the startup mode or the flag indicating whether or not an LDAP connection is being used for Policy.

To modify a Directory Service Property

Display the Directory Service Properties for the service you want to modify.

To navigate to a Directory Service Properties page, click on the **Zone** container, **Configuration** container, **Directory Services** container, and then select the Directory Service object.

Click **Modify** from the Model Administration task group.

The Modify page for the specific object type opens. Figure 4.9 shows a sample Modify LDAP page.

Figure 4.9 ~ Sample Modify LDAP page.

Change any entries to reflect the modified properties. For details on these fields, refer to the appropriate table in the topic *Adding a Directory Service*.

If this Directory Service is being used for Policy Administration, open the drop-down list next to the **Use for Policy** field, and click **true**. This setting enables the use of all policy tasks for this Directory Service.

> **Note**
>
> If the LDAP Directory Service is being used for policy but with a custom policy prefix (that is, other than edm as in edmPolicy), you must specify the custom prefix using the PREFIX parameter in the rmp.cfg file. See *Configuring for a Custom LDAP Policy Extension Prefix* on page 162 for more information.

To save the property changes, click **Modify**. The Directory Service Properties page opens and displays the modified properties.

Or to cancel any changes you made to the properties, click **Reset**. To exit the Modify page, click **Cancel**.

Removing a Directory Service

Use the **Remove** task from the **Model Administration** task group to remove a defined connection to a Directory Service.

Tip
As an alternative to removing a Directory Service entry, you can want to disable it from use. To do this, use the Modify task and set the Startup field to **disabled**.

To remove a Directory Service object

Warning
If you remove a directory service that is in use by another user, the user will be redirected to a parent object and receive an error message.

Follow the same steps as removing any object from the Radia Management Portal:

Display the object properties by navigating to the **Zone**, **Configuration**, **Directory Services** container, and click on the directory service to be removed.

Click **Remove** from the Model Administration task group.

The Remove Directory Service dialog asks you to confirm this delete.

Click the green check mark to confirm the delete, or the red X to cancel the delete.

Connecting to a Directory Service

Use the **Connect to Directory Service** task in the **Infrastructure** task group to connect to an external directory service or network mount point.

■ To connect to a Directory Service that has been defined in the Zone Configuration container, use the procedure starting below. This is needed when the Directory Service is newly defined, or defined with a startup mode of manual or disabled.

■ To connect to a Directory Service from its entry in the Devices container, use the procedure starting on page 155. This access will prompt you to add the service to the Directory Services container if it does not currently exist there.

For details on defining or modifying a directory service mount point, see Adding a Directory Service on page 143 or *Modifying Directory Service Properties* on page 151.

To connect to a predefined Directory Service

Display the Directory Service Properties for the service with which you want to connect.

To navigate to a Directory Service Properties page, go to the **Zone Configuration** container and click **Directory Services**. In the Workspace, click the Directory Service object.

Figure 4.10 ~ Connect to a Directory Service or RCS database.

Click the **Connect to Directory Service** task within the **Infrastructure** task group.

The connection is initiated immediately. The Workspace displays the objects at the highest level of the directory defined by the connection mount point.

Your navigation location changes to where that type of directory service is accessed, and the tasks available for working with the objects also display as you navigate through the structure. See the following table for a list of where each type of Directory Service is accessed from in the Directory.

Table 4.7 ~ Locations for Accessing Directories and Mount Points

Object	Directory Locations
Active Directory, other LDAP Directory	Directory level – same level as Zone
Primary file of RCS	Zone, Configuration, Primary object
Network mount point	Zone, Networks container
DSML (Subordinate Zone or RIB)	Zone, Zone Access Points container
Metakit directory service (Advanced User)	Defined by Template

Figure 4.11 shows a sample connection to an RCS Database.

Figure 4.11 ~ Accessing the Primary RCS Database from an RMP Zone.

To connect to a service defined for a Device

Use the **Navigation aid** to go to the **Zone Devices** container.

Select the **Device** containing the service to which you want to connect.

In the Workspace, select the **service** to which you want to connect.

The Service Properties page opens.

Figure 4.12 ~ Accessing a Service from the Devices Container.

In the Workspace, select the **service** to which you want to connect.

Click **Connect to Directory Service** from the **Infrastructure** task group.

If you are connecting to an RCS whose service has not been added as a Directory Service to the Zone Configuration container, the following dialog box opens and gives you a choice of how to continue.

Figure 4.13 ~ Prompt to Add the RCS as a Directory Service.

- Click **Add** to first add the RCS as a Directory Service to the Zone Configuration container, and then connect to the service.

  Adding a Directory Service entry allows an automatic connection to this RCS directory whenever the Radia Management Portal Zone starts up. If this is the first RCS being added to the Zone, the Common Name will default to primary. If a primary RCS exists in this zone, the Common Name will default to rcs1. For details on adding the RCS as a Directory Service, see *Specifying RCS Directory Service Properties* on page 147.

- Click **Connect** to simply connect to the RCS from this location.

Figure 4.11on page 155 shows a sample connection to an RCS Database.

Disconnecting from a Directory Service

Use the **Disconnect from Directory Service** task in the **Infrastructure** task group to remove a current connection to an external directory service or device service. After disconnecting, the objects in that Directory Service are no longer available for performing Radia Management Portal operations until another connection is made.

- To disconnect from a service defined as a Directory Service, use the following procedure *To disconnect from a Directory Service.*

- To disconnect from an RCS Service from its Service Properties page within the Device container, use the procedure *To disconnect from a service defined for a Device* on page 158.

To disconnect from a Directory Service

Display the **Directory Service Properties** page from which you want to disconnect.

To navigate to a Directory Service Properties page:

a. Use the **Navigation aid** to go to the **Zone, Configuration, Directory Services** container.

b. In the Workspace, click the Directory Service object.

c. If necessary, click the Toolbar **View Properties** icon 🔍 .

Figure 4.14 ~ Disconnecting from a Directory Service or RCS database.

Click the **Disconnect from Directory Service** task within the **Infrastructure** task group. The connection is terminated immediately.

To disconnect from a service defined for a Device

Use the **Navigation aid** to go to the **Zone Devices** container.

Select the **Device** containing the service to which you want to disconnect.

In the Workspace, select the **service** to which you want to disconnect.

The Service Properties page opens.

Figure 4.15 ~ Accessing a Service from the Devices Container.

Click the **Disconnect from Directory Service** task within the **Infrastructure** task group.

The connection is terminated immediately.

Configuring for External LDAP Authentication

Use the procedures and the rmp.cfg configuration parameters listed in this topic to implement external LDAP authentication for users of the Radia Management Portal. Table 4.8 ~ rmp.cfg Parameters for External LDAP Authentication lists the entries for configuring external LDAP authentication. These entries specify:

■ default external authentication setting for all users of the Radia Management Portal (on or off)

■ domain a user will bind to

■ hostname and port of the LDAP server

> **Note**
>
> By default, the Admin userID only binds to the local RMP directory.

If you set the default external authentication mode to on, you will also need to specify the external user ID and passwords for each user on the Person properties page. For details, see *Adding Users*

on page 97. To disable LDAP authentication for individual users, see *Modifying the Default LDAP Authentication for Specific Users* on page 161.

If you set the default external authentication mode to off, use the Add Person or Modify Person pages to turn on External authentication as well as specify an External User ID and external password for anyone to be externally authenticated.

To configure external LDAP authentication for the Radia Management Portal

Stop the **Radia Integration Server** service.

Use a text editor to open the Radia Management Portal configuration file, rmp.cfg, located by default in **SystemDrive:\Novadigm\IntegrationServer\etc**.

```
# RMP Module (Radia Management Portal)
#

# This section provides the core configuration for the
# RMP Sub-system. Please take care when hand-editing this.
#
rmp::init {
    URL            /

    LDAP_AUTH       1
    LDAP_AUTH_DN    <<user>>@mydomain.com
    LDAP_AUTH_HOST  myldaphostname:389



    }
#
# END OF CONFIG
#
```

Sample parameters to enable LDAP authentication for all users, by default.

Figure 4.16 ~ Sample rmp.cfg file defining an external LDAP authentication.

Insert the LDAP_AUTH, LDAP_AUTH_DN, and LDAP_AUTH_HOST parameters using uppercase into this file before the finishing curly bracket (}), as shown in *Figure 4.16 ~ Sample rmp.cfg file defining an external LDAP authentication*, above.

> **Note**
>
> The LDAP_AUTH value determines whether all users are enabled or disabled for LDAP authentication, by default. To override the default LDAP authentication value for specific users, see Modifying the Default LDAP Authentication for Specific Users on page 161.

Use one or more spaces to separate the parameter and its value. Refer to Table 4.8 ~ rmp.cfg Parameters for External LDAP Authentication on page 161.

Table 4.8 ~ rmp.cfg Parameters for External LDAP Authentication

Parameter and value	Definition and Examples
LDAP_AUTH 1 *or* LDAP_AUTH 0	Sets the default value of external authentication for all users logging onto the Radia Management Portal. Use the External Authentication? field on on the Person properties page to override the default value for any user. Set to **1** to enable external LDAP authentication, by default, for all users. Set to **0** to disable external authentication, by default, for all users. If unspecified, LDAP_AUTH is set to **0.**
LDAP_AUTH_DN *<<user>>*@*<mydomain*.com>	Defines the domain that a user will bind to. Replace *<mydomain*.com> with the domain that users will bind to. The *<<user>>* portion will be substituted with the value entered on the login page. LDAP_AUTH_DN *<<user>>*@*mydomain*.com LDAP_AUTH_DN *<<user>>*@*domainA*.com
LDAP_AUTH_HOST hostname:389	The hostname and port of the LDAP server. Where "myldaphostname" is the hostname of the LDAP server.

Save and close the file.

Restart the Radia Integration Server and open the Radia Management Portal.

Modifying the Default LDAP Authentication for Specific Users

To change the default LDAP authentication value for specific users, use the Modify Person task and reset the value of External authentication for that person to the desired value.

■   To enable External authentication, set the value to **1**.

■   To disable External authentication, set the value to the number **0**.

These values are the equivalents of selecting **Yes** or **No** for External authentication on the Add Person dialog box. For details, see *Adding Users* on page 232 and *Modifying Users* on page 236.

Figure 4.17 ~ Set External authentication to 0 (zero) to disable LDAP authentication for a user.

By default, any Portal Administrators (Admin) have their external authentication set to No (or 0 on the Modify Person dialog box) when a new directory is created through the Radia Management Portal.

Configuring for a Custom LDAP Policy Extension Prefix

Many Radia Policy Server implementations use the default LDAP Policy Extension prefix of **edm**—as in edmPolicy. If you have defined an LDAP Directory Service for policy tasks, but it uses a policy extension prefix other than **edm**, use the following procedure to define its LDAP Policy Extension prefix value to the Radia Management Portal. This procedure adds a PREFIX parameter to the rmp.cfg file where you specify a policy prefix value other than **edm**.

See the *Radia Policy Server Guide* for more information on configuring the Radia Policy Server and the LDAP Policy Extension.

To configure the Radia Management Portal for a Custom LDAP Policy Prefix (other than edm)

Stop the **Radia Integration Server** service.

Use a text editor to open the Radia Management Portal configuration file, rmp.cfg, located by default in **SystemDrive:\Novadigm\IntegrationServer\etc**.

```
#
# Copyright (C) 1997-2001 HP. All Rights Reserved.
#
# $Header: /cvs/nvd/rmp/default.rc,v 1.6 2002/02/01 17:56:24 Exp $
#
#
# RMP Module (Radia Management Portal)
#

# This section provides the core configuration for the
# RMP Sub-system. Please take care when hand-editing this.
#
rmp::init {
    URL             /

    PREFIX     rad          ◄──── Inserted PREFIX parameter defines a custom LDAP policy prefix.

    }
#
# END OF CONFIG
#
```

Figure 4.18 ~ Sample rmp.cfg file defining an LDAP Policy prefix other than edm.

Insert the PREFIX parameter (must be uppercase) into this file before the finishing curly bracket (}) as shown in *Figure 4.18 ~ Sample rmp.cfg file defining an LDAP Policy prefix other than* **edm** above.

Use one or more spaces to separate the PREFIX parameter and its value. Specify the value using the same case as is entered for the LDAP Policy Extension prefix defined in the Radia Policy Server.

Table 4.9 ~ Parameter to Configure a Custom Policy Prefix

Parameter	Explanation
PREFIX	Defines an LDAP Policy Extension prefix other than the default value of edm. Enter one or more spaces to separate the PREFIX parameter and its value. The value must match the LDAP Policy Extension prefix defined in the Radia Policy Manager. For example: `PREFIX  rad` defines a Policy prefix of rad instead of edm.

Save and close the file.

Restart the Radia Integration Server and open the Radia Management Portal.

Configuring Zone Access Points

Access Points to other Radia Management Portal Zones in your enterprise are automatically configured whenever you install multiple portal zones using the **Install RMP** task.

To access another zone in your Radia Infrastructure, go to the Zone Access Points container, and click on the icon for the Zone you want to view.

Figure 4.19 ~ Access the Chicago Zone from the Zone Access Points container.

Establishing Devices and Device Groups

There are a number of ways to bring devices under the control of a Radia Management Portal Zone.

■   The first step is to add computers to the Devices container of the Zone. As part of this step, devices also become members of the Default Group of the Group container. For details, see *Adding Devices to an RMP Zone*, which follows.

> **Note**
>
> As of RMP 2.0.1, you can perform the install tasks found in the Operations task group directly from a discovered Network or LDAP directory location. The RMP will add the selected computers to the Devices container of the RMP Zone automatically, and create links between the Network or LDAP directory location and the Zone Device location.

■   The next step is to create Groups to facilitate operations on the members of the groups. Topics related to Adding Groups of Devices begin on page 189.

■   The third step is to install the Radia Management Agent on devices. By installing the Radia Management Agent on devices, they automatically become members of the appropriate Cross-Reference container groups, which is an advantage when you need to Notify all devices with specific operating, software, or hardware configurations. For details, see *Installing the Radia Management Agent* on page 307.

Adding Devices to an RMP Zone

There are various ways to add devices to your RMP Zone. Table 4.10 on page 166 explains the various methods. Choose the methods that are easiest for your enterprise. All computers are added as devices to the Devices container. Unless otherwise specified, devices will also be added as members of the Default Group container, as well.

Table 4.10 ~ Methods of Adding Computers to a Zone Devices Container	
Method	**Description and Reference**
Network Selection	As of RMP 2.0.1, browse to computers discovered in your Networks and perform any Install task in the Operations task group. If the selected network devices are not currently in the Zone Devices container, they are added automatically to it before the install task is performed. A link is created between the Network location and RMP Zone location of each device.
	Or
	Browse to computers in your Networks container and select **Manage Computer** from the Operations task group. For details, see *Managing Computers* in the Operations chapter.
Active Directory Selection	As of RMP 2.0.1, browse to computers from a mounted and connected Active Directory location and perform any Install task from the Operations task group. If the devices in the selected LDAP location are not currently in the Zone Devices container, they are added automatically to it before the install task is performed. A link is created between the LDAP location and the RMP Zone location of each device.
	Or
	Browse to a computer in your LDAP directory and select the **Manage Computer** task in the Operations task group. For details, see *Managing Computers* in the Operations chapter.
Hostname List	Prepare a list of hostnames and use the **Import Devices** task. For details, see *Importing Devices* on page 202.
Individual Entry	Browse to a group in the Groups container and use **Add Device** from the Model Administration task group. For details, see *Adding a Single Device* on page 182.
Installed Radia Management Agent	Any computer that has the Radia Management Agent from this release installed on it will automatically be added to the Device container when it contacts the Radia Management Portal.

Several of the tasks used to bring devices under control of the Radia Management Portal employ a common browse and select window. Before continuing, we recommend you know how to use the window's features. For details, see *Basic Procedures for Modifying Groups*, which follows.

Basic Procedures for Modifying Groups

Many tasks in the Radia Management Portal use a similar set of windows to browse and modify items in a group. This topic describes how to use these windows. The same procedures apply regardless of the exact task you are performing.

The tasks using this window use 3 or 4 steps. Three steps apply when you can modify the changes at once; four steps are needed for tasks that present a Review of the changes before they are applied.

Step 1: Navigate to group and click task.

Step 2: Change the items in the group.

Step 3: Modify/Commit/ Review changes.

Step 4: After Review, click Modify.

Figure 4.20 ~ Overview of tasks that modify a group of items.

Using the Browse and Modify Window

Figure 4.21 shows a sample **Browse and Modify** window. The Move Device window opens when you select the **Move/Copy Device(s)** from the Model Administration task group.

There are three areas of this window: the group list area, the browse area, and the Modify buttons. Please review the use of each area. If you are working with Services or Policy objects, the group list area will also contain editors for service attributes and expressions.

Please review the use of each area, as discussed below.

Figure 4.21 ~ Sample Browse and Modify window for the Move/Copy Device(s) task.

Tip

You must click **Review** to continue and confirm the modifications.

■ **Group List**
The top area lists the items in the group being modified. For example, Figure 4.21 lists the items in **New Group**, which is a group of devices in the **Zone Groups** container.

To modify or remove items listed in the group area, see the topic *Using the Group List Area* on page 169.

When working with Radia Service objects, you can select a service in the Group List area and use the **Attribute Editor** to specify values for its attributes. See *Using the Attribute Editor* on page 172 for more information.

When working with Radia Service objects, you can also select a service in the Group List area and use the **Expression Editor** to specify additional constraints. See *Using the Expression Editor* on page 176 for more information.

■ **Browse area**
The bottom area allows you to browse your Radia Management Portal Zone to select items,

and then add, move, or copy the items into the group list. For details on using this area, see *Using the Browse Area* on page 180.

■ **Buttons**
The exact button names will vary, but the first button is the one to use to accept the changes.

- Click **Modify** or **Commit** to make and save the changes to the group list.

- If **Review** is available, you must first review the changes before saving them. Click **Review** to see a window summarizing the changes. Next, click **Modify** to make the changes and complete the task.

- Click **Reset** to abandon any changes to the group items you made since starting the task.

- Click **Cancel** to exit the task.

Using the Group List Area

Use the group list area of the **Browse and Modify** window to delete items from the group and manually modify or add an item. To manually modify or add an item, you must specify its X500 Distinguished Name.

> **Tip**
>
> The X500 Distinguished Name is listed in the Object Information area of an item's Properties page. It is also available when you hover the mouse over an object's name in the Workspace or the Navigation area.

To delete one or more items in the list

Click the check box to the right of each item in the group list area to be removed.

Figure 4.22 ~ Selecting items to be removed from a list.

Click ✖ to delete the items from the list.

Click the **Modify** or **Commit** button below the Browse group area to save the modified list.

> **Note**
>
> Some tasks include a **Review** button instead of a **Modify** button. In this case, click **Review** and then click **Modify** after reviewing the changes.

To modify one or more items on the list

Click the check box to the right of each item in the group list area to be modified.

Click ⬤ to modify the checked items.

Please review the use of each area, as discussed below.

Figure 4.23 ~ Item in a list ready for modification.

In the text box area, modify the X500 Distinguished Name for the item.

Click ✔ to accept the changes.

Click the **Modify** button at the bottom of the page to save the modified list.

> **Note**
>
> Some tasks include a **Review** button instead of a **Modify** button. In this case, click **Review** and then click **Modify** after reviewing the changes.

To manually add an item to the list

Click ⊕ to manually add an item to the list.

The list area displays a text box entry area, where you can specify the X500 Distinguished Name for an object.

Figure 4.24 ~ Text box entry area for adding an item to a group.

Tip

The X500 Distinguished Name is listed in the Object Information area of an item's Properties page. It is also available when you hover the mouse over an object's name in the Workspace or the Navigation area.

In the text-box area, type the X500 Distinguished Name for the object to be added. For example, the X500 Distinguished Name for the **Default Group** of devices is:

cn=default, cn=group, cn=myzone, cn=radia

Click ✔ to accept the changes.

Click the **Modify** or **Commit** button below the Browse area to save the modified list.

Note

Some tasks include a **Review** button. In this case, click **Review** and then click **Modify** after reviewing the changes.

Figure 4.25 ~ Text box entry area for adding an item to a group.

In the text box area, type the X500 Distinguished Name entry for the item.

Click ✔ to accept the changes.

Click the **Modify** or **Commit** button below the Browse area to save the modified list.

> **Note**
>
> Some tasks include a **Review** button instead of **Modify** or **Commit**. In this case, click **Review** and then click **Modify** after reviewing the changes.

Using the Attribute Editor

After selecting a service in the **Browse and Modify** window, use the Attribute Editor to specify values for the attributes for Radia services. The values that you are specifying are for policy (see *Modifying Policies* on page 115), defaults (see *Modifying Defaults* on page 130) or overrides (see *Modifying Overrides* on page 131).

The following procedure demonstrates how to use the Attribute Editor to set the default version of the Amortize application to version 1.0.

To use the Attribute Editor

After selecting the appropriate task from the **Policy (Advanced)** task group, use the **Browse** window to select the appropriate service, such as Amortize.

Figure 4.26 ~ Modify Policy Defaults window – Amortize service selected.

Click the ⊞ to the left of the **Attributes** text box.

The **Attributes Editor** area opens.

Figure 4.27 ~ Attribute Editor.

In the **Attribute Editor** area, click ⊕ to add a new attribute.

Figure 4.28 ~ Adding an attribute.

In the text box on the left, type the name of the attribute to be added, such as version. You can specify any attribute that is available for the service.

In the text box on the right, type the value for the attribute, such as 1.0.

Click ✔ to accept the changes to the attribute.

Figure 4.29 ~ Attribute added.

The correct syntax for the attribute and the value you specified appear in the Attributes text box in the Policy Defaults area of the window.

When you are done with your changes, click **Commit**.

Using the Expression Editor

After selecting a service in the **Browse and Modify** window, use the **Expression Editor** to specify additional constraints for the selected service. The expressions that you are specifying are for policy (see *Modifying Policies* on page 115), defaults (see *Modifying Defaults* on page 130) or overrides (see *Modifying Overrides* on page 131).

The following procedure demonstrates how to use the Expression Editor to set a constraint on the Amortize service so that in addition to deploying version 1.0 (as described in the topic Using the Attribute Editor, this service will only be deployed to machines with a Windows NT operating system.

To use the Expression Editor

After selecting the appropriate task from the **Policy (Advanced)** task group, use the **Browse** window to select the appropriate service, such as Amortize.

Note
In the example shown in this procedure, the version attribute has also been set to 1.0.

Click the ⊞ to the left of the **Expression** text box.

The **Expression Editor** area opens.

Figure 4.30 ~ Expression Editor.

In the **Expression Editor** area, click ⊕ to add a new expression.

Figure 4.31 ~ Add a new expression.

From the **Add** drop-down list, select one of the following pre-defined operands:

> ### Note
>
> If you want to use an operand other than the ones that are pre-defined in the **Add** drop-down list, you can type any operand in the text field.

- **<<in.os>>**
  References the operating system

- **<<in.uid>>**
  References the user ID

- **<<in.host>>**
  References the host computer

- **<<in.zcontext>>**
  References the ZCONTEXT attribute. See the *Radia Application Manager Guide* for more information about this attribute.

Each of these options represents substitution of attributes that were supplied as input during policy resolution. See the *Policy Server Guide* for more information.

If necessary, select an operator from the **Operator** drop-down list, such as ==.

Table 4.11 ~ Operators	
Expression	**Meaning**
||	Logical OR
&&	Logical AND
==	Test for equality (case-sensitive)
!=	Test for inequality
<=	Dictionary comparison for less than or equal to
>=	Dictionary comparison for greater than or equal to (C locale)
<	Numerical comparison for less than
>	Numerical comparison for greater than
!	Logical NOT
Contains	Is contained anywhere within the string. This is not case sensitive.
Begins with	The beginning of the string matches. This is not case sensitive.
Ends with	The ending of the string matches. This is not case sensitive.
Matches	Exact match. This is not case sensitive.

In the **Operand2** text box, type the appropriate value, such as NT.

Click ✔ to accept the changes to the expression.

Figure 4.32 ~ Expression.

When you are done with your changes, click **Commit**.

Using the Browse Area

The browse area icons provides a toolbar to select the items that are to be added, moved, or copied into the group list on the top.

■ Use this topic to become familiar with the browse area toolbar icons and how to use the browse area.

■ To become familiar with browsing, selecting and adding items from the browse area to the group list area, we recommend you follow the step-by-step procedures in *Moving or Copying Devices into a Group* on page 182.

> **Note**
>
> After using the browse area to select and add items to the group list area, you must complete the task by clicking one of the buttons on the bottom of the page. For example, **Modify, Commit,** or **Review**. If the button is **Review,** you must also click **Modify** on the next window.

Current Navigation Location

The Browse area label identifies the current navigation location. For example, the following figure shows the browse location is the Default Group within the Radia Zone Groups container.

Figure 4.33 ~ Browse area label identifies current navigation location.

Navigation Icons

■ Click ![icon] to go up one level in your Zone directory.

■ Click ![icon] to refresh the view.

■ Click ![icon] to return home to the browse location when you started the task.

■ Click ![icon] (a group or container icon) to browse the items in that group.

Action Icons

■ Click ![icon] to add selected objects to the top area.

■ Click ![icon] to move selected objects to the top area.

■ Click ![icon] to copy selected objects to the top area.

View Icons

- Click to show the potential targets with large icons.

- Click to show the potential targets in a list view.

- Click to show the potential targets in a detailed view.

Paging and Filtering Icons

The following icons assist in browsing and selecting from large numbers of items.

- Use the drop-down list box to set the maximum number of items for the current page:

- Use the scroll bar to scroll to items not currently in view.

- In the text box, type a filter value and click to filter the items on the current page. Valid filter characters include the asterisk (*) and the question mark (?).

- Use the drop-down list box and the arrows to page through multiple pages.

Selection Icons

- Click to select all of the targets listed. The icon will change to .

- Click the individual check boxes to select specific targets from the list.

- Click to view the properties for the target.

Configuring the Zone Infrastructure

Use the tasks in this topic to configure the Zone Devices and Device Groups that are being managed by a Radia Management Portal Zone.

Before proceeding, you should be familiar with the use of the Browse and Select Windows. This is discussed in *Basic Procedures for Modifying Groups* on page 166.

Adding a Single Device

Use the **Add Device** task in the **Model Administration** task group to add a single device to the Zone Devices container. The device becomes a member of the group within the Groups container where you begin the task, as well as the **Default Group**.

If you want to have this device added to a new group, first create the group using the procedure *To add a Group of devices* on page 189, and then use the **Add Device** task, below.

To add a single device

If necessary, set the **Navigate aid** to **Location** mode.

Figure 4.34 ~ Click the icon on the title bar to switch from Navigation Location to History mode.

Navigate to the **Zone**, **Groups** container.

Figure 4.35 ~ Zone Groups container.

In the Workspace, select the Group in which you want the new device to become a member. If you select a group other than the Default Group, the new device will also become a member of Default Group.

From the **Model Administration** task group, click **Add Device.**

The **Add Device** dialog box opens.

Figure 4.36 ~ Add Device dialog box.

Enter the following Add Device Properties for the new device.

● In the **Display Name** text box, type a display name for the device. This name will appear as the label of the object in the infrastructure representation. If omitted, a validated DNS Host Name entry is used. If omitted and a valid DNS Host Name is not available, the Radia Management Portal generates a unique alphanumeric Common Name, and that is also used as the Display Name.

● In the **DNS Host Name** text box, type a fully qualified DNS Host Name for the computer as it is known in the network. For example, test900.usa.mydomain.com.

● In the **IP Address** text box, enter the IP address for the computer, if known.

Click **Add.**

The Radia Management Portal adds the device to the Devices container.

● If the device has unique properties (DNS host name and/or IP address), the device is added to the group from which you began the task. You will see a new entry for the device in the Workspace of the Group from which you began the task. Devices are listed alphabetically by Display Name.

Figure 4.37 ~ 'A Test 900' Device successful added to the Default Group container.

● If the device properties match those of an existing device entry, the new device is not added.

Generated Common Names for Devices

All Common Names assigned to device entries must be unique within a given Zone Device container. At times, the Radia Management Portal must generate a unique Common Name for a device. A generated Common Name is illustrated below:

Figure 4.38 ~ Sample Common Name generated for a Device.

Viewing Device Properties

🔍 Click the **View Properties** icon on the toolbar above the Workspace to View Properties for a Device.

You can do this after navigating to the Device's entry in a Group container, or from the Device's entry in the Devices Container.

Figure 4.39 ~ Viewing Device Properties for a newly added Device, no RMA installed.

After a Radia Management Agent is installed on a Device, the known device properties are substantially increased, as illustrated in Figure 4.40. The Radia Management Portal uses this information to create memberships for the device in the appropriate Cross-Reference container groups.

■ From a Device Properties page, click on any underlined entry to go to the linked location.

■ To return, use the back arrow on the toolbar.

Figure 4.40 ~ Device Properties after installing the Radia Management Agent.

Adding Groups

Use the **Add Group** task in the **Model Administration** task group to add a new device group to the Groups container. The **Add Group** task also gives you the option of copying or moving devices into the new group from the other groups in the Groups container.

■ For procedures on adding a group without adding or moving devices into it, see the procedure *To add a Group of devices*, which follows.

■ For procedures on adding devices to the new group, see *Adding Devices to a New Group* on page 191.

■ For procedures on import devices into their own group, first use **Add Group** to create a new group of devices. Then select that group before using the **Import Devices** task. For details, see *Importing Devices* on page 202.

To add a Group of devices

Use this procedure to create a new group for devices, but not move or copy any devices into the group at this time.

If necessary, set the **Navigate aid** to **Location** mode.

Figure 4.41 ~ Click the icon on the title bar to switch from Navigation Location to History mode.

Navigate to the **Zone**, **Groups** container.

Figure 4.42 ~ Zone Groups container.

From the **Model Administration** task group, click **Add Group.**

The **Add Group** dialog box opens.

Enter the following Properties for the new group.

- In the Common Name text box, type a unique group name. The common name must be unique for the object class.

Caution
The Common Name for the object must be unique. If you attempt to create an object with a name that has already been used, an error appears in the workspace indicating that the object already exists.

- In the Display Name text box, type a display name for the group. This name will appear as the label of the object in the infrastructure representation.
- In the Description text box, type a description that reflects the intended membership of the group. The description displays in details view.

Click **Add.**

The Modify Group dialog box opens. It shows:

- Properties previously entered.
- No devices defined in the group list.
- Browse area containing current Groups in the zone.

Figure 4.43 ~ Initial window opens for Modify Test Group of devices.

To save the group, click **Modify**.

The task ends, and the Navigation aid indicates the new group location in the Groups container. There won't be any members of the group until you move/copy or import devices into it. Refer to the **Import Devices** or **Move/Copy Device(s)** tasks.

Adding Devices to a New Group

Use the **Add Group** task in the **Model Administration** task group to create a new group and then move or copy devices from other groups in your Zone Groups containers into the group.

The procedure that follows adds a group named Test Group to the Groups container, and then uses the Modify Group page to copy two devices from the Default Group to the Test Group.

Note
Use this sample procedure to become familiar with using the Browse area.

To add devices to a new group

If necessary, set the **Navigate aid** to **Location** mode.

Figure 4.44 ~ Click the icon on the title bar to switch from Navigation Location to History mode.

Navigate to the **Zone**, **Groups** container.

Figure 4.45 ~ Zone Groups container.

From the **Model Administration** task group, click **Add Group.**

The **Add Group** dialog box opens.

Enter the following Properties for the new group.

- In the Common Name text box, type **Test Group**.
- In the Display Name text box, type **Test Group**. This name will appear as the label of the object in the infrastructure representation.
- In the Description text box, type **Test Group of Devices**. The description displays in details view.

Caution
The Common Name for the object must be unique. If you attempt to create an object with a name that has already been used, an error appears in the workspace indicating that the object already exists.

Click **Add.**

The Modify Group dialog box opens. It shows:

● Properties previously entered.

● No devices defined in the group list.

● Browse area containing current Groups in the zone.

Figure 4.46 ~ Initial window opens for Modify Test Group of devices.

> **Note**
>
> Your groups listed in the Browse area will vary, but they will always include the Default Group and the newly created Test Group.

In the Browse area, click Default Group icon.

The Browse area refreshes to display all devices that are members of your Default Group.

Typically, there will be a large number of devices in the Default Group, since all devices are automatically added to this group unless specified otherwise.

At a minimum, the Default Group includes the device hosting your Radia Management Portal.

Click the check box next to at least one device in the browse area.

Figure 4.47 ~ Browse area with two devices selected.

Click on the Browse area toolbar to add the selected devices to the group list.

Figure 4.48 ~ Selected items from Browse area added to Device List.

 Click the **Modify** button below the Browse area to complete the task.

The devices are added to the **Test Group**, and the **Modify Group** dialog box closes. The Radia Management Portal indicates the new location of the Test Group within the Groups container, and the Workspace lists the current devices in the group.

Figure 4.49 ~ View of added Test Group Location and Contents.

Moving or Copying Devices into a Group

Use the **Move/Copy Device(s)** task in the Model Administration task group whenever you need to switch members of an existing device group. The task is flexible and allows you to switch device group memberships, copy devices that are members of another group, or remove devices from a group's membership.

> **Tips**
>
> To create a new group for devices, see *Adding User Groups* on page 191.
>
> Using any of the install tasks from the Operations task group against devices in the Network container or devices in an LDAP directory automatically creates entries for the devices in the Zone Devices container and makes them members of the Default Group. Use this Move/Copy Devices task to switch or add group memberships, as needed.

To remove devices from a group, see the procedure *To remove devices from a Group* on page 199.

To move or copy devices into a group

Use the **Navigation aid** to select the group in the **Zone Groups** container whose members you want to change.

In the **Model Administration** task group, click **Move/Copy Device(s)**.

Figure 4.50 ~ Locate Group to change device members, click Move/Copy Device(s).

The **Move Device to <<selected>> Group** window opens. Use this window to make any changes to the device membership for this group.

Figure 4.51 ~ Initial page for Move/Copy Device(s) task.

For general instructions on how to navigate and use this window, see the topic *Basic Procedures for Modifying Groups* on page 166.

Use the **Browse Devices** area to browse to the appropriate device targets.

The following devices or device groups can be selected for group membership:

● Devices from the **Devices** container.

● Devices or Groups from the **Groups** container.

● Devices or Groups from the **Cross References** container.

> **Note**
>
> You cannot move or copy devices into Groups until they have been added to the Devices and Groups containers of your Zone. For example, you cannot move or copy devices accessed from the Network container—they first must be added to your Zone. This is done automatically when you use any of the **Install** tasks of the Operations task group. Alternatively, you can also add a device explicitly using the **Manage Computer** task, the **Import Devices** task on page 202, or the **Add Device** task.

Select the devices or device groups from the browse area and copy or move them into the Devices area.

- Click ⬤ to copy devices and have the selected devices retain membership in the source group.

- Click 📁 to move devices from one group into another. The selected devices will be removed as members of the source group.

If necessary, repeat the browse and move/copy steps until all devices and groups are listed in the **Devices** area.

Click the **Review** button on the bottom of the page.

A page listing the summary of devices being added or removed from the current group opens. The following figure illustrates the device **DAC_W2KS** being moved from the **South Wing Group** to the **Test Group**. The device **Pubs 2** is being added to the Test Group.

Figure 4.52 ~ Reviewing Move/Copy Device(s) Summary.

To accept the changes, click **Modify**. To revise the changes, click **Reset**.

If you click **Modify**, the changes on the review page are made to the Group. The Modify Group task ends, and the Workgroup displays the current group members.

Figure 4.53 ~ Move/Copy Device(s) task completed.

To remove devices from a Group

1. Use the **Navigation aid** to select the group in the **Zone Groups** container whose members you want to change.

2. In the **Model Administration** task group, click **Move/Copy Device(s)**.

The **Move Device to <<selected>> Group** window opens.

3. On the right-side of the Devices area, use the check boxes to select the members of the group to be deleted.

Figure 4.54 ~ Selecting Devices to be Removed.

4. After selecting the devices to be deleted, click ✖ to delete the checked items.

5. Click **Review** to review the changes.

    A window opens to list the devices to remove from the group.

Figure 4.55 ~ Review of devices to be removed from a group. Click Modify to finish.

6. Click **Modify** to complete the removal of the devices.

The task ends, and the Workspace displays the devices remaining in the group.

Removing Groups of Devices

Use the **Remove** task from the **Model Administration** task group to remove a group of devices from the Groups container that is no longer required for operational purposes. The **Default Group** of devices cannot be removed.

Removing a group removes all device memberships in that group, but does not remove the devices themselves from the Portal Zone. The group will no longer be available for selection and for use with Operations that can be performed against groups of devices.

To remove a group of devices

1. Use the **Navigation aid** to go to the appropriate group in the Groups container.

2. In the **Model Administration** task group, click **Remove**.

A confirmation appears in the workspace.

Figure 4.56 ~ Remove Group message.

3. Click ✔ to confirm that you want to remove the group from the Radia Management Portal Directory.

OR

Click ✖ to indicate that you do not want to remove the group.

4. The remove is completed if the group does not have any other groups as its members.

If the group you want to remove has groups as members (children), a notification and confirmation appears in the workspace.

Remove Group

"South Wing Group" has children
Are you sure you want to remove this object and all its children? ✔ ✘

Selective Delete of Child Objects

Figure 4.57 ~ Remove with Children message.

---

5. Click ✔ to confirm that you want to remove the group and any groups that are members of it from the Radia Management Portal Directory.

OR

Click ✘ to indicate that you do not want to remove the group and its group members. The remove is cancelled; none of the groups or memberships is removed.

Importing Devices

Use the **Import Devices** task in the Model Administration task group to add a list of devices with fully qualified DNS names into the Zone Devices container. The devices become members of the Zone Groups container group from which you begin this task, as well as the **Default Group** of devices.

If you want to import the devices into a separate group, first use **Add Group** to create the group within the **Zone, Groups** container. Then use the procedures below to import the devices.

To import devices from a text file or list

Outside the Radia Management Portal, prepare a text-based list or text file of the devices to be added to the group. The list needs to specify a fully qualified DNS name for each computer.

> **Note**
>
> You can modify the group members later. However, portal operations can only be performed on the entire group (not a subset). Thus, plan your groups accordingly.

You can cut and paste entries from your prepared list into the text box available in Step 6 of this procedure on page 203, or you can import the text file list.

To automatically input the entire file during this task, place the ***.txt** file in the **\etc\group** folder of the Radia Integration Server location. By default, this location is:

⟨*SystemDrive*⟩:¥Novadigm¥IntegrationServer¥etc¥group

From the Radia Management Portal, locate or create a Group within the Zone Groups container where the imported devices will hold membership. For details on adding a new group of devices, see *Adding Groups* on page 189.

> **Note**
>
> All imported devices automatically become members of the **Default Group**. If you import the devices into a group other than the Default Group, they will hold memberships in both groups.

Navigate to the **Zone Groups** container and select the Group to hold the imported devices.

From the **Model Administration** task group, click **Import Devices** task.

The **Import Devices** dialog box opens, prompting you to select an input method.

Figure 4.58 ~ Select input method from Add Group of Devices dialog box.

Choose how you want to input the members of the group using one of the following methods:

- Select **Text** to type (or cut and paste) the members of your group into a text box in the next dialog box. The following dialog box opens.

Figure 4.59 ~ Import Devices from text window.

Use the **Input Text** box to type (or cut and paste in) the members of the group. Enter DNS hostnames for the devices separated by one or more spaces. You can remove members from this source input list in the next step.

● Click **File** to select a *.txt file you have prepared and placed in the **\etc\group** folder of the Radia Management Portal installation directory. The following dialog box opens.

Figure 4.60 ~ Import Devices from File window.

Use the **Filename** list box to select the text file to serve as the source of the group members. You can remove members from this source list in the next step.

> **Caution**
>
> As soon as you click **Submit**, all new devices from the input list or text file are added as members of the selected device group in your infrastructure zone.

Click **Submit** to add the devices to Zone as members of the selected group.

Once a group is added, you can select that group before performing an operation. The operation will be performed on all members of the selected group.

To split the devices into different groups, see *Moving or Copying Devices into a Group* on page 195.

To move some of the devices into a new group, see *Adding Devices to a New Group* on page 191.

Dynamic Job Scheduling Against Groups of Devices

Jobs scheduled for the following Operations tasks are dynamic when used against a group of devices:

- Install Client
- Install Management Agent
- Install Proxy Server
- Notify
- Synchronize Proxy Server
- Purge Dynamic Cache (of Proxy Server)

This means the target list is recalculated against the group each time the job is initiated, as opposed to when the job is scheduled.

This dynamic feature can be used to notify a series of devices, for example, with minimal effort. You can create a group of devices and schedule a daily Notify against the group. By changing the members in the group of devices between executions, the job continues to notify the new group members each day.

Adding Services

Use the **Add Service** task to manually add a service to a Device within your Zone. This can be done before a Radia Management Agent is installed on the Device to manually enable a connection to the service, or to enable the Radia Management Portal tasks available for the specific service.

For example, if you manually add a service for a Radia Proxy Server to a Device, then the Synchronize Proxy Server and Purge Dynamic Cache tasks become available from the Operations task group when you navigate to the service. See Figure 4.63 on page 208 for an example of how to add a service for a Radia Proxy Server to a Device.

> **Note**
>
> Once the Radia Management Agent has been installed on a Device, its Services will be automatically detected.

To add a service

Use the **Navigation aid** to go to the Device entry for which you want to add a service. Devices can be accessed from either the **Zone Devices** container or from one of the **Zone Groups** containers.

If the Device already includes services discovered or entered, the Workspace displays the list of services.

If the Device does not have any services at this point, the Properties page for the Device opens.

Figure 4.61 ~ Authority – Zone Devices instance.

In the **Model Administration** task group, click **Add Service**.

The **Add Server** dialog box opens.

Figure 4.62 ~ Add Service dialog box.

In the Service Type area, use the drop-down list to select the type of service to add:

- Select **Generic** to add a generic service.
- Select **RCS** to add a ZTOPTASK.EXE service on a Radia Configuration Server.
- Select **HTTPD** to add a service running under the Radia Integration Service {httpd}, such a service for the Radia Proxy Server or the Radia Inventory Manager Server.

The page refreshes after your selection to display the appropriate fields for the selected service type.

In the **Common Name** text box, type a name for the object.

- To identify a service for a Radia Proxy Server, type **rps**.

> **Caution**
>
> The Common Name for the object must be unique for the device. If you attempt to create an object with a name that has already been used, an error appears in the workspace indicating that the object already exists.

In the **Display Name** text box, type a name for the server that will appear in the infrastructure representation.

In the **Description** text box, type a description that will appear in the Details view of the infrastructure representation.

In the **Port Number** text box, type the port number used to connect to the service.

● **3466** is the default port number for a Radia httpd service, such as for the Radia Proxy Server. See *Figure 4.63 ~ Adding a Service for a Radia Proxy Server,* below, for an example.

Figure 4.63 ~ Adding a Service for a Radia Proxy Server.

> **Note**
>
> The following fields apply to the RCS Service Type, only. For other types, skip to Step 12.

In the **Path** text box, type the exact path of ztoptask.exe on the **RCS** machine. For example: C:/Novadigm/ConfigurationServer/bin/ztoptask.exe.

In the **User** text box, type the Username needed to use to connect to the RCS.

7. In the **User Password** text box, type the password for the user to connect to the RCS.

In the **Timeout** text box, leave the default value of 0 to never have an RCS connection timeout. To have the RCS connection timeout after a specific period of inactivity, type the timeout period in seconds in the **Timeout** text box.

Click **Add** to add the service to your Device.

The new service is added to the properties for the Device. The Service Properties page for the new service opens in the Workspace.

To connect to the service just defined, use the **Connect to Directory Service** task in the Infrastructure task group. For details, see *Connecting to a Directory Service* on page 154.

Modifying Objects

Use the **Modify** task in the **Model Administration** task group to make changes to any object in the representation of your infrastructure. If you are modifying group objects, also refer to the topic *Basic Procedures for Modifying Groups* on page 166.

To modify an object

1. Use the Navigation aid to go to the object that you want to modify.
2. In the **Model Administration** task group, click **Modify**.

    The **Modify <<object type>>** dialog box opens.

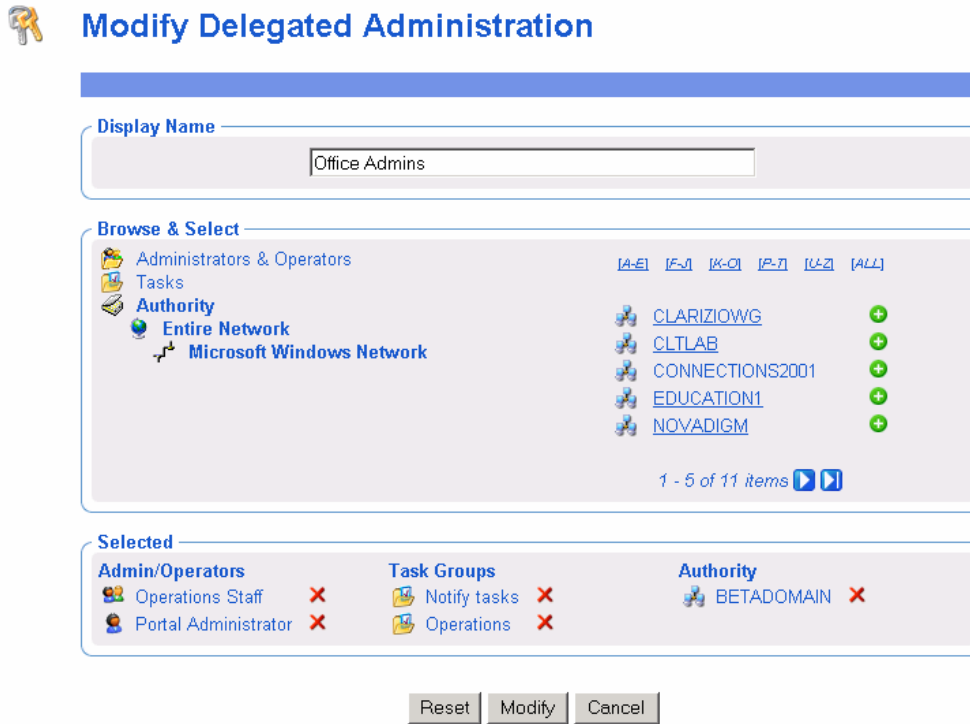
Figure 4.64 ~ Modify Device dialog box.

3. Make the necessary changes.
4. Click **Modify** to save your changes.

    OR

    Click **Reset** to undo the changes that you made.

    OR

    Click **Cancel** to cancel the modify task.

Removing Objects

Use the **Remove** task in the **Model Administration** task group to remove an object from the Zone. If the object has children, you are given the option of reviewing and then removing all of the children as well. For example, if you remove a Group of devices whose members include other

Groups of devices, you are prompted as to whether or not you want to remove the children of the objects.

> **Caution**
>
> Prior to removing an object with children, you may want to navigate through the child-objects to make sure you want everything removed.

To remove an object and its children

1. Use the Navigation aid to go to the appropriate object.

2. In the **Model Administration** task group, click **Remove**.

   A confirmation appears in the workspace.

Figure 4.65 ~ Remove Group message.

---

3. Click ✔ to confirm that you want to remove the object from the Radia Management Portal Directory.

   OR

   Click ✖ to indicate that you do not want to remove the object.

4. The remove is completed if the object has no children.

   If the object you want to remove has children, a notification and confirmation appears in the workspace.

Remove Group

"West Coast Group" has children
Are you sure you want to remove this object and all its children? ✔ ✗

Selective Delete of Child Objects

Figure 4.66 ~ Remove Domain with Children message.

5. To first review the Child Objects, click **Selective Delete of Child Objects**.

6. Click ✔ to confirm that you want to remove the object and all its children from the Radia Management Portal Directory.

OR

Click ✗ to indicate that you do not want to remove the object and its children. The remove is cancelled; none of the objects is removed.

Configuring Task Groups

The Taskbar contains logical groups of tasks (called *task groups*). A *task* is an activity that a person performs to initiate a job. The available tasks vary based on the selected Authority, as well as your role. In addition to the standard task groups (see *Taskbar* on page 82 for more information), you can create your own task groups.

Adding Task Groups

To add a task group

1. Use the Navigation aid to go to **Directory**, **Zone, Configuration, Tasks**.

    The workspace displays the current set of **Tasks** and **Task Groups**. Task Groups are represented by the yellow folder icons, tasks by the blue page icons.

Figure 4.67 ~ Authority – Tasks in the Zone Configuration container..

2. In the **Model Administration** task group, click **Add Task Group**.

    The **Add Task Container** dialog box opens.

Figure 4.68 ~ Add Task Container dialog box.

3. In the **Common Name** text box, type a name for the task group object.

Caution
The Common Name for the object must be unique. If you attempt to create an object with a name that has already been used, an error appears in the workspace indicating that the object already exists.

4. In the **Description** text box, type a description that will appear in the **Details** view.

5. In the **Display Name** text box, type a name for the task group. If omitted, the Common Name is used.

6. Click **Add**.

The **Modify Task Container** dialog box opens.

Figure 4.69 ~ Modify Task Container dialog box.

7. From the **Available** list, select one or more tasks to add to the task group.

8. Click ▶▶ to add the selected groups to the **Selected** list.

9. Click **Modify**.

The Workspace displays the contents of the new **Notify Operations** task group.

10. In the toolbar above the workspace, click the View Properties icon: 🔍.

The **Task Container Properties** for **Notify Operations** opens.

Figure 4.70 ~ View Properties Task Container dialog box.

11. To see this new Task Group, use the **Navigation aid** to go to **Directory**, **Zone, Groups, Default Groups**.

In the Taskbar, your new task group, such as **Notify Operations**, is available. Task Groups are listed alphabetically.

Figure 4.71 ~ New task group.

If you would like to configure the Radia Management Portal so that only some administrators can access this task group, see *Configuring Delegated Administration* on page 219 for more information.

Modifying Task Groups

To modify a task group

1. Use the Navigation aid to go to **Directory, Zone, Configuration, Tasks**.

2. In the Workspace, select the task group that you want to modify.

3. In the **Model Administration** task group, click **Modify**.

The **Modify Task Container** dialog box opens.

Figure 4.72 ~ Modify Task Container dialog box.

4. Make any necessary changes. For detailed information about configuring task groups, see *Adding Task Groups* on page 212 for more information.

5. Click **Modify** to save your changes.

   OR

   Click **Reset** to undo the changes that you made to this role.

   OR

   Click **Cancel** to close this dialog box without saving your changes.

   The Workspace displays the objects in the selected task group and you can see your changes.

Removing Task Groups

To remove a task group

Use the Navigation aid to go to **Directory, Zone, Configuration, Tasks**.

In the workspace, select the task group that you want to remove.

In the **Model Administration** task group, click **Remove**.

The **Remove Task Container** dialog box opens.

Figure 4.73 ~ Remove Task Container dialog box.

Click ✔ to confirm that you want to remove the task group from the Radia Management Portal Directory.

OR

Click ✘ to indicate that you do not want to remove the task group.

Configuring Delegated Administration

Use the Radia Management Portal to configure delegated administration information so that your administrators can access only the *tasks* that are relevant to them and their *roles*. A *task* is a single operational function, or an action, that is performed on the selected target audience. A *role* is a logical grouping of tasks that defines an administrative function. In other words, you will configure *who* can do *what*, and specify *where*, in the infrastructure, they may do it.

The Radia Management Portal contains several standard roles. To view the existing roles click **Directory, Zone, Configuration** in the navigation aid. Then, in the workspace, click **Delegated Administration**.

The following roles are used to perform Core Radia Management Portal operations:

- **Global Default Policy**
  Allows the Radia Management Portal administrator to access Model Administration and Operations tasks in the following Scopes of Action—**Zone, Administrators & Operators**, **Tasks** and **Job History**.

- **Operations Policy**
  Allows operations staff to access Operations tasks in the following Scopes of Action—**Zone**, **Administrators & Operators**, and **Tasks**.

- **System-Wide Access**
  Allows the Radia Management Portal administrator to access all tasks in all Scopes of Action.

> **Note**
>
> This role cannot be modified in order to prevent you from being locked out of the Radia Management Portal.

- **Test Global Policy**
  Allows you to experiment with entitlement options.

The following roles are used to administer the RCS database and Policy:

- **Account Administration**
- **Advanced Policy Administration**
- **Auditing Administration**
- **Infrastructure Administration**
- **Package Administration**
- **Policy Administration**
- **RCS Administration**
- **Service Administration**

In the workspace, click any of these delegated administration roles to view the properties for the role.

Adding Delegated Administration Roles

Adding new delegated administration information for your administrators is a three-step process. First, you will assign administrators and operators to the role. Next, you will specify what tasks the administrators or operators will be able to perform. And, finally, you will select where, in the infrastructure, the administrators or operators can perform these tasks.

To add a delegated administration role

Note
The Figures in this procedure do not reflect the latest changes to the Radia Management Portal.

1. Use the Navigation aid to go to **Directory, Zone, Configuration**.

2. In the workspace, click **Delegated Administration**.

Figure 4.74 ~ Authority – Delegated Administration.

3. In the **Model Administration** task group, click **Add Delegated Administration**.

The **Add Delegated Administration** dialog box opens.

Figure 4.75 ~ Add Delegated Administration dialog box.

4. In the **Display Name** text box, type a name for the role.

5. Click **Add**.

    The **Modify Delegated Administration** dialog box opens. First, you will select the administrators and operators that you want to assign to this role.

Figure 4.76 ~ Modify Delegated Administration dialog box – Administrators & Operators.

6. In the **Browse & Select** area of the dialog box, make sure that **Administrators & Operators** is selected. Selected text is bold.

7. Click ⊕ next to the each of the administrators and operators that you want to add.

Notice that as you select administrators and operators, they appear in the **Selected** area of the dialog box under the **Admin/Operators** column.

Figure 4.77 ~ Modify Delegated Administration dialog box – selecting Administrators & Operators.

If you want to remove an administrator or operator from the list of selected items, click ✖.

Next, select the tasks that you want to include in this role.

8. In the **Browse & Select** area of the dialog box, click **Tasks**.

The **Browse & Select** area updates to allow you to select *what* groups of tasks to include in this role.

Figure 4.78 ~ Modify Delegated Administration dialog box – selecting Tasks.

9. Click ▶ below the list, if you do not see the container that you want to select. If there are five or more task groups to select from, you can click the appropriate range of letters above the list to narrow it.

10. Click ⊕ next to the each of the task groups that you want to add.

Notice that as you select task groups, they appear in the **Selected** area of the dialog box under the **Task Groups** column.

Figure 4.79 ~ Modify Delegated Administration dialog box – selecting Task Groups.

If you want to remove a Task Group from the list of selected items, click ✖.

Next, select the areas in the infrastructure that administrators and operators assigned to this role are entitled to manage.

11. In the **Browse & Select** area of the dialog box, click **Authority**.

The **Browse & Select** area updates to allow you to select *where*, in the infrastructure, the administrators and operators assigned to this role are entitled to manage.

Figure 4.80 ~ Modify Delegated Administration dialog box – selecting Authority.

12. Click below the list, if you do not see the container that you want to select. If there are five or more task groups to select from, you can click the appropriate range of letters above the list to narrow it.

13. If necessary, you can browse the containers on the right to limit the Authority further. To do this, click the name of the container that you want to browse, such as **Zone**, and then **Networks**.

Figure 4.81 ~ Modify Delegated Administration dialog box – browsing for an Authority in a container.

Notice that the list of items that you can add to the delegated administration role narrows as you browse further into a specific container. For example, click **Microsoft Windows Network**.

Figure 4.82 ~ Modify Delegated Administration dialog box – browsing for an Authority in a domain.

Now, you can select a specific domain, such as the BETADOMAIN. This allows you to limit the administrator's access to a very specific area of your network.

At any time, you can click an item on the left (such as Entire Network) to return to a broader authority.

14. Click ⊕ next to the items that you want to add.

Notice that as you select an Authority, it appears in the **Selected** area of the dialog box under the **Authority** column.

Figure 4.83 ~ Modify Delegated Administration dialog box – selecting the Authority.

If you want to remove an Authority from the list of selected items, click ✖.

15. Click **Modify**.

The **Delegated Administration Properties** dialog box opens.

Figure 4.84 ~ View Properties Delegated Administration dialog box.

Modifying Delegated Administration Roles

To modify a delegated administration role

1. Use the Navigation aid to go to **Directory, Zone, Configuration, Delegated Administration.**

2. In the workspace, select the delegated administration role that you want to modify.

3. In the **Model Administration** task group, click **Modify**.

   The **Modify Delegated Administration** dialog box opens.

Figure 4.85 ~ Modify Delegated Administration dialog box .

4. Make any necessary changes. For detailed information about configuring delegated administration roles, see *Adding Delegated Administration Roles* on page 220.

5. Click **Modify** to save your changes.

   OR

   Click **Reset** to undo the changes that you made to this role.

OR

Click **Cancel** to close this dialog box without saving your changes.

The **Delegated Administration Properties** dialog box opens and you can review your changes.

Removing Delegated Administration Roles

To remove a delegated administration role

1. Use the Navigation aid to go to **Directory, Zone, Configuration, Delegated Administration.**

2. In the workspace, select the delegated administration role that you want to remove.

3. In the **Model Administration** task group, click **Remove**.

   The **Remove Delegated Administration** message opens.

Figure 4.86 ~ Remove Delegated Administration message.

4. Click ✔ to confirm that you want to remove the Delegated Administration role from the Radia Management Portal Directory.

   OR

   Click ✖ to indicate that you do not want to remove the Delegated Administration role.

Querying a User's Delegated Administration

Use the **Query User's Delegated Administration** task in the **Model Administration** task group to display information about the selected user's role.

To query a user's delegated administration

1. Use the Navigation aid to go to **Directory, Zone, Administrators & Operators**.

2. In the workspace, select the appropriate user.

3. In the **Operations** task group, click **Query User's Delegated Administration**.

   A table similar to the following appears.

Figure 4.87 ~ Delegated Administration Properties dialog box for a user.

4. Click any link in the table to view the properties for that object.

Configuring Administrators and Operators

The **Administrators & Operators** container in the Radia Management Portal Zone Directory stores authentication information. Every administrator must be added at the top level of this container. After adding administrators and assigning them to groups, you can assign them to the appropriate delegated administration policies. See *Modifying Delegated Administration Roles* on page 229 for more information.

Adding Users

When adding a user, assign the person a unique user ID and password. You can also assign the user to groups. If LDAP Authorization has been enabled for all users, you can assign an External User ID or disable LDAP authorization for this user.

Note
External LDAP Authentication is disabled for all users by default. To enable it, see *Configuring for External LDAP Authentication* on page 159 for details.

To add a user

1. Use the Navigation aid to go to **Directory**, **Zone.**

2. In the workspace, click **Administrators & Operators**.

Figure 4.88 ~ Authority is Zone, Administrators and Operators.

Chapter 4

3. In the **Model Administration** task group, click **Add Person**.

The **Add Person** dialog box opens.

Figure 4.89 ~ Add Person dialog box.

4. In the **User ID** text box, type the user name.

Caution
The User ID for the object must be unique. If you attempt to create an object with a user ID that has already been used, an error appears in the workspace indicating that the object already exists.

5. In the **Description** text box, type a description that will appear in the Details view.

6. In the **Display Name** text box, type a name for the user that will appear in the Radia Management Portal.

8. In the **User Password** text box, type the user's password. Specify the password associated with the External User ID if external authentication is turned on for this user.

Passwords may include alphanumeric characters as well as spaces and special characters, such as #, $, and \.

7. In the **External User ID** text box, type an external user ID that should be accepted for authentication by an external service, such as AD or another LDAP service.

Note

The out-of-the-box default for external LDAP Authentication is **off**. To enable the default value to **on**, see *Configuring for External LDAP Authentication* on page 159.

---

8. Using the **External authentication?** radio buttons, select whether or not to permit external authentication of this person when LDAP authentication has been enabled for the Radia Management Poral. Select **No** to disable external authentication for this user. Select **Yes** to enable external authentication for this user.

9. Click **Add**.

    The **Modify Person** dialog box opens.

Note

Instead of radio buttons, the External authentication? values on the Modify Person dialog box are viewed or entered using the numbers **1** for **on**, and **0** for **off**.

---

10. From the **Available** list, select one or more groups to add the user to.

11. Click [▶▶] to add the selected groups to the **Selected** list.

    OR

    If you want to select all of the groups in the list, you do not need to select anything from the **Available** list. Simply click [▶▶|] to add all of the groups to the **Selected** list. See *Selecting an Audience* on page 287 for more information about how to use this dialog box.

Figure 4.90 ~ Modify Person dialog box.

12. Click **Modify**.

The **Person Properties** dialog box opens.

Figure 4.91 ~ Person Properties dialog box.

Modifying Users

To modify a user

1. Use the Navigation aid to go to **Directory, Zone**.

2. In the workspace, click **Administrators & Operators**.

3. Select the user that you want to modify.

4. In the **Model Administration** task group, click **Modify**.

The **Modify Person** dialog box opens.

Figure 4.92 ~ Modify Person dialog box.

5. Make any necessary changes. For detailed information about configuring users, see *Adding Users* on page 232.

> **Note**
>
> Instead of radio buttons, the External authentication? field on the Modify Person dialog box displays a text box. Valid values are the numbers **1** for **Yes** (allow external authenticaton for this user), and **0** for **No** (disable external authentication for this user).

6. Click **Modify** to save your changes.

OR

Click **Reset** to undo the changes that you made to this role.

OR

Click **Cancel** to close this dialog box without saving your changes.

The **View Properties** dialog box opens and you can review your changes.

Removing Users

To remove a user

1. Use the Navigation aid to go to **Directory, Zone**.

2. In the workspace, click **Administrators & Operators**.

3. Select the user that you want to remove.

4. In the **Model Administration** task group, click **Remove**.

   The **Remove Person** message opens.

Figure 4.93 ~ Remove Person message.

---

5. Click ✔ to confirm that you want to remove the user from the Radia Management Portal Directory.

   OR

   Click ✖ to indicate that you do not want to remove the user.

Adding User Groups

To add a group

1. Use the Navigation aid to go to **Directory**.

2. In the workspace, click **Administrators & Operators**.

Figure 4.94 ~ Authority is Zone, Administrators & Operators.

3. In the **Model Administration** task group, click **Add Group**.

The **Add Group** dialog box opens.

Figure 4.95 ~ Add Group dialog box .

4. In the **Common Name** text box, type a name for the container object.

Caution

The Common Name for the object must be unique. If you attempt to create an object with a name that has already been used, an error appears in the workspace indicating that the object already exists.

---

5. In the **Display Name** text box, type a name for the group that will appear in the Radia Management Portal.

6. In the **Description** text box, type a description that will appear in the Details view.

7. Click **Add**.

The **Modify Group** dialog box opens.

Figure 4.96 ~ Modify Group dialog box.

8. From the **Available** list, select the users and groups that you want to assign to this group.

9. Click ▶▶ to add the selected users to the **Selected** list.

OR

If you want to select all of the users in the list, you do not need to select anything from the **Available** list. Simply click ▶▶ to add all of the users to the **Selected** list. See *Selecting an Audience* on page 287 for more information about how to use this dialog box.

10. Click **Modify**.

The new group is added to the Administrators & Operators containers.

11. To display the Properties, click the View Properties icon in the toolbar: 🔍.

The **Group Properties** dialog box opens and you can review your changes.

Figure 4.97 ~ Group Properties dialog box for added group.

Modifying Groups

To modify a group

1. Use the Navigation aid to go to **Directory, Zone**.

2. In the workspace, click **Administrators & Operators**.

3. Select the group that you want to modify.

4. In the **Model Administration** task group, click **Modify**.

   The **Modify Group** dialog box opens.

Figure 4.98 ~ Modify Group dialog box.

5. Make any necessary changes. For detailed information about configuring users, see *Adding User* Groups on page 240.

6. Click **Modify** to save your changes.

   OR

   Click **Reset** to undo the changes that you made to this role.

   OR

   Click **Cancel** to close this dialog box without saving your changes.

Use the **View Properties** icon in the toolbar to review your changes: 🔍.

Removing Groups

To remove a group

1. Use the Navigation aid to go to **Directory, Zone**.
2. In the workspace, click **Administrators & Operators**.
3. Select the group that you want to remove.
4. In the **Model Administration** task group, click **Remove**.

   The **Remove Group** message opens.

Figure 4.99 ~ Remove Group message .

---

5. Click ✔ to confirm that you want to remove the group from the Radia Management Portal Directory.

   OR

   Click ✖ to indicate that you do not want to remove the group.

Managing the Portal Zone Directory

The Radia Management Portal Zone Directory, zone.mk, together with the set of metakit (*.mk) files that it loads as services, contains all configuration and entitlement information for the Radia Management Portal Zone, as well as infrastructure and job status and history information. This section describes how to backup, restore, or query the Radia Management Portal Directory, as well as how to import and export subsets of the Radia Management Portal Directory.

Creating a Backup of the Portal Zone Directory

Use the **Backup Directory** task to create a backup copy of the entire Radia Management Portal Zone Directory. If you are entitled to create backups, this task is available when you navigate to the authority of **Zone**.

■ Before running a backup, we recommend reading the topic *Backup Directory Naming, Contents, and Maintenance* on page 245.

■ The procedure *To backup the Radia Management Portal Directory* begins on page 247.

■ If you would like to export a portion of the Radia Management Portal Directory, see *Exporting Data from the Portal Directory* on page 253 for more information.

> **Note**
>
> Prior to release 2.0, the Backup Directory task created a single directory file, rmp.mk. As of release 2.0, the rmp.mk directory file no longer exists. Instead, the Radia Management Portal directory is represented by the zone.mk directory file together with the set of *.mk files that the zone loads as services.

Backup Directory Naming, Contents, and Maintenance

This topic explains where backups are located, named, their contents, and how you can easily use the naming convention to have the Radia Management Portal automatically maintain the backups for you.

Each backup creates a new subdirectory in the **\etc\backup** directory of where the Radia Management Portal was installed. By default, this location is:

⟨SystemDrive⟩:¥Novadigm¥IntegrationServer¥etc¥backup¥

Backup Subdirectory Name

A backup's subdirectory name is composed of a user-assigned name, appended by the creation date and time of the backup. The prefix is the name assigned during the Backup Directory task. The addition of the creation date and time makes it easy to identify the appropriate backup directory for a restore.

Thus, the full name of each backup directory includes the format:

<name>.YYYYMMDD-HHMM

> *where:*
>
> - **<name>** is the user-entered name entered for the backup directory.
> - **YYYYMMDD** is the backup date in year, month, and day format.
> - **HHMM** is the backup time in hours and minutes.

Figure 4.100 shows a sample backup subdirectory created after running the Backup Directory task. The directory prefix of **chicagodaily** reflects the name given during the backup task. The date and time is appended to the given name. This backup was created in 2004 on April 30th, at 3:07 pm.

Figure 4.100 ~ Backup subdirectory and contents.

Backup Subdirectory Contents

The backup subdirectory includes the **zone.mk** file, as well as additional directories that contain the *.mk files for the zone's configuration and loaded services. Table 4.12 summarizes the location of additional *.mk files in a typical zone backup subdirectory.

Table 4.12 ~ Sample Backup Subdirectory Contents	
Location	**Contents (*.mk files)**
<<backup-subdirectory>>\zone	device, group, user, xref
<<backup-subdirectory>>\zone\config	entitlement, msg, task
<<backup-subdirectory>>\zone\jobs	history
<<backup-subdirectory>>\zone\network	dns, lanmanredirector

Backup Directory Maintenance

The Radia Management Portal automatically manages backup directories using the assigned-name prefix. It saves up to seven sets of backups with the same assigned name. After that, it

deletes the oldest one when a new one is saved. If you assign the same name to a daily backup, this allows you to keep seven days of backups. If you assign another name to a backup made once a week, this means you can keep seven weeks of backups.

> **Tip**
>
> Create a Radia Management Portal backup job to run periodically to ensure that you back up data. If you create a daily backup with the same assigned name, the appended dates and times will keep the backup directories unique. The Radia Management Portal keeps up to seven backup directories with the same initial name, then automatically deletes the oldest one when the next one is saved.

To backup the Radia Management Portal Directory

1. Use the **Navigation aid** to go to the **Zone** level.

2. In the **Directory Management** task group, click **Backup Directory**.

   The **Submit Backup**—**Backup Opts** dialog box opens.

Figure 4.101 ~ Submit Backup—Options dialog box.

3. In the **Filename** text box, type a name for the **subdirectory** for this backup within the backup directory. The creation date and time of the backup will be appended to this assigned name. Thus, the directory name for this backup will be:

   <assigned name>.YYYYMMDD-HHMM

   For details, see *Backup Directory Naming, Contents, and Maintenance* on page 245.

4. Click **Next**.

The **Schedule** dialog box opens.

5. In the **Schedule** dialog box, specify when you want this job to run. Backups may be scheduled once or periodically. For more information, see *Scheduling Jobs* on page 289.

6. Click **Next**.

   The **Submit Backup—Summary** dialog box opens.

Figure 4.102 ~ Submit Backup—Summary dialog box.

---

7. Click **Submit**.

   A list of the jobs appears. Now, you can use the **View Properties** task to view detailed information, such as the status of the job. See *Viewing Properties* on page 274 for more information.

8. Go to **<*SystemDrive:*>\Novadigm\IntegrationServer\etc\backup** to access the backup directories for the Radia Management Portal.

   The Radia Management Portal maintains up to seven backup directories with the same assigned name, then automatically purges the oldest one if an eighth one is created. This allows you to keep seven daily backups with the same name, and keep seven weekly backups with the same assigned name.

Restoring the Portal Directory

Use the **Restore Directory** task to restore a backup of the entire Radia Management Portal Directory.

To restore the Radia Management Portal Directory

1. Use the **Navigation aid** to go to the **Zone** level.

2. In the **Directory Management** task group, click **Restore Directory**.

   The **Submit Restore—File** dialog box opens.

Figure 4.103 ~ Submit Restore—File dialog box.

3. From the **Name** list, select the backup that you want to restore.

   Use the appended date-time stamps of the backups to select a backup directory based on its creation date. The format of the date-time stamp used is: YYYYMMDD-HHSS, which indicates the Year Month Day – Hours Minutes. For example, the name **chicagodaily.20030515-1641** represents a backup created in the year 2003 on May 15 at 16:41, or 4:41 PM.

4. Click **Next**.

   A confirmation dialog box opens.

Figure 4.104 ~ Submit Restore—Confirm dialog box.

5. Click ✔ to confirm that you want to restore the Radia Management Portal Directory.

   OR

   Click ✖ to indicate that you do not want to restore the Radia Management Portal Directory.

6. After the confirmation of a restore, the **Finish** dialog box opens when the restore is complete. Click **Finish** to continue.

Figure 4.105 ~ Submit Restore—Finish dialog box.

The restore of the selected backup is complete.

Querying the Portal Directory

Use the **Query** task icon on the Toolbar to locate objects in the Radia Management Portal Directory. You may use the results of the query to view information, or to select the authority for a job.

To perform a query

Use the **Navigation aid** to go to the place in your infrastructure where you want to perform a query.

Click the **Query** icon on the Toolbar ![icon] .

The **Query Directory** dialog box opens.

Figure 4.106 ~ Query Directory dialog box.

In the **Type of Query** area, select the **Query Depth**.

● **One Level**
Queries one level below the selected Authority.

● **Current Level & All Below**
Queries the current level and all levels below the selected Authority.

From the **Query Filter** drop-down list, select the type of object that you want to find.

For example, if your selected authority is **Administrators & Operators**, you might select **Users** from this drop-down list so that your query results contain only the users that match your criteria.

The fields in the **Query Constraints** area change based on this selection.

If you want to constrain your query, type the appropriate information in the text boxes listed in the **Query Constraints** area.

Notes

You can use wildcards in these text boxes. For example, if you want to search for all Administrator and Operators, users and groups, beginning with the letter "a":

1. Select **Current Level & All Below** in the **Query Depth** area.
2. Select **Administrators & Operators** from the **Query Filter** drop-down list.
3. In the **Common Name** text box, type **a***.

A list of all Administrators and Operators, users and groups, beginning with the letter "a" is returned.

You can also search for more than one pattern in the **Common Name** text box by typing the following characters directly between each pattern (do not use spaces): **)(cn=**
For example, if you want to search for all users and groups beginning with either the letter **a** or the letter **o**:

1. Repeat steps 1 and 2, above.
2. In the **Common Name** text box, type **a*)(cn=o*** .

A list of all Administrator & Operators, users and groups, beginning with the letters **a** or **o** is returned.

Select **Match All Constraints?** if you want the results of your query to match all of the specifications that you typed in the **Query Constraints** area.

Click **Next** to initiate the query.

The results of the query appear in the workspace.

Caution

The query results contain information intended only for viewing.

If you want to perform a task on an object in the query results, click the object to set the Authority. Then, select the appropriate task from the task group.

For example, if you searched the current level and below for Computers with a common name of **nova***, the results might appear as shown in Figure 4.107 on page 253.

Figure 4.107 ~ Results of query.

Reminder

If you want to perform a task on an object in the query results, you must click the object to set the Authority.

Exporting Data from the Portal Directory

Use the **Export** task to export a subset of your Radia Management Portal Directory to an LDIF (LDAP Data Interchange Format) file. LDIF is a standard format that allows you to transfer data between LDAP-compliant directory services in ASCII format.

The default export location is the Radia Integration Server's **\etc\export** directory.

To export the Radia Management Portal Directory

1. Use the **Navigation aid** to select the place in your infrastructure that you want to export.

2. In the **Directory Management** task group, click **Export**.

The **Query** dialog box opens.

3. Specify criteria to narrow the scope of the job. See *Performing Queries* on page 285 for more information.

4. Click **Next**.

The **Select** dialog box opens.

5. Select the audience from the **Available** list, and then click ▶▶ to add it to the **Selected** list. See *Selecting an Audience* on page 287 for more information.

6. Click **Next**.

The **Submit Export—Options** dialog box opens.

Figure 4.108 ~ Submit Export—Options dialog box.

7. In the **Name** text box, type a name for the LDIF file that will be saved in the directory.

8. Click **Next**.

The **Schedule** dialog box opens.

9. In the **Schedule** dialog box, specify when you want this job to run. For more information, see *Scheduling Jobs* on page 289.

10. Click **Next**.

The **Submit Export—Summary** dialog box opens.

Figure 4.109 ~ Submit Export—Summary dialog box.

11. Click **Submit**.

A window listing the job group opens. Click the Display Name entry to view the job properties. To return to the previous job window, click [image] on the job window toolbar. See *Viewing Properties* on page 274 for more information.

Figure 4.110 ~ Export Successful in Job Status Window.

12. Go to *SystemDrive***:\Novadigm\IntegrationServer\etc\export** to access the LDIF file that you exported from the Portal Directory.

Importing Data into the Portal Directory

Use the **Import** task to import an LDIF file into your Radia Management Portal Directory. For example, if you prefer to modify the Radia Management Portal Directory manually, in a text file, rather than through the Radia Management Portal user interface, you can export the directory, make your modifications, and then import the file into the Radia Management Portal Directory.

Caution

Be sure to back up your Radia Management Portal Directory before importing any data. See *Creating a Backup of the Portal Zone Directory* on page 245 for more information.

To import the Radia Management Portal Directory

Use the **Navigation aid** to select the place in your infrastructure where you want to place the imported data.

In the **Directory Management** task group, click **Import**.

The **Submit Import—Pick File** dialog box opens and contains a list of the files stored in the default export location (the Radia Integration Server's **\etc\export** directory).

Figure 4.111 ~ Submit Import—Pick File dialog box.

Click the file that you want to import.

Click **Next**.

The **Submit Import—Pick roots** dialog box opens. Use this dialog box to select which pieces (or, root domain names) of the imported LDIF file to compare to the existing Portal directory. For example, if you exported the entire directory, then made changes to only one area of the directory,

such as Administrators & Operators, you would select Administrators & Operators as the "root" during the import. The rest of the LDIF file will be ignored.

Figure 4.112 ~ Submit Import—Pick roots dialog box.

Click **Next**.

The **Submit Import—Import select** dialog box opens. This dialog box displays the differences between the LDIF file that you are importing and the Portal directory.

Figure 4.113 ~ Submit Import—Summary dialog box.

If necessary, use the **Nodes to display** drop-down list to limit the information that appears in the Differences area.

- Select **All** to review all items changed to the LDIF file at once.
- Select **Add** to review only those items that have been added to the LDIF file.
- Select **Delete** to review only those items that have been removed from the LDIF file.
- Select **Modify** to review only those items that have been modified in the LDIF file.

In the **Differences** area, click the items that you want to accept as changes. For example, if you want to add **Test User** to the Portal Directory, click ⊕.

OR

If you want to accept all of the changes, click **Select All**.

The items that you selected are added to the appropriate list below. If you want to remove an item from the list, click its name.

Figure 4.114 ~ Submit Import—Import Select dialog box.

Click **Commit**.

The items are added to the Portal directory.

Figure 4.115 ~ Result of import to Portal directory.

Updating Tasks

Use **Update Tasks** to update the tasks available to you when you receive a new build of the Radia Management Portal.

To update tasks

Stop the Radia Management Portal. See *Starting and Stopping the Radia Management Portal* on page 55 for more information.

Copy the new **rmp.tkd** into the **\modules** folder of your Radia Integration Server directory (by default *SystemDrive*:\Novadigm\IntegrationServer\modules).

Start the Radia Management Portal. See *Starting and Stopping the Radia Management Portal* on page 55 for more information.

Use the **Navigation aid** to go to the **Zone Configuration Tasks** container.

In the **Directory Management** task group, click **Update Tasks**.

Figure 4.116 ~ Navigate to the Zone Configuration Tasks container to Update Tasks.

The **Update tasks – Select** dialog box opens.

Figure 4.117 ~ Update tasks – Select dialog box.

If necessary, use the **Nodes to display** drop-down list to limit the information that appears in the Differences area.

- Select **All** to review all task changes at once.
- Select **Add** to review only those tasks that can be added to the Radia Management Portal.
- Select **Delete** to review only those tasks that can be removed from the Radia Management Portal.
- Select **Modify** to review only those tasks that can be changed in the Radia Management Portal.

In the **Differences** area, click the items that you want to accept as changes.

OR

If you want to accept all of the changes, click **Select All**.

The tasks that you selected are added to the appropriate Add, Delete, or Modify list. If you want to remove a task from the list, click its name.

Figure 4.118 ~ Submit Update – Update- tasks- select dialog box.

Click **Commit**.

The selected tasks (shown in the Add, Delete, and Modify areas) are updated in the Radia Management Portal Tasks container.

Managing Jobs

The Jobs container in the Radia Management Portal Zone Directory stores objects that represent all of the current jobs in the system, and jobs completed within the past four days.

Note
Jobs can be viewed in the History Container as soon as they are executed. See *Viewing Job History* on page 273.

Filtering Job Groups or Jobs by Status

Use the Status list box on the Authority toolbar to quickly filter a Jobs container display by job status. For example, if you are viewing all Jobs (that is, a list of all Job Groups), select a Status of "Failed" to view only the Job Groups having one or more failed jobs. Or, if you are viewing a specific Job group, you can select a status of "Waiting to Start" to see how many jobs in the group have yet to run.

Note
Use the Query Jobs task to further locate a set of jobs that meet additional criteria, such as a scheduled start time or period, the target audience, and who submitted the job or job group. For details, see *Querying Jobs or Job Groups* on page 267.

To filter Jobs by Status

1. Use the Navigation aid to go to **Directory, Zone** containers.
2. In the workspace, click **Jobs.**
3. From the toolbar, open the **Status** drop-down list, and click a job status.

Figure 4.119 ~ Viewing Jobs for a selected Status.

The workspace displays only the jobs with the selected status.

4. To return to a view of all jobs in the container, open the **Status** drop-down list, and select **ALL.**

Modifying Job Groups

Use the **Modify** task to make changes to job groups that are not currently in progress.

To modify a job group

1. Use the Navigation aid to go to **Directory, Zone** containers.

2. In the workspace, click **Jobs**.

3. Select the job group that you want to modify.

4. In the **Model Administration** task group, click **Modify**.

The **Modify Job Group** dialog box opens.

Figure 4.120 ~ Modify Job Group dialog box.

5. Modify the job as necessary.

- In the **Name** text box, change the name of the job group.

- In the **Description** text box, change the description of the job group.

- In the **Tracing Enabled?** field, select the **on** option so that additional messages are written to the log about the execution of the job group. It is recommended that you leave this option set to **off** unless otherwise instructed by HP Technical Support.

- In the **Jobs running at any time** text box, type the total number of jobs that can be active at any time within this job group. An entry of 0 means there is no limit. The default is 30.

- In the **Start in batches of** text box, type the number of jobs that can start within a specified time period, as defined by the following **Per seconds** field. An entry of 0 (zero) means there is no limit.

- In the **Per seconds** text box, specify the time period (in seconds) to wait before starting the next batch of jobs. An entry of 0 (zero) means there is no limit. The default is one batch per minute, or per 60 seconds.

- In the **Run** drop-down list box, change how often the job group runs.

- In the **Starting on** drop-down list box, change the date and time when the job group should start.

6. When you are done making changes, click **Modify**.

The changes are saved and the Job Group is the selected Authority.

Querying Jobs or Job Groups

Use the **Query Jobs** task in the **Model Administration** task group to locate existing jobs or job groups, review their status, and make changes to the job groups. You can focus your query on jobs or job groups or both, and limit your query to a scheduled start time or period, a specific job status (such as Failed), the target audience, and who submitted the job or job group. For example, you can query all jobs that failed in the last 12 or 24 hours.

To perform a query for a job or job group

1. Use the Navigation aid to go to the **Directory, Zone** containers.

2. In the workspace, click **Jobs**.

3. In the **Model Administration** task group, click **Query Jobs**.

The **Query Job Group** dialog box opens.

Figure 4.121 ~ Query Job Group dialog box.

Use the **Time Window** area to limit your query to those jobs or job groups scheduled to start between the dates and times you select.

4. In the **Scheduled From Time** drop-down lists, select the earliest date and time when the job or job group was scheduled to start.

5. In the **Scheduled To Time** drop-down lists, select the latest date and time when the job or job group is scheduled to start.

    Use the **Display Selection** area to specify whether you want to limit your query to Jobs, to Job Groups, or to both Jobs and Job Groups.

6. In the **Display** drop-down list, select **Jobs** or **Job Groups**.

> **Note**
>
> If you want to restart failed jobs, query for **Job Groups**. The **Restart Failed Jobs** task is only available at the level of a **Job Group**.

Use the **Job Characteristics** area to further limit your query.

7. Select **Match All Constraints?** if you want the results of your query to match all of the specifications that you will set in the fields below.

8. In the **Job Status** drop-down list, optionally select a specific job status to limit the query to jobs or job groups with that status. Specific job statuses include **Waiting to Start**, **Successful**, **Failed**, **Active**, and **Disabled**.

9. In the **Target Audience** text box, optionally type the name of the computer on which the job or job group is being performed. You can use the asterisk (*) as a wildcard in your entry.

10. In the **Created By** text box, optionally type the logon ID of the user who scheduled the job or job group. You can use the asterisk (*) as a wildcard in your entry.

11. Click **Next**.

    A list of the jobs or job groups that match the criteria opens.

Status: Failed   [0-9] [A-E] [F-J] [K-O] [P-T] [U-Z] **[ALL]**   1 - 2 of 2 items

Install Management Agent	Ended with Errors	Portal Administrator	2003/01/16:12:55
Notify By Device	Failed	Portal Administrator	2003/01/14:12:20

Figure 4.122 ~ Results of a query for failed job groups.

Restarting Failed Jobs in a Job Group

Go to the **Jobs** container, and display a job group containing one or more failed jobs.

Notes
If the jobs failed due to an incorrect User log on or Password, restarting and/or modifying the job will not fix the problem. You must create a new job with the correct Administrator-authorized User and Password entries.

Figure 4.123 ~ Restart Failed Jobs.

Click **Restart Failed Jobs** from the **Model Administration** task group to restart the failed jobs in this job group.

The jobs are restarted immediately, as shown in the active jobs page (see *Figure 4.124 ~ Restarted failed jobs of Install Management Agent show active status* on page 270).

Figure 4.124 ~ Restarted failed jobs of Install Management Agent show active status.

Close the job status page when the restarted jobs finish.

Stopping Job Groups

Use the **Stop** task to stop an active job group from running. If the job group is set to recur, it will run as scheduled in the future.

Note
This task applies to job groups only and is not available for individual jobs.

To stop job groups

Use the Navigation aid to go to the **Directory**, **Zone** containers.

In the Workspace, click **Jobs**.

Click the job group that you want to stop.

In the **Model Administration** task group, click **Stop**.

A confirmation appears in the workspace.

Figure 4.125 ~ Stop Job Group message.

Click ✔ to confirm that you want to stop the job group.

OR

Click ✖ to indicate that you do not want to stop the job group.

Disabling Jobs or Job Groups

Use the **Disable** task to prevent a job or job group from being processed. You must use the Enable task to reinstate processing of a disabled job or job group.

To disable jobs or job groups

1. Use the Navigation aid to go to the authority of **Directory**, **Zone.**
2. In the workspace, click **Jobs**.
2. Click the job or job group that you want to disable.
3. In the **Model Administration** task group, click **Disable**.

    A confirmation appears in the workspace.

Figure 4.126 ~ Disable Job Group message.

4. Click ✔ to confirm that you want to disable the job or job group.
    OR
    Click ✖ to indicate that you do not want to disable the job or job group.

Enabling Jobs or Job Groups

Use the **Enable** task to restart a disabled job or job group the next time it is scheduled to run.

To enable jobs or job groups

Use the Navigation aid to go to the **Directory**, **Zone** containers.

In the workspace, click **Jobs**.

Click the job or job group that you want to enable.

In the **Model Administration** task group, click **Enable**.

A confirmation appears in the workspace.

Figure 4.127 ~ Enable Job Group message.

Click ✔ to confirm that you want to enable the job or job group.

OR

Click ✖ to indicate that you do not want to enable the job or job group.

Removing Jobs or Job Groups

Use the **Remove** task to completely disable a job or job group and remove it from the list of jobs.

To remove jobs or job groups

Use the Navigation aid to go to the authority of **Directory**, **Zone.**

In the workspace, click **Jobs**.

Click the job or job group that you want to remove.

In the **Model Administration** task group, click **Remove**.

A confirmation appears in the workspace.

Figure 4.128 ~ Remove Job Group message.

Click ✔ to confirm that you want to remove the job or job group.

OR

Click ✖ to indicate that you do not want to remove the job or job group.

Viewing Job History

The History Container stores daily histories of all executed jobs, displayed in reverse date and time order. Jobs are written to the current day's history file as soon as execution stops (with or without errors).

To view job history

Use the Navigation aid to go to the **Directory, Zone** containers.

In the workspace, click **Jobs**.

In the workspace, click **History**.

Job histories are listed in reverse chronological order by date and time. History files include the date in the format: YYYYMMDD.

Click the history file for the date whose jobs you want to review.

> **Note**
>
> Click Details to view a concise summary of the job groups for that day.

Figure 4.129 ~ History file for jobs on April 30, 2004.

Click a specific job group from those displayed in the workspace.

The workspace lists the jobs that ran in that job group.

Click a job in the workspace.

The **Job Properties** dialog box displays the details of the job.

Viewing Properties

Click the **View Properties** icon ![icon] on the toolbar to display the properties for an object or a job. The properties that appear vary based on the selected object.

Figure 4.130 ~ Group Properties dialog box.

Most Properties pages will display the group areas shown in Figure 4.130: Properties and Object Information. To easily navigate a Properties page:

■ Click one of the top labels to jump to that group area. Some objects contain an **Advanced** label giving you access to advanced properties for that object.

■ Click on a **Back to top** label to return to the top of the page.

Any items <u>underlined</u> on a Properties page represent an active link to that object. For example, in the previous figure, all Members listed in the Properties area and the Parent Object in the Object Information area are underlined.

■ Click on any underlined object to jump to that object's Properties.

■ Use the **Back** button on your web browser to return.

Summary

■ Run **Update Tasks** when you receive a new build of the Radia Management Portal to update the tasks available to you.

■ You can add, modify, and remove task groups.

■ Adding **delegated administration roles** is a three step process that consists of:

● Assigning administrators and operators to a role.

● Specifying the tasks that the administrators and operators in the role will have access to.

● Selecting where, in the infrastructure, the administrators and operators can perform the tasks.

■ Use the **Backup Directory** task to backup the entire Radia Management Portal Zone Directory. The creation date and time is appended to the given backup directory name to make it easy to select the appropriate backup directory for a restore.

■ Use the **Restore Directory** task to restore a backup of the entire Radia Management Portal Zone Directory.

■ Use the **Export** task to export a subset of your Radia Management Portal Directory to an LDIF file.

■ Use the **Import** task to import an LDIF file into your Radia Management Portal Directory.

■ Use the **Move/Copy Devices** task to move devices among your Groups defined in the Groups container.

■ Use the **Query Jobs** task to locate existing jobs or job groups, or both, by scheduled start time, status, submitter, or target audience. From the results of the query, you can view job properties and even make changes to a job or job group.

■ Use the **Modify, Disable, Enable, Remove, and Stop** tasks to manage your jobs or job groups.

■ Use the **Restart Failed Jobs** task to restart all failed jobs in a job group.

■ Use the **History container** to review jobs already executed.

■ Use the **View Properties** task to display the properties for any object. From any Properties page, you can use the links available with a member or parent object's listing to jump to the properties page from that object.

5

Operations Functions

At the end of this chapter, you will:

■ Be familiar with the lifecycle of every task.

■ Be familiar with the basic procedures that you will follow for every operations task.

■ Be able to select computers for management by the Portal Zone.

■ Be able to use Help Desk Notify to quickly notify a computer by name.

■ Be able to install the Radia Clients using default or customized profiles.

■ Be able to add, modify, or delete Client Install Profiles.

■ Be able to install the Radia Management Agent using a Dynamic or Static port assignment.

■ Be able to install the Radia Proxy Server.

■ Be able to synchronize the Radia Proxy Server.

■ Be able to install and open a remote Radia Management Portal Zone.

■ Be able to add Task Templates for scheduling jobs.

■ Be able to schedule jobs to run in multiple Radia Management Portal Zones.

■ Be able to run a sequence of jobs in a single task.

■ Be able to use Remote Control to manage Radia Clients.

The Radia Management Portal offers several core tasks. A *task* is an activity that a person performs to initiate a job. A *job* is a unit of work performed by the computer that is initiated by a person (via a task) or a scheduled operation.

> ### Note
>
> This chapter discusses the operational details of how to perform these tasks using the Radia Management Portal and assumes that you have an understanding of how to use the Radia product suite.
>
> If you are not familiar with the operations, please refer to the HP OpenView web site for more information.

The core tasks in the Radia Management Portal are:

■   **Manage Computer**
Click **Manage Computer** to explicitly bring one or more computers into your Radia Management Portal Zone. Managed computers have an entry in the RMP Zone Devices container, and an automatic membership in the Default Group. For details, see *Managing Computers from your Radia Management Portal Zone* on page 280.

■   **Add Task Template**
Use **Add Task Template** to preset the options for a Task Type, such as Notify or Install RPS, as a saved Task Template. Task templates can be selected and applied during the Schedule Zone Operations task, as well. **Add Task Template** is available from the Task Template container within the Zone, Configuration container.

■   **Install Client**
Click **Install Client** to install the Radia Client on remote computers. See *Installing the Radia Client* on page 314 for more information. Multiple Client Install Profiles are supported. For details, see *Supporting Remote Installs Using Multiple Profiles* on page 320.

■   **Install Management Agent**
Click **Install Management Agent** to install the Radia Management Agent on remote computers. See *Installing the Radia Management Agent* on page 307 for more information.

■   **Install Proxy Server**
Click **Install Proxy Server** to install the Radia Proxy Server on remote computers. See *Installing the Radia Proxy Server* on page 329 for more information.

■   **Synchronize Proxy Server**
Click **Synchronize Proxy Server** to force the Radia Proxy Server to connect to the Radia Configuration Server to preload the files to the static cache on the Radia Proxy Server. See *Synchronizing the Radia Proxy Server* on page 335 for more information.

■   **Purge Dynamic Cache**
Click **Purge Dynamic Cache** to purge the dynamic cache of the Radia Proxy Server. See *Purging the Dynamic Cache of the Radia Proxy Server* on page 336 for more information.

■   **Notify**
Use the **Notify** tasks to perform an action on the selected audience. See *Using the Notify Tasks* on page 291 for more information.

■ **Help Desk Notify**
Click the **Help Desk Notify** icon on the toolbar to quickly Notify a single computer, whose name you already know. See *Using Help Desk Notify* on page 295 for more information.

■ **Sequence Task**
Use **Sequence Task** to enter and submit a series of jobs, in a single step, from a master portal. Access the task from the **Jobs** container. Sequencing jobs can be an efficient tool for managing jobs common to many devices across many zones. Future plans include the ability to select conditions that must be met before executing the next job in the sequence.

■ **Install Radia Management Portal**
Click **Install Radia Management Portal** to remotely install another Radia Management Portal Zone in your infrastructure. See *Installing Additional RMP Zones (Subordinate Zones)* on page 344 for more information. Also refer to the tasks for **Open Subordinate Zone** and **Schedule Zone Operation**.

■ **Update RMP**
Click **Update RMP** to remotely update the code delivered with a new build to the subordinate Radia Management Portal Zones in your infrastructure. See *Updating Subordinate RMP Zones* on page 349 for more information.

■ **Open Subordinate Zone**
Click **Open Subordinate Zone** to quickly access the Radia Management Portal of another Zone in your enterprise from the **Zone Access Points** container. See *Opening a Subordinate Zone* on page 356 for more information.

■ **Schedule Zone Operation**
Click **Schedule Zone Operation** from the **Zone Access Points** container to run a Notify or Install RPS job on all devices in each of the selected zones in your enterprise. The job options must be predefined as a Task Template. See *Scheduling Zone Operations* on page 349 for more information.

Managing Computers in Your Radia Management Portal Zone

Use the **Manage Computer** task to bring the computers in your network or external directories under the control of the Radia Management Portal Zone explicitly.

> **Important Note**
>
> There are other ways to add devices to your RMP Zone. For details, see *Adding Devices to an RMP Zone* on page 165 of *Chapter 4: Administrative Functions*.
>
> As of RMP 2.0.1, you do not need to perform the Manage Computer task prior to performing an install task against a device in your Network or LDAP directory. Prior to performing the install, the RMP will bring any selected devices under management automatically.

The **Manage Computer** task:

■ Places the selected computer(s) in the **Zone Devices** container, which establishes it as a unique *device* in the Zone directory.

■ Makes the devices members of the **Zone Groups** container **Default Group**.

Once a device is under management of the Radia Management Portal Zone, it can be selected for an operation or for other group memberships.

Use the following procedures to manage computers that are located in your network. If your Administrator has configured access to an Active Directory, you can also use the same procedures to manage computers that exist in locations in your Active Directory.

To manage a computer in your network

> **Note**
>
> As of RMP 2.0.1, you do not need to perform this task before running an install task; the RMP install tasks will automatically bring a device in your network under management before proceeding with the install.

Use the **Navigation aid** to go to the **Zone Networks** container.

In the Workspace, select the Network containing the computer to be managed. For example, **Microsoft Windows Network**.

In the Workspace, navigate through the Network hierarchy to the computer object. For example, select the **Domain** and then select the **Computer**.

Figure 5.1 ~ Selected computer in Domain of Microsoft Windows Network.

Click **Manage Computer** in the **Operations** task group.

At this point, the Radia Management Portal creates a unique device entry in the Zone Devices container for this computer. The Navigation location switches to the Device object in the Devices container.

Figure 5.2 ~ Radia Management Portal after selecting Manage Computer task.

Notice that the Operation task group now displays many tasks that are available for this managed Device. To take the best advantage of the Radia Management Portal, after adding a device you'll want to:

● Move or copy it into all appropriate Groups of devices that are needed for operations on this device. For details, see *Moving or Copying Devices into a Group* on page 195.

● Install the Radia Management Agent on the Device to make use of Cross References groups. For more advantages of adding the Radia Management Agent, see *Installing the Radia Management Agent* on page 307.

To manage a group of computers in your network

Note

As of RMP 2.0.1, you do not need to perform this task before performing an install task; the RMP install tasks will automatically bring any devices in a targeted network group under managemement before proceeding with the installs.

Before selecting a group of computers, you should become familiar with the dialogs to browse and select devices for a group as discussed in *Basic Procedures for Modifying Groups on page 166*.

Navigate to the **Zone, Networks** container.

Navigate to a Network level containing the group of computers that you want to have managed by the Radia Management Portal.

Click **Manage Computer** in the Operations task group.

Complete the selection of the computers to be brought under management.

Click **Modify**.

All selected computers are added to the **Zone, Devices** container and the **Default Group** of the Zone Groups container.

To move or copy these devices into different groups, see *Moving or Copying Devices into a Group* on page 195.

To manage one or more computers located in Active Directory

> **Note**
>
> As of RMP 2.0.1, you do not need to perform this task prior to performing an install task; the RMP install tasks will automatically bring selected LDAP directory devices under management before proceeding with an install.

An Active Directory can be configured for access by a Radia Administrator. In this case, it will appear as an object in the Radia Management Portal at the same level as your Zone.

You can use the **Manage Computer** task to add one or more computers in a connected Active Directory to your Zone Devices container.

For details on configuring or connecting to an Active Directory, see *Adding a Directory Service* on page 143.

About the Task Lifecycle

Operational tasks are performed on devices and device groups under management by the Radia Management Portal Zone. These devices and group membership exist in one of three locations:

■   Device Container (individually)

■   Groups Container (Default Group and created Groups)

■   Cross References Container Groups (groups generated from devices with installed Radia Management Agents)

To perform any operational task, you select a device or group of devices and then select the task to perform from the Operations task group. Each operational task follows a similar lifecycle, as shown in Figure 5.3 on page 284.

Figure 5.3 ~ The task lifecycle.

Select a Zone location.

Begin by navigating to a Zone location that includes the member objects on which to perform some action. These members are also called the audience of the task.

Typically, a starting location is the **Zone's Device**, **Groups**, or **Cross References** containers, depending on whether you are performing a task on either an individual device or a group of devices.

If you select a starting location with a wide device audience, a **Query** dialog opens to narrow the scope of the job. For example, if you begin a task from a navigation location of **Zone**, you can query the directory for a list of **Groups** in your Radia Management Portal Directory.

> **Important Note**
>
> The query does *not* check status information because the environment may change in the time between when the query is performed, and when the job runs.

Select the task.

The tasks available are filtered according to your selected starting location. For example, the Synchronize Radia Proxy Server task is available when the starting location is the Radia Proxy Service object under a Device object, or a Cross Reference container of all Radia Proxy Servers.

Specify job options.

The options vary depending on the selected task. For example, if you are performing a notify task, specify the command line that you want to run on the target devices.

Specify scheduling options.

Specify when you want the job to run.

Review the summary.

When you are done specifying the information for the job, a summary of your selections opens. When you are done viewing the summary, submit the job.

Basic Procedures for Operations Tasks

Because the task lifecycle is the same for each task, you will encounter several basic procedures every time you want to perform some action. When you select a task, these basic procedures

appear as a series of dialog boxes in the workspace of the Radia Management Portal. When you finish entering the necessary information, a job is created.

This section covers these basic procedures in detail.

Selecting a Starting Zone, Network, or Directory Location

When starting an operation, select a Zone location for performing the task that includes all objects on which you want to perform the task. Become familiar with the Zone containers, as discussed in *About the Zone Containers* on page 97. Different Zone containers contain different object classes.

■ Most operational tasks are started from a **Zone's Device**, **Groups**, or **Cross References** containers—depending on whether you are performing a task on either an individual device or a group of devices. For details on creating and modifying groups of devices, see *Establishing Devices and Device Groups* on page 165.

■ As of RMP 2.0.1, Install operations can also be started from locations in a **Zone, Network** container or from an **LDAP Directory Services** location. The Radia Management Portal will first bring the devices targeted for the install under management before performing the install operation.

■ Operations related to other Zones that exist in your enterprise are started from **the Zone Access Points** container.

■ For details on how to navigate to the different Zone containers, see *Navigating the Portal Directory and the Zone Containers* on page 76.

Figure 5.4 ~ Typical starting location: A group in the Zone, Groups container.

Performing Queries

Use the **Query** dialog box to narrow the scope of the job. For example, if you want to export information about all computers that begin with the letter "N", use the **Query** dialog box to search for a list of all of the computers discovered in the Microsoft Windows Network that begin with the letter "N".

_

> **Note**
>
> If you selected a single Authority, such as a particular computer, and then select a task, you will bypass the **Query** dialog box.

Figure 5.5 ~ Query dialog box.

To perform a query

1. In the **Type of Query** area, select the **Query Depth**.

   - **One Level**
     Queries one level below the selected Authority.

   - **Current Level & All Below**
     Queries the current level and all levels below the selected Authority.

2. From the **Query Filter** drop-down list, select the type of object that you want to find.

   For example, if your selected Authority is **Administrators & Operators**, you might select **Users** from this drop-down list so that your query results contain only the users that match your criteria.

   The fields in the **Query Constraints** area change, based on this selection.

3. If you want to constrain your query, type the appropriate information in the text boxes listed in the **Query Constraints** area.

> **Note**
>
> You can use wildcards in these text boxes. For example, if you want to search for all Administrator & Operators, users and groups, beginning with the letter **a**:
>
> 1. Select **Current Level & All Below** in the **Query Depth** area.
> 2. Select **Administrators & Operators** from the **Query Filter** drop-down list.
> 3. In the **Common Name** text box, type **a***.
>
> A list of all Administrator & Operators, users and groups, beginning with the letter **a** is returned.
>
> You can also search for more than one pattern in the **Common Name** text box by typing
>
> the following characters directly between each pattern (do not use spaces): **)(cn=**
> For example, if you want to search for all users and groups beginning with either the letter **a** or the letter **o**:
>
> 1. Repeat steps 1 and 2, above.
> 2. In the **Common Name** text box, type **a*)(cn=o*** .
>
> A list of all Administrator & Operators, users and groups, beginning with the letters **a** or **o** is returned.

4. Select **Match All Constraints?** if you want the results of your query to match all of the specifications that you typed in the **Query Constraints** area.
5. Click **Next** to initiate the query and to move to the next step in the task.

Selecting an Audience

Use the **Select** dialog box to narrow your audience. An *audience* is a group of devices or objects on which you want to perform some action.

> **Note**
>
> You will bypass the **Select** dialog box if:
> - Your starting Zone location is a single object when you select the task.
> - The result of the Query is a single object.

Figure 5.6 ~ Select dialog box.

This window displays the potential audience based on your starting Navigation location when you selected the task. Therefore, if you began the task from the **Zone** level, the potential audience is much greater than if your starting location is the **Zone, Administrators & Operators, Account Administrators Group**.

To select an audience

From the **Available** list, select one or more devices.

Click [icon] to add the selected devices to the **Selected** list.

OR

If you want to select all of the devices in the list, you do not need to select anything from the **Available** list. Simply click [icon] to add all of the devices to the **Selected** list.

If you want to remove devices from the audience list, select the appropriate devices from the **Selected** list and then click [icon].

OR

If you want to remove all of the devices from the list, simply click [icon] to remove all of the devices from the **Selected** list.

Click **Next** to move to the next step in the task.

Note

The next step in the task is to specify the job options. The information that you need to enter in this window varies depending on the specific task. See the instructions for the task that you are performing for detailed information.

Scheduling Jobs

Use the **Schedule** dialog box to set the scheduling options for the job. By default, a job will begin immediately and run only once. However, you can modify these settings.

Jobs are organized in a tree view. At the highest level is the Scheduler, which is used to schedule and dispatch jobs. The next level contains Job Groups, which contain groupings of jobs. For example, you might have a job group that is intended to notify 10 computers. Below this job group 10 jobs are listed—one for each computer to be notified.

Job groups are scheduled to run within a specified time frame. In order to run, the job group has to get permission from the Scheduler. Similarly, a job must get permission to run from its job group. Therefore, all jobs receive permission to run from their parent object—whether that is a job group or the Scheduler.

The Scheduler sorts jobs based on their priorities. So, if two jobs are set to run at the same time, the one with the highest priority will receive permission to run first. If the time period expires and the Scheduler has not been able to run a job, it will be cancelled.

Figure 5.7 ~ Submit Notify—Schedule dialog box (Windows).

To schedule a job

1. Complete **Scheduler Information** group items.

- For Notify jobs, in the **Job Name** text box, type a name for the job group. The Job Name appears in the **Alias** column of a Job Summary, next to the Display Name.

- In the **Description** text box, type a description for the scheduled job. The description appears in the **View Properties** dialog box for the job.

- In the **Priority** drop-down list, select the priority for the job. The Scheduler sorts all of the jobs scheduled to run at a specific time by priority.

2. Complete **Scheduler Information** group items.

3. Complete **Time Window** group items.

- In the **Run** drop-down list, specify how often you want the job to run.

The other Time Window options change based on the schedule type that you selected.

- In the **On Day** drop-down list, select which day of the week the job should run on. (*Applies only to jobs set to run Every Week*)

- In the **Starting on** drop-down lists, select:

  ♦ The date when you want the job to run.

  ♦ The time (in hours and minutes) when you want the job to run.

  ♦ How often you want the job to run (in days or hours). (Applies only to jobs set to run Every *n* Days or Every *n* Hours)

- In the **Duration** drop-down lists, indicate how long (in hours and minutes) you want the job to run. When the duration expires, the job is cancelled.

4. Complete the Job Throttling group items to limit the number of jobs running concurrently, and the number of jobs started per minute for this job group. The Job Throttling settings are especially beneficial when scheduling job groups with a large number of jobs.

- **Have a maximum of *n* jobs running at any time.**
  Accept or change the maximum number of jobs to be active at any time from this job group. The default will vary according to the job type. An entry of 0 means there is no limit.

- **And start them in batches of n jobs per minute.**
  If this number is not zero, the jobs in this job group will be batched, and one batch is started each minute. Type the number of jobs to be placed in each batch. An entry of 0 means there is no batch-size limit.

5. Click **Next** to view the **Summary** dialog box for the job.

The **Summary** dialog box contains a summary of the job. Review the summary and then click **Submit** to save the job.

Core Tasks

The Radia Management Portal contains a core set of tasks. Use this section to learn how to use each of the core tasks.

Using the Notify Tasks

The Notify tasks can be used to quickly notify a target audience or a single device.

- **Notify**
  Allows you to perform an open-ended query to create the target audience that you want to notify.

  Once Radia Management Agents are installed on devices in your Zone, you can also use the **Notify** task from the **Zone, Cross References** container groups to quickly identify a target audience based on the characteristics of a device, such as the same Hardware, Operating System, IP address Subnet, Radia Infrastructure or Managed Services.

> **Note**
>
> Use the Notify task from the Cross References container groups for Hardware, Operating System, IP address Subnet, or Radia Infrastructure to quickly identify a target audience based on device characteristics. This feature in RMP 2.x replaces the Notify by Audience task available in RMP 1.x.
>
> Use the Notify task from the Cross References Managed Services to quickly identify a target audience based on an application currently being managed by Radia. This RMP 2.x feature replaces the Notify by Subscription task available in RMP 1.x

- **Help Desk Notify**
  Click the **Help Desk Notify** icon on the toolbar to quickly Notify a single computer, whose name you already know. See *Using Help Desk Notify* on page 295 for more information.

See the *Radia Application Manager Guide* or *Radia Software Manager Guide* for more information about notifying Radia Clients.

Notifying an Audience

Use the **Notify** task to perform an action on the target devices that you select.

A group of devices can be selected as the audience for the Notify task.

> **Note**
>
> The Radia Management Portal has embedded support for Wake-on-LAN (WOL). If you attempt to notify a machine that is not "awake" and the machine supports the Wake-on-LAN capability, the Notify job will send a WOL message to wake up the machine and will subsequently try to notify the machine two more times at intervals of 120 seconds. The WOL message is sent only if the MAC address of the targeted machine is available in the machine properties.

To notify an audience

1. Use the **Navigation aid** to select the Authority.

2. From the **Operations** task group, click **Notify**.

> **Note**
>
> If you selected a single Authority, such as a particular computer, and then select a task, you will bypass the **Select** dialog box. Go to step 5.

The **Query** dialog box opens.

3. Specify criteria to narrow the scope of the job. See *Performing Queries* on page 285 for more information.

> **Note**
>
> To target one or more groups of devices for a Notify, do not select Computers as your Query Filter, since you want to select from available Group objects in the next step.

4. Click **Next**.

   The **Select** dialog box opens.

5. Select the audience from the **Available** list, and then click to add it to the **Selected** list. See *Selecting an Audience* on page 287 for more information.

6. Click **Next**.

The **Submit Notify—Notify Opts** dialog box opens.

Figure 5.8 ~ Submit Notify—Notify Opts dialog box.

7. In the **Notify Type** drop-down list, select the type of Notify that you would like to perform. The **Command** text box changes based on your selection.

In the **Command** text box, modify the command line as necessary. For example, if you select **Radia Refresh Catalog** in the **Notify Type** drop-down list, the **Command** text box is pre-filled with the following command line:

```
radskman.exe req="Refresh Catalog",mname=|mgrname|,dname=SOFTWARE,
ip=|mgr_ip|,port=|mgr_port|,cat=y
```

You must replace information between the pipes (|) with the necessary information to perform the notification. For example, you might modify the command line above to read:

```
radskman.exe req="Refresh Catalog",mname=EastCoast,dname=SOFTWARE,
ip=10.10.10.1,port=3464,cat=y
```

> **Note**
>
> If you repeat a Notify operation often, you may want to modify the appropriate Notify task so that it has default options that pertain to your organization. See *Setting Default Options for Notify Commands* on page 297 for more information.

8. In the **Port number** text box, type the port number that the Notify daemon will be listening on. By default, the port number is 3465.

9. If necessary, in the **User** text box, type the user name for the target device.

10. If necessary, in the **User Password** text box, type the password for the target device.

11. Click **Next**.

The **Schedule** dialog box opens.

12. In the **Schedule** dialog box, specify when you want this job to run. For more information, see *Scheduling Jobs* on page 289

13. Click **Next**.

The **Summary** dialog box opens.

Figure 5.9 ~ Summary dialog box.

14. Click **Submit**.

The **Job Status** window opens with list of the jobs. This dialog box automatically refreshes every 60 seconds.

Figure 5.10 ~ Job Status window.

- Click ![icon] to go up one level in the job or directory tree. For example, after viewing job details, click this icon to return to the Job Group Summary.

- Click ![icon] if you want to refresh the window to display the latest status.

- Click ![icon] to view detailed properties for the job or job group. This gives you detailed information on the job status.

- Click ![icon] to add a shortcut for Jobs to your Desktop.

- Click ![icon] to obtain a printable view of the Jobs Status page.

15. When you are done viewing the job status, click ![icon] to close the **Job Status** dialog box, and return to the Radia Management Portal.

Using Help Desk Notify

Use to quickly submit an immediate, one-time, Notify task to a specific computer whose DNS name is known. Typically, this is used by Help Desk staff working on an issue, and includes a single window to speed this one-time Notify.

The options and command syntax for the Notify task submitted through the Help Desk Notify need to be previously set or customized. For details, refer to one of the following sections:

■ *Setting Default Options for Notify Commands* on page 297.

■ *Creating Custom Notify Commands* on page 301.

To notify a single computer from the Help Desk Tasks group

From anywhere in the **Directory Zone**, click the toolbar icon for **Help Desk Notify** ![icon]

The **Submit Help Desk Notify** window opens.

Figure 5.11 ~ Notifying from the Help Desk Tasks group.

In the **DNS Host Name** field, type the DNS Host Name of the client computer to be notified.

In the **Notify Type** field, open the drop-down list and select the type of Notify to be performed. The options for each type of Notify must be preset, as discussed in *Setting Default Options for Notify Commands* on page 297.

Click **Submit**.

The selected Notify is run immediately, and the Job Status window opens.

Figure 5.12 ~ Sample Help Desk Notify Job Status Window.

Press **F5** to refresh this status window. To see the job details, click on the **Display Name** for the job.

Setting Default Options for Notify Commands

If you often repeat a Notify operation, you may want to modify the appropriate Notify task so that it has default options that pertain to your organization. To do this, you will navigate to a specific Notify task and then modify the properties for the appropriate type of Notify, such as Radia Full Connect.

Prior to using the Help Desk Notify task, you must use these procedures to preset the default options and command syntax for the available Help Desk Notify Task operations.

You can set default options for Notify operations issued from the following tasks:

■ **Help Desk Notify** (listed under H's)

■ **Notify**

To set default options for Notify commands

1. In the Navigation area, go to **Directory, Zone, Configuration**.

2. In the workspace, click **Tasks**.

3. In the workspace, click the Notify task that you want to modify, such as **Notify**.

> ### Tip
>
> Use the alphanumeric tabs and the paging arrows on the toolbar to page to the objects whose names start with those letters. For example, click **[K-O]** to quickly page to the Notify tasks. Click Next Page ▶

Figure 5.13 ~ Location of Notify tasks.

4. In the workspace, click the type of Notify operation for which you want to set defaults, such as **Refresh Catalog**.

The **Options Properties** dialog box opens.

Figure 5.14 ~ Options Properties dialog box.

---

5. In the **Model Administration** task group, click **Modify**.

The **Modify Options** dialog box opens.

Figure 5.15 ~ Modify Options dialog box.

6. Modify the fields as necessary.

   - In the **Display Name** text box, change the display name of the task.
   - In the **Command** text box, change the default command line for the Notify that you want to perform.
   - In the **Port number** text box, change the default port number that the Notify daemon will be listening on.
   - If necessary, in the **User** text box, type the default user name for the target device.
   - If necessary, in the **User Password** text box, type the default password for the target device.
   - From the **Complete When** drop-down list, indicate when the Notify is considered completed. See the HP OpenView web site for detailed information about the Radia Client and the Application Event (APPEVENT) object. If you are unsure about which option to select, select **Client Contacted**.

Complete When Selection:	Complete When Job Property:
Client Contacted	adhoc
Client Connects to RCS	radia/catalog
Client Sends Application Event	radia/service

7. Click **Modify**.

   The **Options Properties** dialog box opens and you can review your changes.

Note

The command line in *Figure 5.16 ~ Options Properties after modifying* is used for example purposes only.

Figure 5.16 ~ Options Properties after modifying.

The next time you initiate a Notify and select the notification type that you modified, such as **Refresh Catalog**, the new default settings appear in the **Submit Notify—Notify Opts** dialog box. For example, notice that the properties specified in *Figure 5.16 ~ Options Properties after modifying* on page 300 match the default settings for the fields in Figure 5.17 below.

Figure 5.17 ~ Sample Submit Notify—Notify Opts dialog box.

See *Notifying an Audience* on page 291 for more information about the **Options** dialog box.

Creating Custom Notify Commands

If you want to create your own Notify commands, you can use the **Add Task Options** task in the **Model Administration** task group.

To add a new Notify command

1. In the Navigation area, go to **Directory, Zone, Configuration**.

2. In the workspace, click **Tasks**.

3. In the workspace, click the Notify task object to which you want to specify a command. For example, click **Help Desk Notify** or **Notify.**

> ## Tip
>
> Use the alphanumeric tabs on the Authority toolbar to page to the objects whose names start with those letters. For example, click **[K-O]** to quickly page to the Notify tasks.

Figure 5.18 ~ Authority—Notify.

4. In the **Model Administration** task group, click **Add Task Options**.

Add options

Figure 5.19 ~ Add Options dialog box .

5. In the **Common Name** text box, type a name for the custom Notify task.

Caution

The Common Name for the object must be unique. If you attempt to create an object with a name that has already been used, an error appears in the workspace indicating that the object already exists.

---

6. In the **Display Name** text box, type a name for the Notify task that will appear in the infrastructure representation.

7. In the **Command** text box, type the Radia command line that you want to run on the selected target devices.

8. In the **Port number** text box, type the port that the Notify daemon is listening on.

9. In the **User** text box, type the administrator ID to obtain administrative authority on the target device's domain.

10. In the **User Password** text box, type the administrator password to obtain administrative authority on the target device's domain.

   If you do not enter the password and administrative authority is required, the job may fail. Check the job status for specific information.

11. In the **Complete When** drop-down list, select the client action that is to indicate this notify task is complete. The following table shows how your selection is reported on a **Task Property** or **Job Property** dialog box.

Table 5.1 ~ Notify Job Completion Options	
"Complete When" Selection	**"Completed When" Entry on Options Properties and Job Reports**
Client contacted	Adhoc
Client connects to RCS	Radia/catalog
Client sends APP event	Radia/service

12. Click **Add**.

The **Options Properties** dialog box opens.

Figure 5.20 ~ Options Properties dialog box.

The next time you initiate a Notify, the new command appears in the **Notify Type** drop-down list on appropriate Notify dialog box.

■   For more information about the **Submit Notify-Notify Opts** dialog box, see *Notifying an Audience* on page 291.

■   For more information about the **Submit Help Desk Notify** dialog box, see *Using Help Desk Notify* on page 295.

Deploying Radia Management Infrastructure Products and Applications

Use the Radia Management Portal to install Radia infrastructure products and applications to remote devices.

Requirements for Remote Installations

In order to install Radia Infrastructure products, you must be aware of the following requirements.

■ For Windows, the remote computer must be running Windows NT 4 SP 6, 2000, XP, or Server 2003.

> **Note**
>
> In some cases, Windows XP may need to be configured to support a remote installation. See the HP OpenView web site for more information.

■ For HP-UX, the remote computer must be running the HP-UX operating system Version 10.20 or above, PA Risc CPU.

■ For Solaris, the remote computer must be running the Solaris operating system Version 2.5.1 or above, SPARC CPU.

■ The installation files for the Radia product must be stored in the Radia Integration Server's **\media** directory. The Radia Management Portal installation program will copy these files automatically. See *Installation Procedures* on page 33 for more information.

If you did not use the installation program to copy the files, you must manually copy these files from the appropriate CD-ROM to the Radia Integration Server's **\media** directory. The directory structure of the media directory should mirror the CD-ROM layout.

Figure 5.21 ~ Directory structure for extended_infrastructure under media.

■ A packing list, which contains a list of the files to be transferred across the network, must exist in the directory with the installation files. The Radia Management Portal creates the packing list when you launch the remote installation.

Specific instructions about how to use the Radia Management Portal to perform each remote install follows.

Installing the Radia Management Agent

You can use the Radia Management Portal to perform operational and administrative tasks on the Radia infrastructure; however, the Radia Management Portal cannot always perform these tasks remotely. Therefore, the Radia Management Agent, which is a thin delegate, is installed on the remote device to perform these tasks on behalf of the Radia Management Portal. It cannot perform any tasks on its own.

When you use the Radia Management Portal to install Radia management services or applications, the Radia Management Agent is automatically installed on the same device. Use the **Install Management Agent** task to install, and optionally re-install, the Radia Management Agent to remote devices. After registering with the Radia Management Portal, the Radia Management Agent performs the task initiated by the Radia Management Portal, such as a remote installation.

The Radia Management Agent is installed as a Windows Service on all supported Windows platforms and is configured to contact the Radia Management Portal at regular intervals in order to make its presence known. The Radia Management Agent will notify the Radia Management Portal when normal operations occur, such as system shut down or restarts.

RMA Registration Throttling

As of RMP 2.0.1, an internal throttling feature is built into the RMP to efficiently manage the processing of large numbers of first-time RMA registrations. This throttling feature avoids a potential RMP-processing deadlock situation that can occur when very large numbers of RMAs are installed at the same time. The registration throttling feature can be fine tuned, if required, in consultation with customer support.

RMA Registration Schedule and Tasks

The Radia Management Agent is configured, by default, to contact the Radia Management Portal every 14 days (this is the keepalive value in rma.cfg), but also report any changes every 24 hours (this is the updatefreq value in rma.cfg). If the Radia Management Agent has no changes to report from the previous day, it does not contact the Radia Management Portal.

The following is a list of some, but not all, of the tasks that the Radia Management Agent can handle on Windows NT, 2000, XP, and Server 2003 systems on behalf of the Radia Management Portal.

- Starting or stopping services.
- Performing remote installations.
- Discovering all Radia services that are currently running on the device, such as the Notify daemon, Radia Client Scheduler, Radia Configuration Service, and the Radia Integration Service and sub-services.
- Discovering the Radia-managed services on the device.

■ Discovering Hardware and Operating system details of the device, including Service Pack levels.

Viewing Device Information Discovered by the Radia Management Agent

For examples of the information collected by the Radia Management Agent, display the Device Properties for the computer hosting your Radia Configuration Server. In addition, take a look at the groups automatically generated and maintained in the Cross-References container of the Zone. These groups are created from the information collected by the Radia Management Agent.

Choosing a Dynamic or Static Port Assignment for the Radia Management Agent

For all tasks that install the Radia Management Agent, you can specify whether the Radia Management Portal should communicate with the Radia Management Agent using a dynamically assigned port or a static port.

■ Using a dynamic port assignment for the Radia Management Agent reduces the risk of security attacks on well-known ports.

■ Using a static port assignment for the Radia Management Agent is available to communicate to an Agent that is behind a firewall.

Modifying the Radia Management Agent Re-Install Option

To facilitate the deployment of newer versions, the **Install Management Agent** task includes an option to force a re-install of the Radia Management Agent. This option is turned on by default. To review or turn off this option, access the **Modify Install Management Agent Options** dialog box.

To set the Install Radia Management Agent task options

1. Go to the Authority of **Directory, Zone, Configuration,** and then **Tasks.**

2. From the Workspace, page forward and then select **Install Management Agent.**

3. Select **Install Management Agent Options**.

4. Click **Modify** in the **Model Administration** task group.

   The **Modify Install Management Agent Options** dialog box opens.

Figure 5.22 ~ Modifying task option to force a re-install of the Radia Management Agent.

5. Click the desired option for the **Force re-install of RMA** property. If set to **on**, you can push out a newer version of the RMA.TKD to a machine with an existing one. If set to **off,** machines with existing RMA.TKDs will not have the Radia Management Agents updated using the **Install Management Agent** task.

Procedure to Install the Radia Management Agent

To install the Radia Management Agent

Caution
Be sure to read *Requirements for Remote Installations* on page 306 before performing this procedure.

Use the **Navigation aid** to select the place in your infrastructure where you want to install the Radia Management Agent.

Notes
A group of devices may be selected as the audience (target) of the Install Management Agent task. If you choose a group of devices, the **Query** dialog box is bypassed.
As of RMP 2.0.1, you can select a location in your Zone, Networks container or a currently connected LDAP directory location that contains computers on which you want to install the Radia Management Agent. If the Radia Management Portal is not currently managing the targeted Network or LDAP devices, the Radia Management Portal will bring them under management as part of the install task.

From the **Operations** task group, click **Install Management Agent**.

The **Query** dialog box opens.

Specify criteria to narrow the scope of the job.

Click **Next**.

The **Select** dialog box opens.

Select the audience from the **Available** list, and then click ⏩ to add them to the **Selected** list.

Click **Next**.

The **Install Management Agent — Install Opts** dialog box opens.

Figure 5.23 ~ Install Radia Management Agent—Install Opts dialog box.

In order to install a Windows service on a remote device, you may need to obtain administrative authority on the target device's domain. Use this dialog box to type the user name and password necessary to obtain access.

> **Note**
>
> If you are installing the Radia Management Agent on the same computer as the Radia Management Portal, delete **Administrator** from the **User** text box.

Use the **Select Client Port** radio buttons to specify whether the Radia Management Portal should communicate with the Radia Management Agent using a dynamically assigned port number or a static port number.

- Using a dynamic port assignment reduces the risk of security attacks on well-known ports.
- Using a static port assignment is available to communicate to an Agent that is behind a firewall.

If you selected a Client Port type of **Static**, type the port number in the **Port Number** text box.

In the **User** text box, type the administrator ID to obtain administrative authority on the target device's domain.

In the **User Password** text box, type the administrator password to obtain administrative authority on the target device's domain.

If you do not enter the password and administrative authority is required, the job may fail. Check the job status for specific information.

Click **Next**.

The **Schedule** dialog box opens.

In the **Schedule** dialog box, specify when you want this job to run.

Click **Next**.

The **Install Management Agent—Summary** dialog box opens.

Figure 5.24 ~ Install Management Agent—Summary dialog box.

Click **Submit**.

The **Job Status** page opens with list of the jobs. This window automatically refreshes every 60 seconds.

- Click to go up one level in the job or directory tree. For example, after viewing job details, click this icon to return to the Job Group Summary.

- Click if you want to refresh the window to display the latest status.

- Click to view detailed properties for the job or job group. This gives you detailed information on the job status.

- Click to add a shortcut for Jobs to your Desktop.

- Click to obtain a printable view of the Jobs Status page.

When you are done viewing the job status, click ![X] to close the **Job Status** page, and return to the Radia Management Portal.

Below is an example of the Radia Management Agent (RMA) service that has been installed on a remote computer. You can also see that the RMA discovers and registers the Radia Integration Server (RIS) sub-services installed on the remote computer.

The Radia Management Portal uses the information discovered by the Radia Management Agent to add the device to the appropriate groups in the Cross-Reference container of the Zone.

Figure 5.25 ~ Radia Management Agent installed.

When the Radia Management Agent is installed to the remote device and the service is started, a log (rma.log) is created in the directory where the RMA is installed. The RMA is installed to *SystemDrive*:\Novadigm\ManagementAgent.

Refreshing the Radia Management Agent

An installed Radia Management Agent discovers and registers the Radia Integration Server (RIS) sub-services installed on the remote computer. If additional RIS sub-services are installed on the remote computer after the Radia Management Agent's last discovery, use the **Refresh Management Agent** task from the **Operations** task group to immediately update the registered sub-services on the Radia Management Portal.

The **Refresh Management Agent** task will also remove the registration of services that have been uninstalled since the previous registration. For example, if a Radia Client has been removed from a computer since the previous registration, running refresh management agent will remove the machine's client-related services, such as the Radia Notify Daemon and the Radia Scheduler Daemon, from the Radia Management Portal's registry.

To refresh a Radia Management Agent's sub-service discovery

In the Navigation area, navigate to the appropriate device object whose Management Agent service discovery needs to be refreshed.

Note
You do not need to navigate to the Management Agent, just to the device object.

From the **Operations** task group, click **Refresh Management Agent**.

Click to refresh the Workspace area of the Radia Management Portal. You'll see the current, newly registered Radia services and sub-services for the object.

Installing the Radia Client

Use the **Install Client** task to install the Radia Clients to remote devices. The Radia Client installation program uses the Microsoft MSI format for Windows Installer. The program consists of one MSI package, with five feature sets, one for each client—Radia Application Manager, Radia Software Manager, Radia Inventory Manager, Radia OS Manager and Radia Patch Manager.

> **Note**
>
> Use the **Manage Proxy Assignment** task prior to the **Install Client** task if you want to deploy a set of Radia Clients from pre-assigned Radia Proxy Servers, instead of directly from the Radia Management Portal. This option allows for existing Radia Proxy Servers in your infrastructure to handle some or all of the client deployment workload, instead of requiring the Radia Management Portal to do all the work. For details, see *Managing Proxy Assignments* on page 324.
>
> The Radia Management Portal supports multiple client profiles. For details, see *Supporting Remote Installs Using Multiple Profiles* on page 320.

To install the Radia 4.x Clients with the Radia Management Portal

> **Cautions**
>
> Be sure to read *Requirements for Remote Installations* on page 306 before performing this procedure.
>
> See the *Radia Application Manager Guide for Windows* or the *Radia Software Manager Guide for Windows* on the HP OpenView web site for detailed information such as system requirements and customization options for the installation.

1. Use the Navigation aid to select the device or group of devices on which you want to install the Radia Clients.

> **Notes**
>
> A group of devices may be selected as the audience (target) of the Install Client task. If you choose a group of devices, the **Query** dialog box is bypassed.
>
> As of RMP 2.0.1, you can select a location in your Zone, Networks container or a currently connected LDAP directory location that contains computers on which you want to install the Radia Clients. If the Radia Management Portal is not currently managing the targeted Network or LDAP devices, the Radia Management Portal will bring them under management as part of the install task.

1. From the **Operations** task group, click **Install Client**.

    The **Query** dialog box opens.
2. Specify criteria to narrow the scope of the job. See *Performing Queries* on page 285 for more information.
3. Click **Next**.

    The **Select** dialog box opens.

4. Select the audience from the **Available** list, and then click to add it to the **Selected** list. See *Selecting an Audience* on page 287 for more information.

5. Click **Next**.

The **Install Client—Client Opts** dialog box opens.

Figure 5.26 ~ Install Client—Opts dialog box.

6. From the **Profile** drop-down list, select a client profile to use for the installation. For details on creating Client Profiles, see *Adding, Modifying, and Deleting Install Profiles* on page 320.

7. In the **Initialization File** area, select the appropriate installation INI file from the drop-down list. This file contains parameters necessary for the Radia Client to run, such as the IP address of the Radia Configuration Server.

   The Radia Management Portal will honor settings placed in a customized *.INI file when it installs the client.

8. In the **Product** area, select the clients that you want to install on the target devices.

Caution
Be sure to install only the clients for which you have licenses. If you install a client for which you do not have a license, the client will not authenticate with the Radia Configuration Server.

9. In the **RCS Host Name** text box, type the IP address or host name that the Radia Client will use to access the Radia Configuration Server.

10. In the **RCS Port number** text box, type the port number that the Radia Client will use to access the Radia Configuration Server.

11. Select the **Perform Silent Install?** check box if you want to install a client without any user interface.

12. Select the **Perform Connect After Install?** check box if you want the client computer to connect to the Radia Configuration Server after the installation. This allows the client computer to register with the Radia Configuration Server. See the *Radia Application Manager Guide* for more information.

    When the client computer connects to the Radia Configuration Server, the Radia Management Portal also captures information about your subscribers and stores it in the Radia Management Portal Directory. See *Discovering Radia Subscriber Information* on page 327 for more information.

13. Using the **Select Client Port** radio buttons, select whether to communicate with the Radia Management Agent on the Client using a Dynamic or Static port number.

    ● Using a dynamic port assignment reduces the risk of security attacks on well-known ports.

    ● Using a static port assignment is available to communicate to an Agent that is behind a firewall.

14. If you selected a Client Port type of **Static**, type the port number in the **Port Number** text box.

15. In the **User** text box, type the administrator ID to obtain administrative authority on the target device's domain.

16. In the **User Password** text box, type the administrator password to obtain administrative authority on the target device's domain.

    If you do not enter the password and administrative authority is required, the job may fail. Check the job status for specific information.

17. Click **Next**.

The **Schedule** dialog box opens.

18. In the **Schedule** dialog box, specify when you want this job to run. For more information, see *Scheduling Jobs* on page 289.

19. Click **Next**.

The **Install Client—Summary** dialog box opens.

Figure 5.27 ~ Install Client—Summary dialog box.

20. Click **Submit**.

The **Job Status** page opens with list of the jobs. This page automatically refreshes every 60 seconds.

Supporting Remote Installs Using Multiple Profiles

This version of the product allows you to remotely install more than one version of the Radia Clients from the Radia Management Portal. For example, you may want to install Radia 4.x Clients on some computers, but Radia 3.x Clients on others. Or, you may want to minimize the size of the client package being installed, and create a client code set that eliminates the required Microsoft .NET code (for those machines you know already have the required .NET installed).

Adding, Modifying, and Deleting Install Profiles

Use the **Add Install Profile** task in the Model Administration task group to add a new profile for a Client Install. The profile points to a code source for the product that is different from the default code source provided by Radia Management Portal.

Topics in this section identify where to place the source code for Client Install Profiles, and procedures for adding, modifying, and deleting them.

Client Install Profiles –Source Code Required Locations

The code source needs to be placed at the following location:

■   `Client Installs: <RIS>¥media¥client¥<profile>¥<OS>`

Where:
<RIS> is the Radia Integration Server location
<profile> is your folder name for the install profile
<OS> is the Operating System folder name. For Windows, <OS> is **Win32.**

The code source for the product needs to be in the <OS> folder. It may contain more than one *.ini file.

To add a Client Install Profile

1. Navigate to the following location in the Radia Management Portal.

Figure 5.28 ~ Location for Adding a Client Install Profile.

2. Click **Add Install Profile** from the **Model Administration** task group.

   The **Add Client Install Profile** window opens.

Add Client Install Profile

Properties

Common Name	
Display Name	
Description	
Product Location	/client/

Add   Cancel

Figure 5.29 ~ Sample Client Install Profile entries.

---

3. Complete the Properties for the Add Client Install Profile, as follows:

   Common Name: A unique name for the Client Install Profile object in the RMP.

   Display Name: The display name for this Client Install Profile in the RMP.

   Description: A full description of the source code installed by this profile.

   Product Location: The directory in the base-RMP **/media/client** directory that contains the code source. Use forward slashes.

          For example: /client/**nodotnet**

          Below the folder specified in the Product Location must be subdirectories for each supported operating system, such as **win32**. The client source code is located in these operating system-level folders.

4. Click **Add**.

   The **Properties** page for the Client Install Profile opens. The Navigation area includes the new entry for this Client Install profile.

5. Radia Management Portal users will now be able to select this profile from the Options page when using the **Install Client** task.

Figure 5.30 ~ Sample Client Install Profile Properties.

6. Radia Management Portal users will now be able to select this profile from the Options page when using the **Install Client** task.

To modify a Client Install Profile

Navigate to the where the profiles for Client Installs are located, shown in the following figure.

Figure 5.31 ~ Location of Client Install Profiles.

Click on the install profile object to be modified. You cannot modify the Default Client Install object.

Click on **Modify** from the Model Administration task group. The **Modify Install Profile** page opens.

Modify any of the fields, and click **Modify.**

Figure 5.32 ~ Modify Install Profile dialog box.

The Properties page opens, showing your modifications.

To delete a Client Install Profile

Deleting an install profile deletes the RMP user's ability to select this profile during the Install Client task. It does not delete the source code from the Product Location.

Navigate to the [Client Installs] container and click on the profile to be deleted.

The Properties page for the Install Profile opens.

Click **Delete** from the Model Administration task group.

A prompt asks you to confirm the delete.

Click the green check mark to confirm the delete.

The profile object is removed from the [Client Installs] container.

Managing Proxy Assignments

Use the **Manage Proxy Assignments** task to designate Radia Proxy Servers in your infrastructure to handle the deployment of client installation scripts for designated devices.

To assign a set of devices to a Radia Proxy Server, first create a group for all devices to be assigned to a given Radia Proxy Server in the Groups container. Create separate groups for devices being managed by different Radia Proxy Servers. See *Adding Devices to a New Group* on page 320 for more information on how to create groups of devices. Then use the **Manage Proxy Assignment** task to assign a Radia Proxy Server to all members of the group. Repeat the **Manage Proxy Assignment** task for each Radia Proxy Server receiving node assignments.

After making all Radia Proxy Server assignments, use the **Install Client** task to schedule the installation of the clients. If a device that is scheduled for a client installation has been assigned to a Radia Proxy Server, the Radia Management Portal will first synchronize with the Radia Proxy Server, and then the Radia Proxy Server will complete the client installation on the device.

To change or remove proxy assignments, first change the group members, and then repeat the same Manage Proxy Assignment steps used to assign nodes to the Radia Proxy Server.

Requirements for Managing Proxy Assignments

■ One or more previously installed Radia Proxy Servers.

■ For each Radia Proxy Server, an installed Radia Management Agent that has also successfully discovered the Radia Proxy Server service.

If these requirements have been met, when you navigate to a device containing the RMA-discovered Radia Proxy Server, the Radia Proxy Server icon will display in the Workspace of the Radia Management Portal.

For example, *Figure 5.33 ~ Radia Proxy Server discovered by the Management Agent on DOCTEST* on page 325 shows the Radia Proxy Server installed and discovered by the Radia Management Agent on the computer DOCTEST. If you had multiple devices in your RMP Zone with a Radia Proxy Server, all would be listed in the **Zone Cross References** container. Go to the **Infrastructure Services** group and click on Radia Proxy Server. All devices that have Radia Management agents and Radia Proxy Servers on them are automatically added to this Cross References group.

Figure 5.33 ~ Radia Proxy Server discovered by the Management Agent on DOCTEST.

To assign devices to a Radia Proxy Server

Create a group of Devices in the Groups container. Move all devices that are to be assigned to a single Radia Proxy Server in the new Group. For details, refer to *Adding Devices to a New Group* on page 320.

Use the **Navigation aid** to select the new Group for making proxy assignments.

From the **Operations** task group, click **Manage Proxy Assignment**.

The **Manage Proxy Assignment - Select proxy** dialog box opens.

Figure 5.34 ~ Select Proxy step of Manage Proxy Assignment dialog box.

Select a Proxy Server from the list to handle the client deployment for the set of devices that are members of the selected Group.

Click **Next**.

The **Manage Proxy Assignment — Summary** dialog box opens.

Figure 5.35 ~ Manage Proxy Assignment – Summary of West Coast Device Group to be assigned to Proxy Server DOCTEST.

Click **Submit** to save the proxy assignment of nodes to the selected server.

After completing all proxy assignments, run the **Install Client** task from the Radia Management Portal **Operations** task group as discussed in *Installing the Radia Client* on page 314. If a proxy-assigned node is selected for the Client Install, the Radia Proxy Server performs the client script deployment, as opposed to the Radia Management Portal.

Discovering Radia Subscriber Information using Managed Services

The Radia Management Portal captures information about your subscribers and stores it in the Radia Management Portal Directory. In the **Cross References** container, there is a group named **Managed Services**. The information about subscribers is used to create automatic groups for each service being managed by Radia for your subscribers.

When the Radia client computers connect to the Radia Configuration Server, the Radia Management Portal captures the information stored in the Radia Database in the following objects—ZCONFIG, ZMASTER, APPEVENT, and ZSTATUS. See the HP OpenView web site for more information about each of these objects.

As of RMP 2.x, the captured information is passed from the RCS to the Radia Messaging Server, which then delivers the information to the Radia Management Portal. See the *Radia Messaging Server Guide* on the HP OpenView web site for more information on how to install and configure the Radia Messaging Service for use with the Radia Management Portal.

To view Radia Managed Services information

1. Navigate to the **Zone Cross References** container.

2. Select **Managed Services**.

The Managed Services container includes groups of devices for which the Radia Configuration Server has reported Radia managed applications.

Figure 5.36 ~ Managed Services container in Zone Cross References container..

3. In the workspace, you will see one or more groups, each representing the name of a service being managed by Radia on devices in this Radia Management Portal Zone.

4. Click on a group in the Managed Services container to see all the devices in the Zone for which Radia is managing that service.

Figure 5.37 ~ A list of devices for which Radia is managing the Drag and View application.

Installing the Radia Proxy Server

Use the **Install Proxy Server** task to install the Radia Proxy Server to remote devices. During the installation, you will receive status information and if the installation fails, it can be rescheduled. The Install Proxy Server Task will prompt you to select a specific CFG file, if multiple ones exist.

See the *Radia Proxy Server Guide* for more information.

See *Preparing and Locating Configuration Files for Proxy Server Installs* on page 334 for details on preparing and locating customized CFG files for this task.

To install the Radia Proxy Server

Caution
Be sure to read *Requirements for Remote Installations* on page 306 before performing this procedure.
You may also want to check the HP OpenView web site for the latest information on this topic.

1. Use the **Navigation aid** to select the place in your infrastructure where you want to install the Radia Proxy Server.

Note

A group of devices may be selected as the audience (target) of the Install Proxy Server task. If you choose a group of devices, the **Query** dialog box is bypassed.

As of RMP 2.0.1, you can begin to install the Radia Proxy Server by selecting one or more devices from a location in your Zone, Networks container or LDAP directory. If the Radia Management Portal is not currently managing the targeted Network or LDAP devices, the Radia Management Portal will bring them under management as part of the install task.

---

2. From the **Operations** task group, click **Install Proxy Server**.

The **Query** dialog box opens.

3. Specify criteria to narrow the scope of the job. See *Performing Queries* on page 285 for more information.

4. Click **Next**.

The **Select** dialog box opens.

5. Select the audience from the **Available** list, and then click ▶▶ to add it to the **Selected** list. See *Selecting an Audience* on page 287 for more information.

6. Click **Next**.

The **Install Proxy Server—RPS Options** dialog box opens.

Figure 5.38 ~ Install Proxy Server—Install Options dialog box.

7. In the **RCS Host Name** text box, type the name or IP address for the Radia Configuration Server.

8. In the **RCS Port number** text box, type the port number for the Radia Configuration Server.

9. In the **RCS User** text box for Install Options, type the user ID to use to connect to the Radia Configuration Server.

10. If available, select which RPS configuration file to use during the installation from the **RPS Config File** drop-down list. This field only appears if customized configuration files have been added to the Radia Management Portal.

> **Note**
>
> To make customized Radia Proxy Server configuration files available for selection during this task, see *Preparing and Locating Configuration Files for Proxy Server Installs* on page 334.

11. In the **User** text box for Remote Client Credentials, type the administrator ID to obtain administrative authority on the target device's domain.

> **Tip**
>
> In order to take advantage of the Install Radia Proxy Server task, consider creating a
> standard administrator ID across the domains in your network.

12. In the **User Password** text box, type the administrator password to obtain administrative
    authority on the target device's domain.

    If you do not enter the password, and administrative authority is required, the job may fail.
    Check the job status for specific information.

13. Click **Next**.

    The **Schedule** dialog box opens.

14. In the **Schedule** dialog box, specify when you want this job to run. For more information, see
    Scheduling Jobs on page 289.

15. Click **Next**.

    The **Install Proxy Server—Summary** dialog box opens.

Figure 5.39 ~ Install Proxy Server—Summary dialog box.

16. Click **Submit**.

The **Job Status** page opens with list of the jobs. This page automatically refreshes every 60 seconds. Press **F5** to manually refresh it.

Figure 5.40 ~ Job Status page.

- Click to go up one level in the job or directory tree. For example, after viewing job details, click this icon to return to the Job Group Summary.

- Click if you want to refresh the status of the installation.

- Click to view detailed properties for the job or job group. This gives you detailed information on the job status.

- Click to add a shortcut for Jobs to your Desktop.

- Click to obtain a printable view of the Jobs Status page.

17. When you are done viewing the job status, click to close the **Job Status** page, and return to the Radia Management Portal.

Preparing and Locating Configuration Files for Proxy Server Installs

Use these procedures to prepare one or more fully configured RPS.CFG files for the **Install Proxy Server** task. The CFG files must be placed in a specific media location for the Radia Management Portal to use them. When you run the Install Proxy Server task from the Radia Management Portal, the task will prompt you to select a specific CFG file, if multiple ones exist. Select your pre-configured CFG file, and the installed Radia Proxy Server will be installed fully configured and ready to go.

To prepare a pre-configured RPS.CFG file for use the Install Proxy Server task

Prepare a fully configured rps.cfg file.

Perform a local installation of the Radia Proxy Server on a test machine that is the same platform as the intended Radia Proxy Server platform. Edit the resulting rps.cfg file using the directions given in the *Radia Proxy Server Guide* in the section *Configuring the Radia Proxy Server*.

Place the configured rps.cfg file in a specific Radia Management Portal media directory.

The appropriate location of a configured rps.cfg file will vary according to the platform on which you are installing the Radia Proxy Server: win32, hpux, or solaris. For example, the location for a Windows Radia Proxy Server installation is similar to this:

C:\Novadigm\IntegrationServer\media\extended_infrastructure\proxy_server\win32\media\etc

a. Go to the directory where the Radia Management Portal is installed.

The default is either
<*SystemDrive*>:\Novadigm\Radia Integration Server

OR

<*SystemDrive*>:\Novadigm\IntegrationServer

depending on when it was installed.

b. Go to the following folder location in the Radia Management Portal directory:
    \media\extended_infrastructure\proxy_server*<platform>*\media
    where *<platform>* is win32, hpux, or solaris, according to which platform you are
    installing the Radia Proxy Server on.

c. Add an **\etc** folder to the **\media** directory.

d. Copy the rps.cfg file to this platform-specific **\media\etc** folder. For example, if the
    Radia Management Portal is installed on **C:\Novadigm\IntegrationServer**, and the
    Radia Proxy Server will be installed on a Windows platform, then place the rps.cfg file in
    the following location:C:\Novadigm\IntegrationServer\media\extended_infrastructure
    \proxy_server\win32\media\etc

Run the **Install Proxy Server** task from the Radia Management Portal, as usual. The
installation task will also transfer the fully configured rps.cfg file.

Synchronizing the Radia Proxy Server

Use the **Synchronize Proxy Server** task to force the Radia Proxy Server to connect to the Radia
Configuration Server to preload the files to the static cache on the Radia Proxy Server. The task is
available for Devices whose properties include a Radia Proxy Server (cn=rps) service.

■ For devices that have a Radia Management Agent installed, the **rps** service is automatically
   discovered.

■ For devices that do not have a Radia Management Agent installed, you can manually add a
   service for the Radia Proxy Server to enable the task. For details, refer to *Adding Services* on
   page 205 and *Figure 4.63 ~ Adding a Service for a Radia Proxy Server* on page 208.

See the *Radia Proxy Server Guide* for more information on the Radia Proxy Server.

To synchronize one or more Radia Proxy Servers

1. Use the **Navigation aid** to select the Radia Proxy Server(s) that you want to synchronize.

    ● To synchronize an individual Radia Proxy Server, navigate to the Device's properties from
       a Group or Device container, and select the service for the Radia Proxy Server.

    ● To synchronize all Radia Proxy Servers identified by the Radia Management Agents in a
       Zone at once, navigate to the **Radia Proxy Server** group in the **Zone, Cross
       References, Infrastructure Services** container.

2. In the **Operations** task group, click **Synchronize Proxy Server**.

    The **Schedule** dialog box opens.

3. In the **Schedule** dialog box, specify when you want this job to run. For more information, see
    Scheduling Jobs on page 289.

4. Click **Next**.

    The **Submit Synchronize—Summary** dialog box opens.

Figure 5.41 ~ Submit Synchronize—Summary dialog box.

5. Click **Submit**.

A list of the jobs appears. Now, you can use the **View Properties** 🔍 toolbar icon to view detailed information, such as the status of the job.

The status of the synchronize proxy job will report the following events:

● Submission of the job request to the Radia Proxy Server.

● Start of session between Radia Proxy Server and Radia Configuration Server (for preloading the files to the static cache on the Radia Proxy Server).

● Job successful.

See *Viewing Properties* on page 274 for more information.

Purging the Dynamic Cache of the Radia Proxy Server

Use the **Purge Dynamic Cache** task to purge the dynamic cache of the Radia Proxy Server. The task is available for Devices whose properties include a Radia Proxy Server (cn=rps) service.

■ For devices that have a Radia Management Agent installed, a Radia Proxy Server service is automatically discovered. These devices are automatically listed in the Zone Cross References Container, within the Infrastructure Services group for Radia Proxy Servers.

■ For devices that do not have a Radia Management Agent installed, you can manually add a service for the Radia Proxy Server to enable the task. For details, refer to *Adding Services* on page 205 and *Figure 4.63 ~ Adding a Service for a Radia Proxy Server* on page 208.

See the *Radia Proxy Server Guide* for more information.

To purge the dynamic cache of the Radia Proxy Server

1. Use the **Navigation aid** to select the Radia Proxy Server service on the Device whose cache you want to purge.

   ● To purge the dynamic cache of an individual Radia Proxy Server, navigate to the Device's properties from a Group or Device container, and select the service for the Radia Proxy Server.

   ● To purge the dynamic cache of all Radia Proxy Servers identified by the Radia Management Agents in a Zone at once, navigate to the **Radia Proxy Server** group in the **Zone, Cross References, Infrastructure Services** container.

Figure 5.42 ~ Location of a device's Radia Proxy Server.

2. In the **Operations** task group, click **Purge Dynamic Cache**.

   The **Schedule** dialog box opens.

3. In the **Schedule** dialog box, specify when you want this job to run. For more information, see *Scheduling Jobs* on page 289.

4. Click **Next**.

   The **Submit Purge—Summary** dialog box opens.

Figure 5.43 ~ Submit Purge—Summary dialog box.

5. Click **Submit**.

A list of the job(s) appears. To view a job's details and the status of the job, click 🔍 on the toolbar or click the **View Properties** task. See *Viewing Properties* on page 274 for more information.

Managing Services

Use the Radia Management Portal to manage services. For example, you can start or stop services on your remote devices.

To manage services

1. In the Navigation area, select the service that you want to manage.

You can access a service from a Device's entry in the Zone Device container, Groups container, or Cross-References Infrastructure Services container. After selecting the Device, select the Service.

2. In the **Operations** task group, click the appropriate action.

- Click **Pause** to temporarily suspend the execution of a service. The service continues to run, but does not perform any action.
- Click **Restart** to stop a service and then start it again.
- Click **Resume** to resume execution of a service that has been paused.
- Click **Start** to run a service.
- Click **Stop** to stop a service.

> **Note**
>
> You cannot stop the Radia Management Agent service.

3. The **Job Status** page opens. This page automatically refreshes every 60 seconds.

   - Click ⟳ to refresh the page to display the latest status.

   - Click 🔍 to view detailed information, such as the status of the installation.

4. When you are done viewing the job status, click ❌ to close the **Job Status** page, and return to the Radia Management Portal.

Managing Task Templates

Use the **Add Task Template** task in the Operations task group to preset options for each type of task needed when scheduling zone operations.

Adding Task Templates

Add task templates for use with the Notify or Install RPS tasks.

To add a task template

Use the Navigation aid to go the **Zone, Configuration, Task Templates** container.

The existing Task Templates (if any are available) are displayed in the Workspace.

Figure 5.44 ~ Task Templates in Zone Configuration Container.

In the **Operations** task group, click **Add Task Template**.

The **Add Task Template** options page opens.

Figure 5.45 ~ Add task template page.

Use the **Task Type** drop-down menu to select the type of task for which you are adding a template.

> **Note**
>
> When you select a Task Type, additional fields for defining that task are displayed on the page.

Type a **Task Name** for the template in the list box.

Enter a Task Name that clearly identifies the job to be run. This allows you to easily select it from other templates in the Task Templates container.

> **Note**
>
> You don't need to repeat the Task Type when entering the Task Name; it is automatically included in the Display Name for the template. For example, a Notify task object is labeled "Notify *<Task Name>*".

Complete the options for the task you selected. For details, refer to the appropriate topics:

● To complete Notify tasks, see *Using the Notify Tasks* on page 291.

● To complete Install Proxy tasks, see *Installing the Radia Proxy Server* on page 329.

Click **Next**.

The **Add Task Template Summary** page opens.

Figure 5.46 ~ Sample Summary for a Notify Task Template.

Review the Selected Options. To change them, click **Back** and revise the options. To save them, click **Submit.**

The Task Template is added to the Task Templates container, and thus can be selected during the **Schedule Zone Operation** task.

Note that the options of a task template exist as children of the task template, itself.

Figure 5.47 ~ Task Templates container shows newly added Notify Tasks.

Removing Task Templates

To remove task templates

Navigate from the Directory to the Zones, Configuration, Task Templates container.

Click on the task template to be deleted.

The Workspace displays the object for the selected Task Template.

In the Model Administration Task group, click **Remove.**

A message asks you to confirm the removal of the template.

Click the green checkmark ✓ to confirm the removal.

Figure 5.48 ~ Confirm removal of Task Template Children (Options).

Since the task's Options are considered a child of the Task Template, another prompt asks you to confirm the removal of the child object.

Click the green check mark to confirm the removal of the Task Template and children.

The Task Template and its Options are removed from the Portal Directory.

Installing Additional RMP Zones (Subordinate Zones)

Once your initial Radia Management Portal zone is installed, you can use the Radia Management Portal to remotely install additional Radia Management Portal zones in your enterprise. These zones are called *subordinate zones*.

Prerequisite for Install RMP task

The media that is needed to run the Install RMP task must be stored in the Radia Integration Server **\media** directory, in a structure that mirrors the original Radia Management Portal installation media.

The Radia Management Portal installation program, **setup.exe**, automatically copies the needed files to the appropriate locations when you select **Yes** to the following prompt:

Figure 5.49 ~ Prompt to copy modules for infrastructure components.

■ To verify that your Radia Management Portal includes the needed install media, you can check that the following directory structure exists:

<<RMP_install_directory>>¥media¥extended_infrastructure¥management_portal¥<platform>¥

■ Below each <platform> directory will be subdirectories for \media\modules. A copy of your **license.nvd** file must exist in the <platform>\media\modules directory.

If the needed directory structure and files are missing, just rerun the **setup.exe** program and elect to update the installable components. When prompted to copy the Remotely Installable **Infrastructure** Components, choose **Yes**. See *Installation Procedures* on page 33 for more information.

To install an RMP Zone from the Master Zone

Login to the Master Zone Radia Management Portal as **Admin**.

The device on which you are installing the RMP zone needs to have a device entry in the Master Portal zone.

- If the device currently exists, browse to and display the Device Properties from a Zone Groups container or Zone Devices container entry.

- If the device entry does not currently exist, add an entry for the device. (For details, see *Adding a Single Device* on page 182.) After adding the device, navigate to and display the Device Properties.

Figure 5.50 ~ To install another RMP zone, display Device Properties for the Remote Computer and select Install RMP.

Click **Install RMP** from the Operations task group to install a subordinate zone onto the selected device.

The **Rmp opts** panel of the Install RMP page opens (Step 3 of 5). Complete the Zone Options and Remote Client Credentials using the following information.

Table 5.2 ~ Zone Options for Install RMP		
Field	**Example**	**Description**
Zone Name	Chicago	Zone name becomes the high-level qualifier for all nodes in this RMP directory. All zone names in an enterprise must be unique.

Table 5.2 ~ Zone Options for Install RMP

Field	Example	Description
Zone Display Name	Chicago_RMP	Zone display name is the label for the Zone in RMP.
RIS Port	3466	The port number of the Radia Management Portal RIS service. Default is 3466.
RIS Install Directory	C:/Novadigm/IntegrationServer	The base directory for the Radia Management Portal on the remote device. **Important:** Use *forward* slashes for both Windows and UNIX path syntax.
RIS Service Name Suffix	ChicagoRMP	Optional entry. If used, this suffix is appended to the Radia Integration Service name, httpd, to allow for a distinct entry from other RIS entries that may be running on the same server. If a suffix is entered, the RMP install checks to see if there is either an existing service with this suffix to allow for a refresh of an RMP service. Otherwise, the RMP install only continues if the above RIS directory is empty. **Note:** If you enter a suffix, then append this suffix to the <httpd> entry when you start the Portal from a command line. For example: nvdkit start httpdChicagoRMP.tkd

Table 5.3 ~ Remote Client Credentials for Install RMP

Field	Example	Description
Select Client Port	Select Dynamic Or Select Static	Dynamic is the default. To use a static port number (normally needed with a firewall), select Static. Also enter a Static Port number.
Port Number		If Client Port is set to Static, a Port Number field allows you to specify the Client Port number to use.
User	Administrator	An RMP Install requires Administrator access to the remote computer. Enter a User ID that has Administrator privileges on the remote computer.
User Password	••••••••••••••	Enter the password associated with the User login to gain access to the remote computer. Entries are encrypted.
Confirm Password	••••••••••••••	Repeat the User Password entry. If the Confirm Password and User Password entries do not match, you will be prompted to correct them.

After completing all entries, click **Next**.

Figure 5.51 ~ Sample Entries to Install an RMP.

The Schedule panel (Step 4 of 5) of the Install RMP page opens. The default schedule is to run the Install RMP task immediately.

To schedule the install immediately, click **Next**. To schedule it at a later time (for example, during a period of lower activity), change the time or date and click **Next**.

The Summary panel of the Install RMP page opens, as shown in the following figure.

Review all entries are as desired, and then click **Submit**.

Figure 5.52 ~ Install RMP Summary.

Review all entries are as desired, and then click **Submit**.

A job summary window opens for the Install RMP job.

To view the Job Properties, click the Display Name entry.

To return to the job summary page, click [icon].

To refresh the status, click [icon].

When the install job finishes, the Radia Management Portal Zone will be installed on the remote device, with the following new entries also made to the Master Zone. These entries permit access to the new zone:

● The Zone, Configuration, Directory Services container will include a ds-dsml definition. When the startup mode is set to auto, the new zone will automatically be connected to the

master zone upon startup. If the startup mode is manual, use the **Connect to Directory Service** task to manually make a connection during the session.

● The Zone Access Points container will show an entry for the new Zone.

Updating Subordinate RMP Zones

After you install an update to the Master Portal for a service pack or release, use the **Update RMP** task in the Operations task group to propogate the code updates to the Subordinate RMP Zones in your enterprise. This task allows you to synchronize the RMP module build numbers throughout the Zones in your enterprise.

Important Note

When applying a service pack update to the Master Zone, respond **Yes** when prompted to install the **Remotely Installable Infrastructure Components**. This will place the code in the necessary media location.

To apply code updates to Subordinate RMP Zones from the Master Zone

1. From the Master Portal, navigate to the **Zone Access Points** container.

2. To update all RMP Zones at once, click **Update RMP** from the **Operations** task group.

   Or

   To update a single RMP Zone, select the individual Zone object and click **Update RMP** from the **Operations** task group.

   The code updates are immediately applied to the subordinate zones.

3. Task changes are often delivered with a service pack or new release. To also update the tasks available to a subordinate zone, use the **Open Subordinate Zone** task to access a Zone remotely, and run **Update Tasks** from the Zone Configuration Tasks container. Repeat this step for each subordinate Zone in your enterprise.

4. If the Radia Management Agent was updated by the service pack or new release, it must be re-installed on the subordinate zone host machines as well as all managed devices in the subordinate zones. See *Installing the Radia Management Agent* on page 307 for more information.

Scheduling Zone Operations

Scheduling Zone Operations requires you to have the following objects in your Zone directory:

■ **Zones** in the Zones Access Points container. When you use Install RMP to install additional Zones in your enterprise, access points to these Zones are automatically created in the Zone Access Points container. For details, see *About the Zone Containers* on page 97.

■ **Task Templates** for the job being scheduled. For details, see *Managing Task Templates* on page 340.

■ **Groups** with member devices in each Zone that represent the devices to be operated upon by the schedule zone operation. For details on creating and adding devices to groups, see the topics in *Chapter 4: Administrative Functions* starting on page 135.

Groups can be selected from the **Groups** container, or the **Cross References** container. If you are using Groups of devices from the Groups container, give the Groups in each Zone the same name. To use the automatically generated groups in the **Cross References** container, make sure the devices in your Zones have the Radia Management Agent installed on them.

To schedule zone operations

1. Navigate to the **Directory, Zone, Zone Access Points** container to schedule zone operations for one or more zones.

Figure 5.53 ~ Navigation path to Zone Access Points.

> **Tip**
>
> You may want to add the Zone Access Points container to your desktop. To do this, navigate to the Zone Access Points container and click the **Add Shortcut to Desktop** icon on the toolbar above the Workspace.

2. From the Operations task group, select the **Schedule Zone Operation** task.

The **Schedule Zone Operations- Query** window opens for you to Query and Select the zones to be included in this schedule.

Figure 5.54 ~ Query window for limiting/selecting zones for scheduling operations.

3. If you have a large number of zones, use the fields on this Query window to limit the list of zones from which to select zones for operations. For example, you can enter a Common Name of B* to limit the list of zones to those starting with B. After entering any filter or Query Constraints, click **Next**.

   or

   To view and then select from all available zones, click **Next**.

   If there is more than one zone meeting your Query constraints, the **Submit Schedule Zone Operation** – **Select** window opens. The Zones meeting your query constraints are listed in the **Available** column.

   If there is only one Zone meeting your Query constraints, skip to Step 6.

4. Move the zones for the job to be scheduled to the **Selected** column using the **Arrow** icons, or, by double-clicking on an entry.

Figure 5.55 ~ Selecting Zones for Scheduling a Zone Operation.

5. Click Next to schedule the job against the zones listed in the **Selected** column.

The **Submit Schedule Zone Operation – ZoneJob opts** window opens.

Figure 5.56 ~ Submit Schedule Zone Operations (ZoneJob options)

6. Use the **Zone Job Name** group fields to select the task template and the Group of Devices for the scheduled zone jobs. The task template defines the job type and options to be scheduled (the WHAT). The Group represents the group of devices to which the job is to apply (WHICH objects in the selected zones).

● Select a **Task Template** from the drop-down list. The list represents the task templates that have been entered in the Task Template container at the Directory level of the Radia Management Portal.

● Click the **Group** drop-down list to select one of the groups of devices. The list represents the self-managed groups in the **Cross-Reference** container as well as the Groups created in the Zone Groups container.

The Cross References groups are automatically created from the hardware, software, managed services, and known Infrastructure services that are installed on the devices within any zone.

The Groups of devices in the Groups container should exist in each of the Zones you want to target for the Operation.

The following selections in Figure 5.57 on page 354 show the **Notify Dell Latitudes** task template has been selected for the **Latitude** group. The Latitude group is automatically generated in the Cross References groups.

Figure 5.57 ~ Task Template and Query for the Scheduled Zone Operation (Zone Job Options).

7. Click **Next** to add a schedule to the zone operation.

    The **Submit Schedule Zone Operations – Schedule** window opens.

Figure 5.58 ~ Submit Schedule Zone Operation Summary window.

8. In the **Scheduler Information** area, enter a **Job Name**, such as Notify Latitudes of Upgrades. If desired, modify the **Description** and **Priority**.

9. In the **Time Window area**, use the **Run** drop-down box to select a frequency for the zone operation job. Complete the schedule options the same as for any other job.

> **Note**
>
> You can select **Do Not Schedule** to save the Job and select the Job for use in the **Sequence Tasks** operation.

10. In the **Job Throttling** area, enter the maximum jobs to run at any time, and how many can run per minute. The throttling options apply to each zone from which the jobs will run.

11. Click **Next** to review the summary and submit the job.

The **Submit Schedule Zone Operation – Summary** window opens.

12. Click **Submit** to submit the job for the selected zones.

The Job window opens, and lists a group job for each zone. Note the **Description** in the banner area lists the Zone Operation Job Description.

Figure 5.59 ~ Zone Jobs created by Schedule Zone Operation.

13. To View Job Properties for any of these zone jobs, click on the job listing, then click on the View Properties toolbar icon: .

What happens with jobs scheduled from Remote Zone Operations?

A job scheduled using zone operations launches remote zone job groups and jobs at the scheduled time. These jobs can be seen at the remote zone's job directory.

Opening a Subordinate Zone

Use **Open Subordinate Zone** in the Operations task group to open any Zone from another one. This task is available when a Zone is selected from the **Zone Access Points** container. You can use it to view jobs launched from another Zone using the Schedule Zone Operation task.

To view the job groups and jobs started at each zone, navigate to the managed zone object in the Zone Access Points container, and then click **Open Subordinate Zone** in the Operations task group.

Figure 5.60 ~ Opening Subordinate Zone: Chicago.

The **Open Subordinate Zone** task opens a new Browser window, accesses the remote Portal Zone, and logs you on using the same credentials as your current login.

Navigate to the **Zone, Jobs** container to see jobs launched from another Portal.

In the following sample figures, the Job Name Scheduled for Zone Operations was: **Notify Dell Latitudes**. The zone audience included the zone: **Chicago**.

Figure 5.61 ~ Viewing Job Launched on Chicago Zone: Notify Dell Latitudes Job Group.

Select the Notify Dell Latitudes Job Group to see the Job details.

Figure 5.62 ~ Viewing individual jobs on the Remote Zone Portal.

To exit a Zone, click Logout in the banner area above the Navigation aid, and close the Browser window.

Sequencing Jobs (In Progress)

Use **Add Job Sequence** in the Operations task group to schedule a set of tasks to run at one or multiple portal sites. To begin the task, go to the **Jobs** container, and click **Add Job Sequence** in the **Operations** task group.

Figure 5.63 ~ Add Job Sequence for a set of Tasks.

This feature is currently under development. Sequence Tasks will support selecting task templates and then conditions. For example, you will be able to establish and then run the following set of tasks and conditions from a series of selection menus:

Run: DMA *{if not fail}* Proxy Preload *{if not fail}* Client Notifies

The benefit is that you only need to create and run this job sequence once from the Master Portal, and it will launch a series of jobs at each individual site (named in your Group of Sites), honoring your conditions.

Remote Control (*Windows Clients Only*)

Use Radia's Remote Control to manage Radia Clients running on a supported Windows platform with TightVNC: Enhanced TightVNC Distribution through the Radia Management Portal. TightVNC: Enhanced TightVNC Distribution is a freely re-distributable solution that allows you to control Radia Clients from a remote location. The source code for TightVNC is available for download from http://www.tightvnc.org.

Note
HP does not provide technical support for the TightVNC product.

System Requirements

■ The remote device must be running Windows NT, 2000, or XP.

■ The Radia Management Agent must be installed on the remote device.

■ A Web browser that supports Java applets.

Prerequisites

■ Ability to use the Radia System Explorer.

■ Ability to distribute applications (with the Radia Client or using a Notify operation).

■ In the ZSERVICE class of the Radia Database, the service installation methods (such as ZCREATE and ZDELETE) must be set to a length of at least 57 characters to prevent values from being truncated during the import.

■ Ability to connect the Remote Control Service to the appropriate users. See *Connecting the Remote Control Service to Users* below for more information.

■ Distribute the Remote Control service to the devices to be managed by Radia. Some examples of ways to do this are to use the Radia Client or the Notify task in the Radia Management Portal.

Connecting the Remote Control Service to Users

Use the Radia System Explorer on the Radia Administrator's Workstation to connect the Remote Control Service to the appropriate users, servers, or groups, representing the devices to be managed by Radia. Make a service connection between the Application (ZSERVICE).Remote Control service and the appropriate class instance in the PRIMARY.POLICY domain, such as a USER, DEPT, or WORKGRP class instance.

To connect the remote control service to users

1. Use the **Radia System Explorer** and go to the **PRIMARY.POLICY** domain.

2. Navigate to the appropriate **DEPT**, **USER**, or **WORKGRP** class instance you want connected to the Remote Control Service. *Figure 5.64 ~ POLICY.DEPT.Sales Instance and Show Connections dialog box for SOFTWARE domain* on page 361 uses the Sales Department instance as an example.

3. Right-click the selected instance (in the tree view) and select **Show Connections**. The **POLICY.DEPT Connections** dialog box opens. This dialog box displays a list of classes you can connect the selected instance to.

Figure 5.64 ~ POLICY.DEPT.Sales Instance and Show Connections dialog box for SOFTWARE domain.

4. From the **Show connectable classes for domain** drop-down list, select **SOFTWARE,** then select **Application (ZSERVICE)**, and then select **Remote Control.**

5. Drag the **Remote Control** instance to the appropriate POLICY instance (in this example, **DEPT.Sales**). When your cursor turns to a paper clip, release the mouse button.

Figure 5.65 ~ Connect (Drag) Remote Control Service to Sales instance.

6. Click **COPY** to create the connection from Department Sales to Application.Remote Control.

7. Click **Yes** to confirm the connection.

8. Click **OK** when you receive the confirmation message that "Sales has been connected to Remote Control."

9. Notice that Remote Control is listed under the Sales department instance, which indicates that the entire department is now authorized to receive the Remote Control application.

Figure 5.66 ~ Remote Control Service authorized for Sales Department.

Now you can distribute the Remote Control service to the devices to be managed using the Radia Client or the Notify task.

Using Remote Control (*Windows Clients Only*)

After using the Radia client or the Notify task to distribute the Remote Control service to the remote device, you can use Remote Control to manage the Radia Clients using TightVNC.

To use the remote administration capabilities

1. In the Navigation area, select a device that has the VNC server installed.
2. Click the **VNC Server**.

   The **Server Properties** page opens for the VNC Server.

Figure 5.67 ~ VNC Server properties.

3. If this is your first time using the VNC Server, go to the **Operations** task list and click **Set Password**. (If this is not your first time, go to step 8.)

The **Set Password** dialog box opens.

Figure 5.68 ~ Set Password dialog box.

4. In the **User Password** text box, type the password for the VNC session.

5. Click **Submit**.

The **View Properties Service** dialog box opens.

Figure 5.69 ~ VNC Server properties.

6. In the **Operations** task list, click **Start** to start the VNC server.

The **Job Status** page opens with list of the jobs. This page automatically refreshes every 60 seconds.

- Click [icon] if you want to refresh the page to display the latest status.

- Click [icon] to view detailed information, such as the status of the installation.

When you are done viewing the job status, click [icon] to close the **Job Status** page, and return to the Radia Management Portal.

7. In the workspace, click [icon] to refresh the view and see that the service started.

Figure 5.70 ~ VNC Server has started.

8. In the **Operations** task list, click **Start Viewer** to start the VNC session.

A prompt for VNC authentication opens.

Note
If your Web browser does not support Java applets, you may see this message "Refresh this page for remote authentication" prompt. Be sure to install the Java component.

Figure 5.71 ~ VNC Authentication page.

9. In the **Password** text box, type the password for the VNC session.

10. Click **OK**.

Now, you can control the Radia client from the remote location.

Note
You can customize the **Start Viewer** task to have the VNC session open a new window, or display the VNC session in the Workspace area of the Radia Management Portal. For details, see the topic *Customizing the Start Viewer Task Properties* on page 368.

Figure 5.72 ~ Controlling a remote client.

> **Note**
>
> The initial request temporarily uses Port 5800. The connection uses Port 5900.

To disconnect the VNC session

At the top of the workspace, click **Disconnect** to disconnect the session. If you browse to another page in the RMP, the session will automatically be disconnected.

Click **Stop** in the **Operations** task group to stop the VNC server. You may need to click 🔄 to refresh the view and see that the service started.

Customizing the Start Viewer Task Properties

You can customize the Start Viewer task of the Radia Management Portal to display the remote session in a new window, as opposed to displaying the remote session within the Radia

Management Portal workspace area (the default). To do this you will modify the Start Viewer task from the Radia Management Portal before you begin the VNC session.

To customize the Start Viewer Task from the Radia Management Portal

Navigation to the **Zone Configuration** container.

In the workspace, click **Tasks**.

Browse to and select the **Start Viewer** task.

Select **Custom Viewer**.

The **Options Properties** dialog box opens.

Figure 5.73 ~ Custom Viewer Options Properties dialog box and settings.

The **Open new window** property can be set to **No** (the default) or **Yes**. **No** means the VNC Remote Control session is displayed within the Workspace of the Radia Management Portal. **Yes** means the remote session is displayed in a new, separate window.

To modify the **Open new window** property, click **Modify** in the **Model Administration** task group.

The **Modify Options** dialog box opens. Use this dialog box to change the value for the **Open new window** property.

Figure 5.74 ~ Modify Options dialog box used to set the Open new window property.

Select **Yes** or **No** from the **Open new window** drop-down selection list. **No** means the VNC Remote Control session is displayed within the Workspace of the Radia Management Portal. **Yes** means the remote session is displayed in a new, separate window.

Click **Modify** to save your selection.

Configuring Remote Control

You can configure several parameters in the Remote Control Service to control the server's behavior. To do this you will use the Registry Editor in the Radia System Explorer.

To configure remote control parameters

Go to **Start**, **Programs**, **Radia Administrator**, **Radia System Explorer**.

In the Radia System Explorer **Security Information** dialog box, type your **User ID** and **Password**, and then click **OK**.

Go to **PRIMARY**, **SOFTWARE**, **Application (ZSERVICE)**, **Remote Control**.

Double-click **TightVNC** and then double-click the registry resource for TightVNC (the last one).

Figure 5.75 ~ Registry Resources for Remote Control.

Right-click **TightVNC:TVNCLM.EDR** and select **Edit Registry Resource**.

Navigate to **WinVNC3** to view the local machine-specific settings.

Figure 5.76 ~ Registry File Editor.

Table 5.4 ~ Local Machine-Specific Settings for TightVNC Service

Property	Description
AuthRequired	Set AuthRequired = 1 (default) to ensure that a password is set when you start the service. Set AuthRequired = 0 to disable null password checking by WinVNC. Use DWORD format.
AllowLoopback	Set AllowLoopback = 0 to disable the ability to remote control the local machine. Set AllowLoopback = 1 to allow the ability to remote control the local machine. Use DWORD format.
AuthHosts	Specifies a set of IP address templates that incoming connections must match in order to be accepted. By default, the template is empty and connections from all hosts are accepted. Three settings are available: - IP address – Specifies a range of IP addresses that are not authorized to connect ? IP address – Specifies a range of IP addresses that you want to be prompted for + IP address – Specifies a range of IP addresses that are not authorized to connect **Example**: +192.10,-192.10.12 This parameter is used in conjunction with the QuerySettings parameter. Use STRING format.
ConnectPriority	By default, the TightVNC server disconnects existing connections when a non-shared connection authenticates. You can change this behavior by setting this value to: 0 - to disconnect all existing connections 1 - to continue all existing connections. 2 - to refuse any new connections. Use DWORD format.

Click **Default** to see the local default user properties that you can set.

Figure 5.77 ~ Registry File Editor.

Table 5.5 ~ Local Default User Properties for TightVNC Service

Property	Description
AllowProperties	Set AllowProperties = 0 to prevent your users from accessing the Properties dialog box to modify settings.
	Set AllowProperties = 1 to allow your users to access the Properties dialog box and modify settings.
	Use DWORD format.
AllowShutdown	Set AllowShutdown = 0 to prevent your users from shutting down the TightVNC server.
	Set AllowShutdown = 1 to allow your users to shut down the TightVNC server.
	Use DWORD format.
QuerySetting	Sets whether you want to prompt the user about an incoming connection. This setting must be used in conjunction with AuthHosts.
	Set this value to:
	0 or 1 – Does not prompt on incoming connection. 2 – Prompts on incoming connection (default).
	Use DWORD format.
QueryTimeout	Specifies how long (in seconds) the prompt panel appears to the user when you begin a remote control session. This panel prompts the user to accept the session.
	Use DWORD format.
IdleTimeout	Indicates how long (in seconds) a VNC client can remain idle for before being disconnected. If this is blank or set to 0, a timeout is not enforced.
	Use DWORD format.
InputsEnabled	Allows incoming connections to send input.
	If InputsEnabled = 1 you can interact with the remote computer.
	If InputsEnabled = 0 you can view the remote computer, but cannot interact with it.
	Use DWORD format.

Summary

■ Bring computers in your network under control of the Radia Management Portal using the Manage Computer task. This is required before performing any other operation from the Portal.

■ Each task in the Radia Management Portal follows a similar lifecycle.

■ The starting location of a task determines the audience for the task. Typical starting locations are groups in the Groups container and Cross Reference Containers.

■ You will encounter a series of dialog boxes that you must complete in order to create the job. These dialog boxes are used to narrow the scope of the job, select from available objects, specify job options, specify scheduling information, and review a summary of the job.

■ Use the Notify tasks to perform an action on a set of target devices.

■ Add Task Templates to streamline tasks for Notifies, Proxy Server installations, and Scheduling Jobs to run in multiple Zones.

■ Before performing remote installations, you must copy the appropriate files to the Radia Management Portal's media directory.

■ Use the **Install Management Agent** task to deploy the Radia Management Agent on remote devices.

■ Use the **Install Client** task to deploy the Radia Clients to remote devices.

■ Use the **Install Proxy Server** task to deploy the Radia Proxy Server to remote devices.

■ Use the **Synchronize Proxy Server** task to preload files from the Radia Configuration Server to the static cache on the Radia Proxy Server.

■ Use the **Purge Dynamic Cache** task to purge the dynamic cache of the Radia Proxy Server.

■ You can use the **Start**, **Stop**, **Pause**, **Restart,** and **Resume** tasks to manage remote infrastructure products.

■ Use the **Install RMP** task to create additional Zones in your enterprise. You can access remotely installed Zones using Open Subordinate Zones from the **Zone Access Points** container.

■ Use the **Update RMP** task to apply the code delivered in an RMP service pack to the remote RMP Zones in your enterprise.

■ Use like-named Groups or Cross Reference Groups to schedule jobs to run on multiple zones in your enterprise.

■ You can use **Remote Control** to manage Radia Clients with TightVNC from a remote location.

6

Troubleshooting

At the end of this chapter, you will:

■ Be familiar with the Radia Management Portal log files.

■ Be familiar with the common message types.

■ Be familiar with the information that you need to collect for HP Technical Support.

■ Be familiar with the Portal Zone Directory (ZONE.MK) file compression and backup utilities.

About the Log Files

The Radia Management Portal writes several logs, which can be used to track progress and diagnose problems. The log files are stored by default in ***SystemDrive*:\Novadigm\ IntegrationServer\logs** for the Radia Management Portal for Windows.

The log files are:

- **httpd-*port*.log**
  This is the main log for the Radia Management Portal. It contains information about the actions that you perform in the Radia Management Portal, operational statistics, as well as the version and build number of the Radia Management Portal.

  Replace *port* with your port number, for example, httpd-3466.log.

  Each time you start the Web server a new log is written. The old log is saved as httpd-*port.nn*.log.

- **httpd-*port.YY.MM.DD*.log**
  This log contains the Web server activity for each day. If the log is empty, it means that there was no activity that day.

- **httpd-3466.error.txt**
  This log contains messages written to any logs that contain the prefix ERROR. This allows you to view all errors in a single location.

Setting Trace Levels

By default the trace level is set to 3, which is the informational tracing level. This displays INFO, WARNING, and ERROR messages. See *Common Message Types* on page 381 for more information.

To change the trace level for the logs

Open the file ***SystemDrive*:\Novadigm\IntegrationServer\etc\httpd.rc** for Windows, which is located on the computer that is running the Radia Management Portal. The following is an excerpt from this file.

```
# Config Array
# Element        Default
# =======        =======
# HOST           [info hostname]
# PORT           3466
# HTTPS_HOST     [info hostname]
# HTTPS_PORT     443
# DEBUG          0
# DOCROOT        [file join $home htdocs]
# IPADDR {}
# HTTPS_IPADDR    {}
# WEBMASTER      support@novadigm.com
# UID            50
# GID            100
# NAME           $tcl_service
# LOG_LEVEL      3
# LOG_LIMIT      7
#
Overrides Config {
    PORT 3466
    HTTPS_PORT      443
    LOG_LEVEL       4
}
#
# (Re)Initialize Logging
#
Log_Init
```

Figure 6.1 ~ Excerpt of httpd.rc showing LOG_LIMIT increased to level 4.

Type LOG_LEVEL and the appropriate trace level, space delimited, within the **Overrides Config** starting and ending brackets { }. Select the appropriate trace level, as follows.

Table 6.1 ~ Trace Levels	
Trace Level	**Description**
0	No logging.
1	Logs errors only.
2	Logs warnings and errors.
3	Logs informational messages, warnings, and errors. *Recommended trace level setting for customers.*
4	Logs all debug information. *Recommended for experienced customers only.*
5 - 9	Full trace *Not recommended for customer use.*

Save the file changes and restart the **Radia Integration Server** service.

Common Message Types

The following message types are used in the main Radia Management Portal log (httpd-*port*.log).

Table 6.2 ~ Common Message Types	
Message Type	**Description/Example**
Info	Provides general information. For example: · `20010913 12:37:55 Info: LdifImport/4: BEGIN` Indicates that a job to import an LDIF has begun. · `20010913 12:37:55 Info: RMP: Starting Scheduler...` Indicates that the RMP Scheduler service is started. · `20010913 12:37:55 Info: RMP: Radia Management Portal ready` Indicates that the Radia Management Portal is up and running.
Audit/success	Indicates a successful change to an object in your Radia Management Portal Directory. For example: · `20010913 12:46:43 Audit/success: RMP: (who/admin) add:` `uid=jbanks, cn=opsys, ou=who` Indicates that a new user was added.
Audit/failure	Indicates an unsuccessful change to an object in your Radia Management Portal Directory. For example: · `20010913 16:26:31 Audit/failure: RMP: (who/admin) add:` `uid=Guest, ou=who, object "uid=guest, ou=who" already exists` Indicates that you were not able to add a user with the ID Guest to the organizational unit "who" because it already exists.
Error	Indicates a critical problem.
Warning	Indicates a non-critical problem. · `20010913 16:20:42 Warning: to: output to 1 job-create-reply 2` `resume: no gate`

Collecting Information for HP Technical Support

If you need to contact HP Technical Support for assistance, be sure to collect the following information:

The log directory, stored by default in the following locations:

For Windows, *SystemDrive*:¥Novadigm¥IntegrationServer¥logs

Version information for nvdkit.exe. See *Viewing the Version Information Window*, below.

The zone.mk file and zone.ldif file, stored by default in the following location:

For Windows, *SystemDrive*:¥Novadigm¥IntegrationServer¥etc

See *Creating a Backup of the Portal Zone Directory* on page 245 for information about these files.

The **etc** directory files and complete **etc/zone** subdirectory contents), stored by default in the following location:

/opt/Novadigm/IntegrationServer/etc

The etc/zone subdirectory holds the *.mk, *.ldif, and *.chkp files for loading all objects in a Radia Management Portal zone.

- device
- group (of devices)
- jobs
- user
- xref
- In the **config** folder are entitlement, msg, and task files.
- In the **jobs** folder are the history files.
- In the **network** folder are the dns and lanmanredirector files.

Viewing the Version Information Window

After logging into the Radia Management Portal, click the Information button ⑦ on the banner area to open the Version Information Window, shown in the following figure.

Figure 6.2 ~ Radia Management Portal Version Information Window.

This window displays the installed Module, Version, and Build levels for the Radia Management Portal, including NVDKIT.EXE, HTTPD.EXE, and RMP.TKD.

Gathering Version Information for NVDKIT.EXE

Use this command-line method of obtaining version information for NVDKIT.EXE as an alternative to viewing it from the Version Information window of an active Radia Management Portal session.

To gather the version information for NVDKIT.EXE

1. Open a command prompt.

2. Navigate to the location of nvdkit.exe (by default, *SystemDrive*:\Novadigm \IntegrationServer)

3. Type **nvdkit version**, and press ENTER.

   Below is an example of the version information.

Figure 6.3 ~ Example of version information for nvdkit.exe.

Note
The httpd-*port*.log also contains version and build information.

Gathering Version Information for RADISH.EXE

Radish.exe runs on the Radia Configuration Server. Its build (version) information can be found using this procedure.

To gather the version information for RADISH.EXE

1. Locate the directory of your radish.exe on the machine running the Radia Configuration Server. The default is *SystemDrive*:\Novadigm\ConfigurationServer\bin for Windows.

2. Open a command prompt and change to the directory for radish.

3. Type **radish version**, and press ENTER.

   Below is an example of the version information.

Figure 6.4 ~ Example of version information for radish.exe, (which is given by the build number of module nvdmtcl).

4. The build number for **radish.exe** is actually given in the build number for module **nvdmtcl** (its predecessor's name) in the line:

   ```
   module nvdmtcl, build xx <date> <time>
   ```

   For example, *Figure 6.4 ~ Example of version information for radish.exe* illustrates a Configuration Server running Build 44 of radish (which is shown as module **nvdmtcl, build 44** in the output).

Note
Radish.exe replaced an earlier program named nvdmtcl.

Managing the Portal Zone Directory (ZONE.MK) File

The **Portal Directory**, zone.mk (in the Radia Integration Server's **\etc** directory), loads all configuration and entitlement information for the Radia Management Portal as well as devices, groups, managed infrastructure, job status, network and mounted services information. A single zone has an absolute upper limit of 10,000 devices.

We recommend limiting the number of devices managed by a single zone to the following:

■ Recommended: 1,000 to 2,000 devices

■ Maximum: 5000 devices

To create additional zones in your enterprise, see *Installing Additional RMP Zones (Subordinate Zones)* on page 344.

Summary

■   The httpd-*port*.log is the main log for the Radia Management Portal.

■   The default trace level is set to 3, which tracks informational messages, warnings, and errors.

■   Collect your logs and version information if requesting support from HP Technical Support.

■   Version and build information can be found by clicking on the Radia Management Portal's banner area after logging on. Alternatively, from a command prompt you can run "nvdkit version" on the client side, and "radish version" on the Manager (Configuration Server) side.

Figures

Tables

Procedures

Index

D

Q

R

S