

HP OpenView Management Portal Using Radia

for the Windows operating system

Radia Release Version: 4.2i

Software Version: 2.2

Installation and Configuration Guide

Document Release Date: September 2006



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

© Copyright 1998-2006 Hewlett-Packard Development Company, L.P.

No part of this document may be copied, reproduced, or translated into another language without the prior written consent of Hewlett-Packard Company. The information contained in this material is subject to change without notice.

Trademark Notices

Linux is a registered trademark of Linus Torvalds.

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

OpenLDAP is a registered trademark of the OpenLDAP Foundation.

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

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

OpenLDAP

Copyright 1999-2001 The OpenLDAP Foundation, Redwood City, California, USA.

Portions Copyright © 1992-1996 Regents of the University of Michigan.

OpenSSL License

Copyright © 1998-2001 The OpenSSLProject.

Original SSLeay License

Copyright © 1995-1998 Eric Young (eay@cryptsoft.com)

DHTML Calendar

Copyright Mihai Bazon, 2002, 2003

Documentation Updates

This manual's title page contains the following identifying information:

- Version number, which indicates the software version.
- Print date, which changes each time the document is updated.

To check for recent updates or to verify that you are using the most recent edition, visit the following URL:

http://ovweb.external.hp.com/lpe/doc_serv/

You will also receive updated or new editions if you subscribe to the appropriate product support service. Contact your HP sales representative for details.

Table 1 indicates changes made to this document since the last released edition.

Table 1 Document Changes

Chapter	Version	Change
All	2.1.1 & 2.2	Updated text and images throughout the guide to reflect the task name changes listed in Table 2 on page 5.
Chapter 1	2.1	Page 17, Introduction: added best practice information. Creating and using device groups greatly improves Management Portal performance. The Management Portal performs best when operations are run against groups of devices, as opposed to running the same operations against against one device at a time.
Chapter 1	2.1	Page 25, New Terminology: added terms for: blade enclosure, rack, and server blade.
Chapter 2	2.2	Page 31, System Requirements: modified Server requirements to include only Windows 2000 and above.
Chapter 2	2.1	Page 45, Specifying the IP Address for a Remote Management Portal: topic replaced with a note because the use of the Messaging Server eliminates this task.
Chapter 2	2.1	Page 45, deleted the post-installation topics: Verifying the Contents of ZTASKEND, and Configuring edmprof.dat. These are no longer needed.
Chapter 2	2.1	Page 45, Posting Client Objects to the Management Portal: new post-installation configuration option.



Chapter	Version	Change
Chapter 3	2.1.1	Page 56, Banner: Clicking the information icon  also logs the version and build information being displayed to <code>httpd-port.log</code> .
Chapter 3	2.2	Page 84, Paging and Filtering Icons: added About LDAP Paging topic.
Chapter 4	2.1.1	Page 127, Understanding Network Discovery: added note that Network Discovery is not supported on a Windows NT 4.0 platform.
Chapter 4	2.1.1	Page 135, Adding a Directory Service: added a new Type of LDAPS (LDAP over SSL). New or revised topics include: <ul style="list-style-type: none"> • Page 136, Preparing for an LDAPS Directory Service Connection: new topic explains requirements for using LDAPS. • Page 140, Specifying LDAP or LDAPS Directory Service Properties: modified topic and Table 5 to include information and properties for adding an LDAPS directory service type. Note: Debug LDAP Level and Debug LDAP Log properties apply to both LDAP and LDAPS.
Chapter 4	2.1.1	Page 140, Table 5, URL definition expanded to include syntax and examples for connecting to a Novell Directory Service (NDS) and an LDAPS Directory Service.
Chapter 6	2.1.1	Page 362, Viewing and Logging Version Information, clicking  both displays and logs the version and build information for the Management Portal modules.

Table 2 Task Name Changes from Version 2.1, by Task Group

Task Group	Old Task Name	New Task Name
Directory Management	Restore Directory	Restore
	Update Tasks	Update Portal Tasks
Infrastructure	Connect to Directory Service	Start Directory Service
	Disconnect from Directory Service	Stop Directory Service

Task Group	Old Task Name	New Task Name
Model Administration	Move/Copy Device(s)	Move Device
	Remove Desktop Shortcuts	Remove Desktop from Shortcut
Operations	Add Job Sequence	Sequence Job
	Install Client	Install Radia Client
	Install RMP	Install Management Portal
	Manage Proxy Assignment	Assign Proxy Server
	Notify by Device	(Deleted)
	Notify via Inventory	(Deleted)
	Notify by Subscription	(Deleted)
	Purge Dynamic Cache	Purge Proxy Server Dynamic Cache
	Schedule Zone Operation	Zone Job
	Update RMP	Update Management Portal
Policy	Modify Defaults	Modify Policy Defaults
Policy (Advanced)	Modify Dependencies	Modify Policy Dependencies
	Modify Flags	Modify Policy Flags
	Modify Overrides	Modify Policy Overrides
	Modify Targets	Modify Policy Targets
RCS Administration	Add Connections	Add Component to Instance
	Copy	Copy Instance
	Create	Create Instance
	Delete	Delete Instance
	Modify	Modify Instance
	Remove Connections	Remove Component from Instance

Support

Please visit the HP OpenView support web site at:

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

This web site provides contact information and details about the products, services, and support that HP OpenView offers.

HP OpenView online software support provides customer self-solve capabilities. It provides a fast and efficient way to access interactive technical support tools needed to manage your business. As a valuable support customer, you can benefit by using the support site to:

- Search for knowledge documents of interest
- Submit enhancement requests online
- Download software patches
- Submit and track progress on support cases
- Manage a support contract
- Look up HP support contacts
- Review information about available services
- Enter discussions with other software customers
- Research and register for software training

Most of the support areas require that you register as an HP Passport user and log in. Many also require a support contract.

To find more information about access levels, go to:

http://www.hp.com/managementsoftware/access_level

To register for an HP Passport ID, go to:

<http://www.managementsoftware.hp.com/passport-registration.html>

Contents

- 1 Introduction 17**
 - Introduction18
 - About the Core Capabilities19
 - About the Product Architecture.....20
 - Management Portal Zones Overview22
 - What is a Zone?22
 - The Zone Directory Structure22
 - About Object Names in a Zone23
 - New Terminology.....25
 - Summary28

- 2 Installing the Management Portal 29**
 - Preparing for Installation30
 - Installing the Management Portal30
 - Radia Prerequisites.....30
 - System Requirements31
 - Directory Size of a Single Zone.....31
 - Installation Procedures.....32
 - Updating Portal Tasks.....43
 - Updating Management Portal Zones with a New Build44
 - Specifying the IP Address for a Remote Management Portal.....45
 - Posting Client Objects to the Management Portal45
 - Starting and Stopping the Management Portal45
 - Accessing the Management Portal46
 - Logging On47
 - Changing Passwords48
 - Summary51

3 Using the Management Portal.....	53
Performing Any Task in the Management Portal.....	54
About the Management Portal 2.x Interface.....	55
Banner.....	56
Using the Navigation Aid.....	57
Navigation Modes: History and Location.....	58
Sample Navigation Session: Viewing Network Objects.....	60
Accessing and Returning to Your Desktop.....	62
Adding Shortcuts to Your Desktop.....	62
Removing Shortcuts from Your Desktop.....	64
Navigating the Portal Directory and the Zone Containers.....	65
Taskbar and Task Summary.....	70
Directory Management Task Group.....	71
Infrastructure Task Group.....	72
Model Administration Task Group.....	72
Operations Task Group.....	75
Policy Task Group.....	78
Policy (Advanced) Task Group.....	80
RCS Administration Task Group.....	80
Toolbar Tasks.....	82
Toolbar.....	82
Navigation Icons.....	83
Task Icons.....	83
Print and Status Icons.....	83
View Icons.....	84
Paging and Filtering Icons.....	84
About LDAP Paging.....	84
Paging and Filter Icon Details.....	85
Workspace.....	86
Radia Directory and Zone Objects.....	86
About the Zone Containers.....	88
Obtaining Descriptions using Details View.....	92
Using the RCS Administration Tasks.....	93
Prerequisites.....	93
About the RCS Administration Tasks.....	94
Creating Instances.....	95
Adding Components to Instances.....	96
Copying Instances.....	98

Deleting Instances	99
Modifying Instances	99
Removing Components from Instances	100
Using RMP to Assign Policy through an LDAP Directory	102
Prerequisites	102
About the Policy Tasks	103
Adding a Policy Object	104
Removing a Policy Object	105
Modifying Policies	105
Modifying Policy Targets	107
Resolving Policy	109
Customizing Domain Filters (DNAMES) in the Resolve Policy Task	114
Refreshing the Managed Services Cache	115
About the Policy (Advanced) Tasks	116
Modifying Policy Dependencies	116
Modifying Policy Flags	118
Modifying Policy Defaults	119
Modifying Policy Overrides	121
Summary	123

4 Administrative Functions 125

Configuring a Management Portal Zone	126
Understanding Network Discovery	127
Configuring Network Discovery	128
Using NETSCAN_INCLUDE to Limit Network Discovery	131
Setting Additional Configuration Parameters	132
Configuring Directory Services	134
Adding a Directory Service	135
Preparing for an LDAPS Directory Service Connection	136
Specifying LDAP or LDAPS Directory Service Properties	140
Specifying RCS Directory Service Properties	143
Specifying DSML Directory Service Properties	146
Specifying Metakit Directory Service Properties	146
Modifying Directory Service Properties	148
Removing a Directory Service	149
Starting a Directory Service	150
Stopping a Directory Service	152
Configuring for External LDAP Authentication	153
Modifying the Default LDAP Authentication for Specific Users	156
Configuring for a Custom LDAP Policy Extension Prefix	156

Configuring Zone Access Points	158
Establishing Devices and Device Groups.....	159
Adding Devices to an RMP Zone.....	159
Basic Procedures for Modifying Groups.....	161
Using the Browse and Modify Window.....	162
Using the Group List Area	164
Using the Attribute Editor	166
Using the Expression Editor	169
Using the Browse Area	173
Current Navigation Location.....	174
Navigation Icons	174
Action Icons.....	174
View Icons	174
Paging and Filtering Icons.....	175
Selection Icons	175
Configuring the Zone Infrastructure.....	175
Adding a Single Device	175
Generated Common Names for Devices.....	177
Viewing Device Properties.....	178
Adding Groups.....	181
Adding Devices to a New Group.....	183
Moving Devices into a Group	186
Removing Groups of Devices	191
Importing Devices	192
Dynamic Job Scheduling Against Groups of Devices	194
Adding Services.....	195
Modifying Objects	198
Removing Objects.....	199
Configuring Blades, Enclosures and Racks	200
About the Predefined Blade Enclosure Configurations.....	203
Adding an Enclosure Configuration	203
Adding an Enclosure.....	206
Applying Policy to Blades, Enclosures and Racks	211
Enabling Policy Configurations for Blades, Enclosures and Racks	211
Assigning Policy Based on Enclosure Model Types.....	212
Assigning Policy Based on Enclosure Configurations.....	212
Configuring Task Groups.....	213
Adding Task Groups	213
Modifying Task Groups	217
Removing Task Groups.....	218

Configuring Delegated Administration	219
Adding Delegated Administration Roles	220
Modifying Delegated Administration Roles	227
Removing Delegated Administration Roles.....	228
Querying a User's Delegated Administration	228
Configuring Administrators and Operators.....	230
Adding Users	230
Modifying Users	233
Removing Users	235
Adding User Groups.....	235
Modifying Groups.....	237
Removing Groups	238
Managing the Portal Zone Directory.....	239
Creating a Backup of the Portal Zone Directory.....	239
Backup Directory Naming, Contents, and Maintenance	240
Restoring the Portal Directory	243
Querying the Portal Directory.....	245
Exporting Data from the Portal Directory	247
Importing Data into the Portal Directory.....	249
Updating Portal Tasks.....	253
Managing Jobs	255
Filtering Job Groups or Jobs by Status	255
Modifying Job Groups	256
Querying Jobs or Job Groups	258
Restarting Failed Jobs in a Job Group	260
Stopping Job Groups	261
Disabling Jobs or Job Groups.....	262
Enabling Jobs or Job Groups.....	262
Removing Jobs or Job Groups	263
Viewing Job History.....	263
Viewing Properties	264
Summary	266

5 Operations Functions 269

Managing Computers in Your Management Portal Zone	272
About the Task Lifecycle	275
Basic Procedures for Operations Tasks.....	276

Selecting a Starting Zone, Network, or Directory Location	276
Performing Queries	277
Selecting an Audience	279
Scheduling Jobs	281
Core Tasks	283
Using the Notify Tasks	283
Notifying an Audience	284
Using Help Desk Notify	286
Setting Default Options for Notify Commands	288
Creating Custom Notify Commands	292
Deploying Radia Management Infrastructure Products and Applications	294
Requirements for Remote Installations	294
Installing the Radia Management Agent	295
Choosing a Dynamic or Static Port Assignment for the Radia Management Agent	297
Refreshing the Radia Management Agent	302
Installing the Radia Client	302
Supporting Remote Installs Using Multiple Profiles	307
Adding, Modifying, and Deleting Install Profiles	308
Client Install Profiles –Source Code Required Locations	308
Assigning Proxy Servers	311
Discovering Radia Subscriber Information using Managed Services	314
Installing the Proxy Server	315
Preparing and Locating Configuration Files for Proxy Server Installs	319
Synchronizing the Proxy Server	320
Purging the Dynamic Cache of the Proxy Server	322
Managing Services	323
Managing Task Templates	324
Adding Task Templates	324
Removing Task Templates	327
Installing Additional Management Portal Zones (Subordinate Zones)	327
Updating Subordinate Management Portal Zones	333
Scheduling Zone Operations	334
What happens with jobs scheduled from Remote Zone Operations?	339
Opening a Subordinate Zone	339
Sequencing Jobs (In Progress)	341
Remote Control (Windows Clients Only)	341
System Requirements	342
Prerequisites	342
Connecting the Remote Control Service to Users	342
Using Remote Control (Windows Clients Only)	345
Customizing the Start Viewer Task Properties	348
Configuring Remote Control	349

Summary	355
6 Troubleshooting.....	357
About the Log Files.....	358
Setting Trace Levels	358
Common Message Types	360
Collecting Information for HP Technical Support.....	362
Viewing and Logging Version Information	362
Gathering Version Information for NVDKIT.EXE	363
Gathering Version Information for RADISH.EXE	364
Managing the Portal Zone Directory (ZONE.MK) File	365
Summary	366
 Index	 367

1 Introduction

At the end of this chapter, you will:

- Understand the benefits and core capabilities of Management Portal.
- Understand the architecture and Directory Structure of any Management Portal Zone.
- Be familiar with new terminology for this release.
- Understand the process of adding devices to your Management Portal zone and grouping them for operational purposes. Creating and using device groups for administrative and operational tasks greatly improves Management Portal performance.



The Management Portal performs best when operations are run against groups of devices, as opposed running the same operation against against one device at a time.

Introduction

The 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 Management Portal to view and manage your existing infrastructure, and remotely install new Radia infrastructure products and applications.

The Management Portal provides the following benefits:

- **Consistency**
A simple, consistent user experience reduces the learning curve for your administrators. When using the 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 Management Portal Directory.
- **Extensibility**
Access any Configuration Server, Radia Database, Active Directory, or other LDAP Directory in your enterprise from within the Management Portal's interface. Administer policy, services, users, and machines directly from the Portal's friendly interface.
- **Enterprise-Wide Solutions**
Create multiple Management Portal Zones, if desired, to administer the infrastructure at different sites in your enterprise. From any Management Portal, you can access any Zone in your enterprise and perform operations across multiple-zones.

About the Core Capabilities

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

- **Network Discovery**
The Management Portal automatically discovers the objects in your networks.
- **Authentication**
Use the Management Portal Directory to authenticate administrators.
- **Delegated Administration**
Create roles in the 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 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 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 Management Portal.
- **Remote Infrastructure Administration**
Use the 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 Configuration Server and Policy Administration**
Use the Management Portal to access the Radia Database on any Configuration Server in your enterprise, perform instance-level tasks, and assign and manage Policy through Active Directory.
- **Cross Referenced Device Groups**
The Management Portal captures detailed information regarding device hardware, operating system, Radia infrastructure and managed services and stores it in the 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 device groups that you select. Notify all devices of a given type in one or all zones in your

enterprise. Notify using Wake-On-Lan (WOL) to perform operations during off-peak hours.

- **Querying**
Use the query feature to extract information from the Management Portal Directory.
- **Scheduling**
Use the scheduling feature to execute and track the progress of any task.
- **Auditing/Logging**
Use the auditing and logging features to view information about administrators and the activities they performed within the Management Portal. All audit events will be stored in the log generated by the Management Portal.

About the Product Architecture

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

The 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 `\modules` directory).
- The **Portal Zone Directory**, `zone.mk` (in the Radia Integration Server `\etc` directory), is an LDAP directory service. When it starts, it loads the set of objects that represent a given instance of the 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`)
 - Chassis container for blade enclosures and racks (`chassis.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 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 Management Portal. See *Installing the Radia Management Agent* on page 295 for more information.

Management Portal Zones Overview

Very large enterprises often find it necessary to use multiple 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 Management Portal by defining a Zone and a specific Zone Directory Structure for each 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 Management Portal.

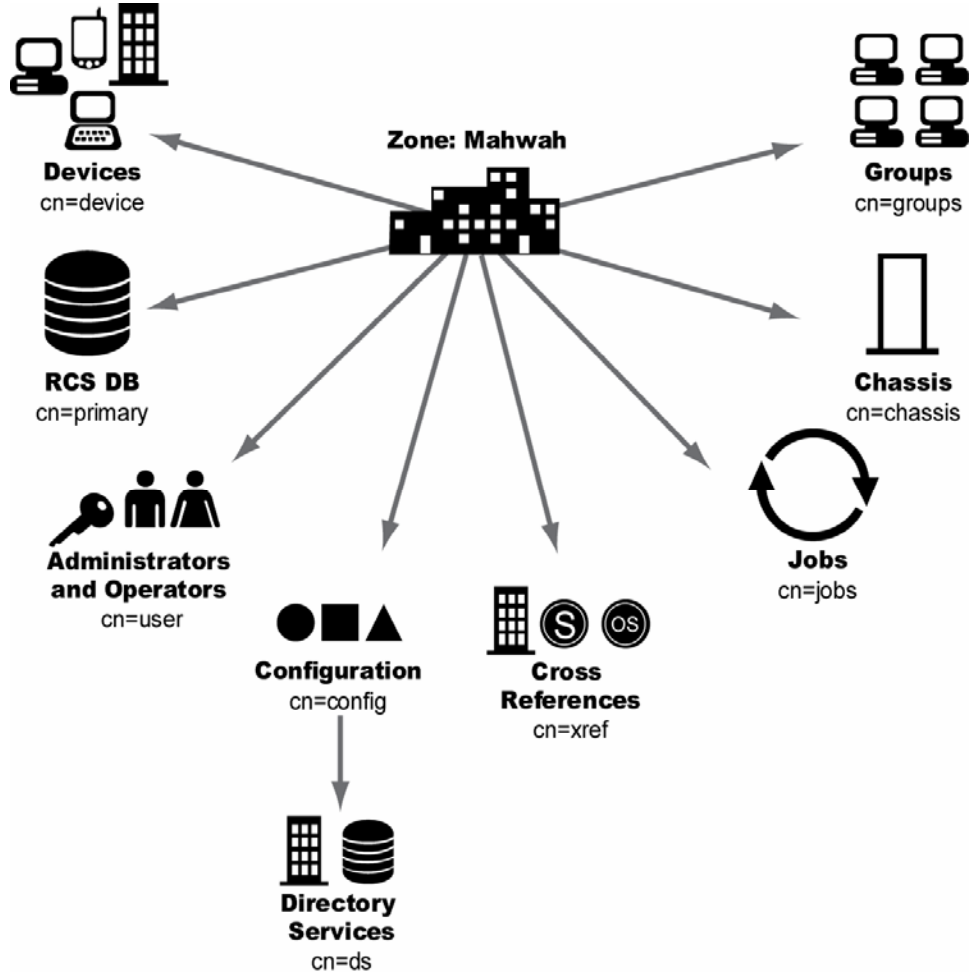
A zone is created whenever the Management Portal is installed, and all objects in the zone include the high-level qualifier of the zone name. The first installed zone is called the master zone and others are called subordinate zones. The properties for the Zone object, itself, include the URL information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

The Zone Directory Structure

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

The next figure illustrates the Zone Directory Structure and Containers. See About the Zone Containers on page 88 for a description of each container and how they are used.

Figure 1 Management Portal Directory of a Zone

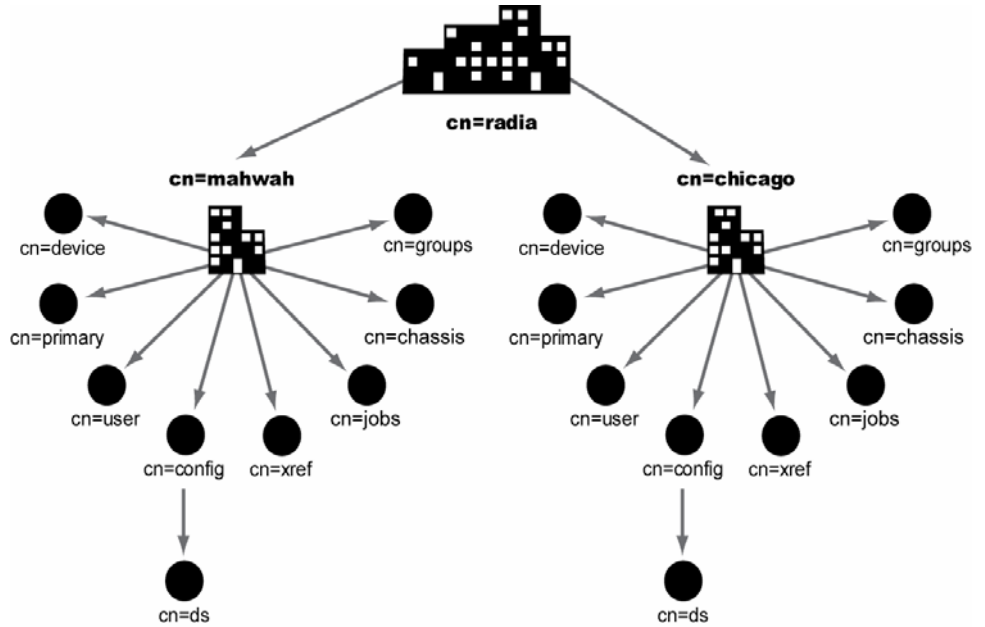


About Object Names in a Zone

The 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 the figure above is `cn=device, cn=Mahwah` and the location of the PRIMARY file on the RCS is `cn=Primary, cn=Mahwah`.

Figure 2 Multiple Zones of the 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 the figure above, 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`.

- ▶ The Common Name for any object displays in a small popup window as you hover your mouse pointer over the object's icon or label in the 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 Management Portal. These include any Lightweight Directory Access Protocol (LDAP) directory, the Configuration Server, DSML (allowing access to another Management Portal zone), and metakit (*.MK) files. Metakit files allow access to a customized Management Portal container.

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

blade enclosure

A physical container for a set of blades servers. It consists of a backplane that routes power and communication signals and additional hardware for cabling and thermal issues. It also hosts the CPU or server power supplies. See rack and server blade.

managed device

A computer or other hardware device in your network, such as a PDA or printer, that has been added to a 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 Management Portal zone installed at an enterprise. Additional Management Portals are installed as subordinate zones to the Management Portal Master Zone, also called the Master Portal.

rack

A set of components cabled together to communicate between themselves. A rack is a container for an enclosure. See enclosure.

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.

server blade

A single circuit board, containing microprocessor(s), memory, and network connections that is usually intended for a single, dedicated application (such as serving Web pages) and that can be easily inserted into a space-saving rack or rack-mountable enclosure with many similar servers. Server blades are more cost-efficient, smaller and consume less power than traditional box-based servers. See enclosure and rack.

subordinate zone

The secondary Management Portal zones installed at an enterprise, usually from the initial 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 Management Portal.

A zone is created whenever the 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 Management Portal zones in your enterprise. Go to the Zone Access Points container to open another zone's 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 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 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 Management Portal consists of the Portal Run-time, the 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 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 Management Portal

At the end of this chapter, you will:

- Be able to install the Management Portal.
- Modify the `\media` folders to include a `\default` directory for client installs.
- Be able to log on to the Management Portal.
- Be able to change your password.

Preparing for Installation

- 1 Before installing the Management Portal, locate your HP license file.
If you need assistance, contact HP Technical Support.
- 2 Assemble the following set of Configuration Management CD-ROMs that are used during a complete Management Portal install:
 - Radia Infrastructure CD-ROM
 - Radia Applications CD-ROM
 - Radia Documentation CD-ROM
- 3 Review the README file delivered with the product for the latest information.

Installing the Management Portal

You can use the 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 Management Portal (RMP) sites using the new zone architecture and features. Each Management Portal site being managed from the master portal site needs to have version 2.1 or above installed.

Radia Prerequisites

Management Portal 2.1 has been optimized to work with the REXX method ZTASKEND (Version 1.8 or above) and the HP OpenView Messaging Server Using Radia (Messaging Server), version 2.0 or above.

We recommend using the Management Portal with the latest ZSTASKEND and the latest Messaging Server to improve the information process flow between the Configuration Server and the Management Portal.

- The minimum ZTASKEND required is Version 1.8. This is installed with the Configuration Server 4.5.4 SP3.

- Using the latest version of ZTASKEND that is available with the latest Configuration Server and Service Pack upgrade enhances Management Portal performance.

For details on migrating your Configuration Server, refer to the *Radia_RCS_Migrate.PDF* located in the `migrate_RCS` folder of the Radia 4.2 RCS media location.

For details on installing the Messaging Server, refer to the *Installation and Configuraton Guide for the Messaging Server using Radia (Messaging Server Guide)*. For details on upgrading to the latest version of the Messaging Server, refer to the Release Notes for that product.

System Requirements

- **Server**
 - Windows 2000 and above, with minimum Server Pack (SP) levels listed below:
 - Windows 2000, SP 3
 - Windows XP Professional, SP2
 - Windows Server 2003, SP1
 - Installation of the Management Portal requires Administrator authority.
- **Web Client**
 - Any platform that supports a Web browser
 - Microsoft Internet Explorer 4.0 or higher or Netscape 4.0 or higher *with cookies enabled*
 - Security for a Microsoft Internet Explorer browser must be set no higher than **medium**

Directory Size of a Single Zone

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

A single Radia Management 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: 5,000 devices

Multiple 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 Management Portal Zones (Subordinate Zones)* on page 327.

Installation Procedures



Do not install this version of the Management Portal on a machine running a 1.x version of the Management Portal. For more information, refer to the *Upgrade Procedures PDF* located in the `management_portal\migrate` folder of the Radia 4.1 Extended Infrastructure media location.

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

To install additional Management Portal Zones in your enterprise, use the *Install Management Portal* task in the *Operations* task group. For details, see *Installing Additional Management Portal Zones (Subordinate Zones)* on page 327.

To install the Management Portal 2.x



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

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

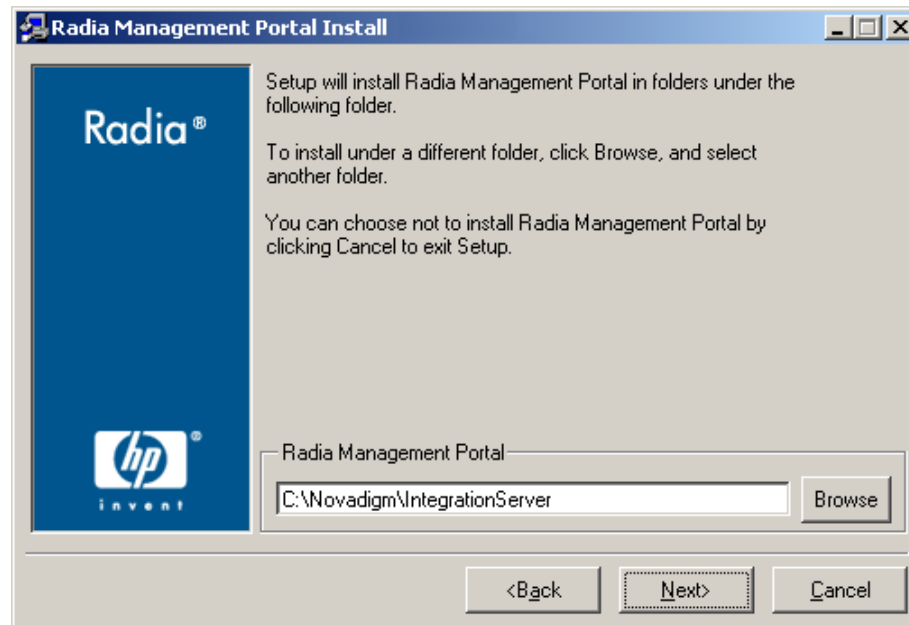
The Welcome window for the Management Portal Setup program opens.

- 2 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 Management Portal can be installed.

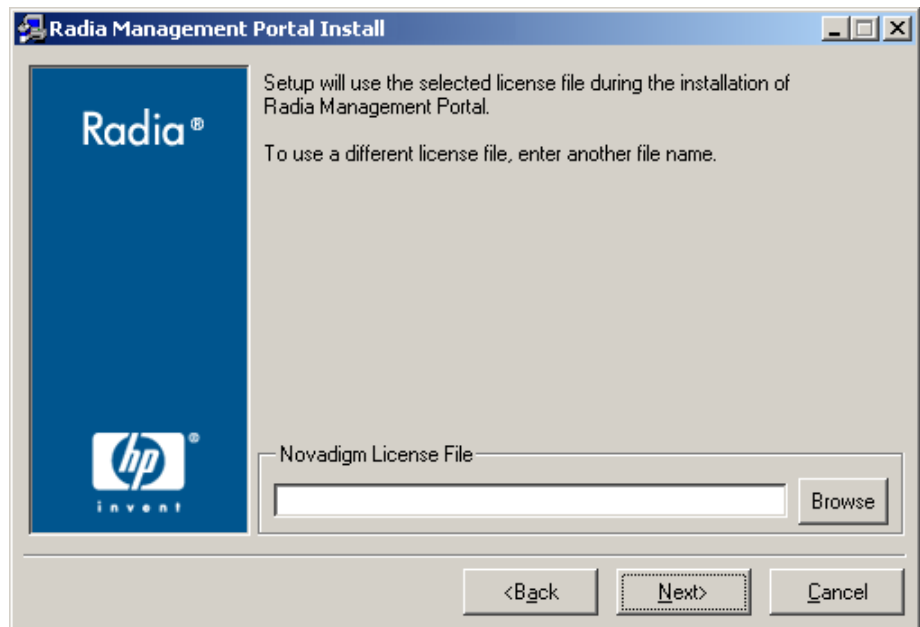
- 3 Click **Accept** to agree to the terms of the software license and continue with the installation.

The Management Portal Location window opens.



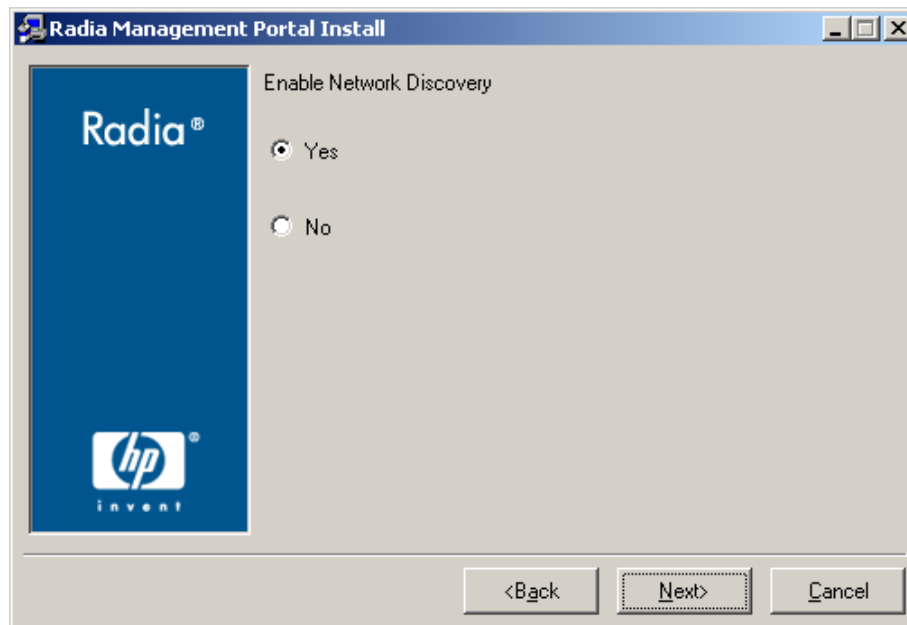
- 4 Use this window to select the folder where you want to install the Management Portal.
 - ▶ If the Inventory Manager is already installed on the computer, the Management Portal will be installed in the same directory, and the prompt for an install location is skipped.
- 5 Click **Next** to accept 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.



- 6 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 `\modules` directory.

The Enable Network Discovery window opens.



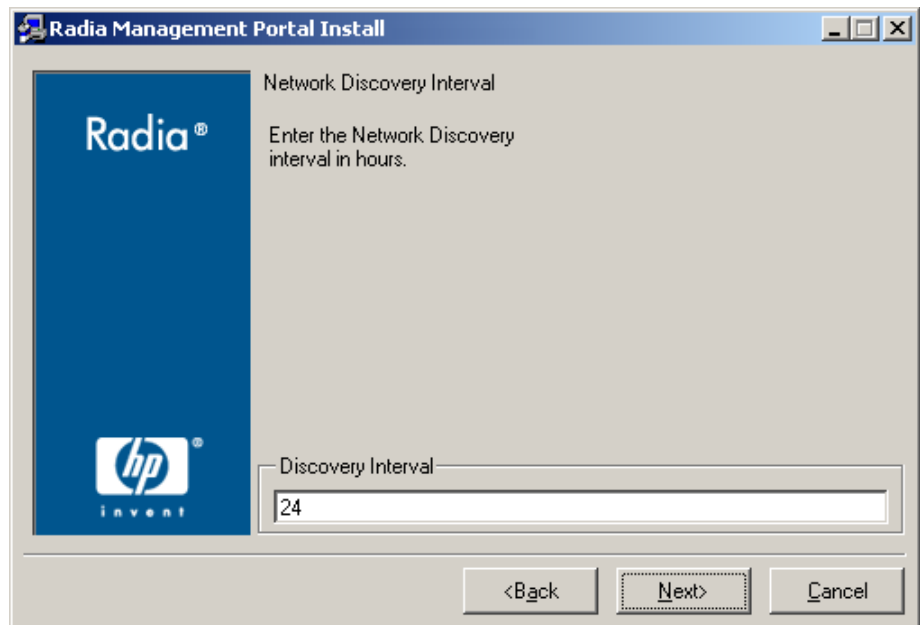
- 7 Click **Yes** to enable Network Discovery (*recommended*). This option enables the Management Portal to automatically discover all devices in your Windows environment that you can manage.

or

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

- 8 Click **Next**.

The Network Discovery Interval window opens.

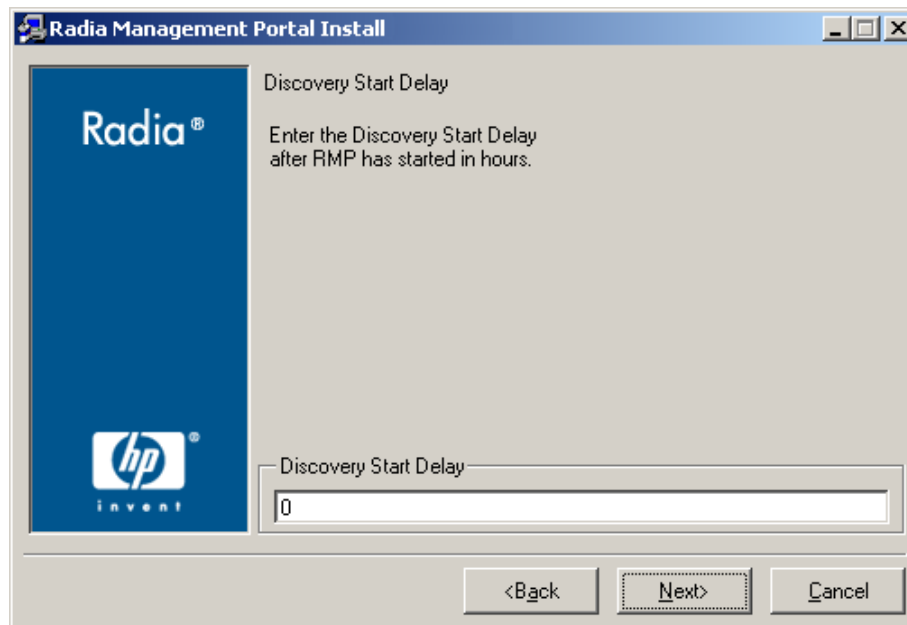


- 9 In the Discovery Interval text box, type how often (in hours) you want the network discovery job to run. Valid entries are 1 to 24. The default is 24 hours.

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 128.

- 10 Click **Next**.

The Discovery Start Delay window opens.

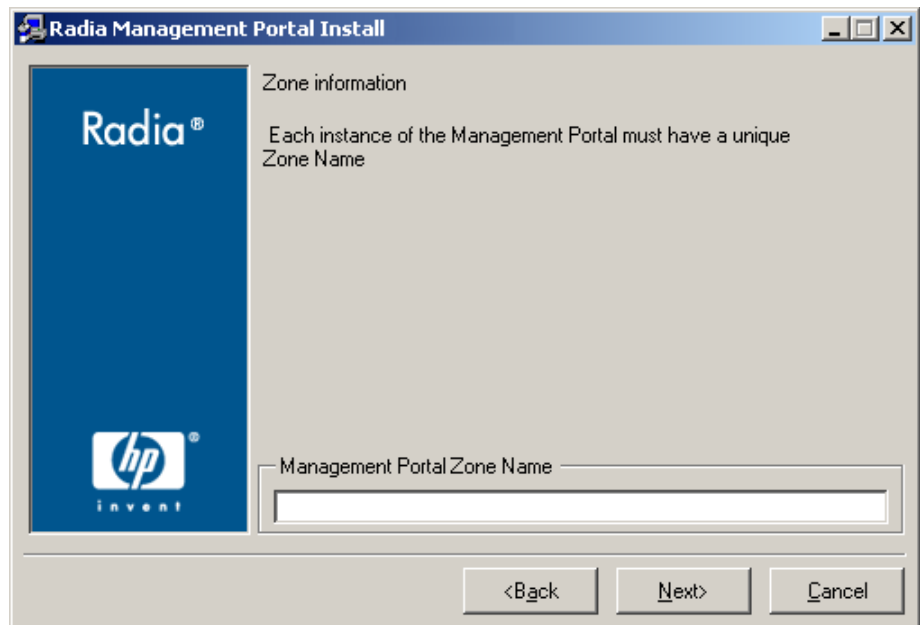


- 11 In the Discovery Start Delay text box, type how long you want to wait (in hours) after the Management Portal starts before starting the network discovery. The delay applies each time the Management Portal is started. Valid entries are 0 to 24 hours. By default, Network Discovery starts when you start the 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 128.

- 12 Click **Next**.

The first Zone information window opens.



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

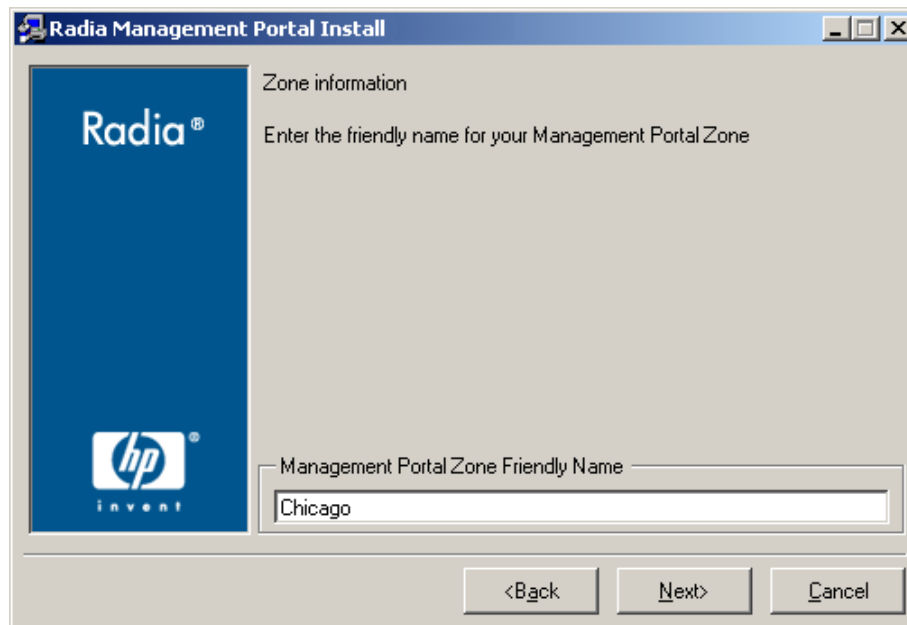
Enter a name up to 64 characters long. Use only letters (a-z and A-Z), numbers (0-9) and the space character. Do not use special characters, such as an underscores, commas, or periods.

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 22 for more information about Zones.

- 14 Click **Next**.

The second Zone information window opens.



- 15 In the Management Portal Zone Friendly Name text box, optionally type a friendly name for this Management Portal Zone. If omitted, the friendly name defaults to the Zone Name.

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

- 16 Click **Next**.

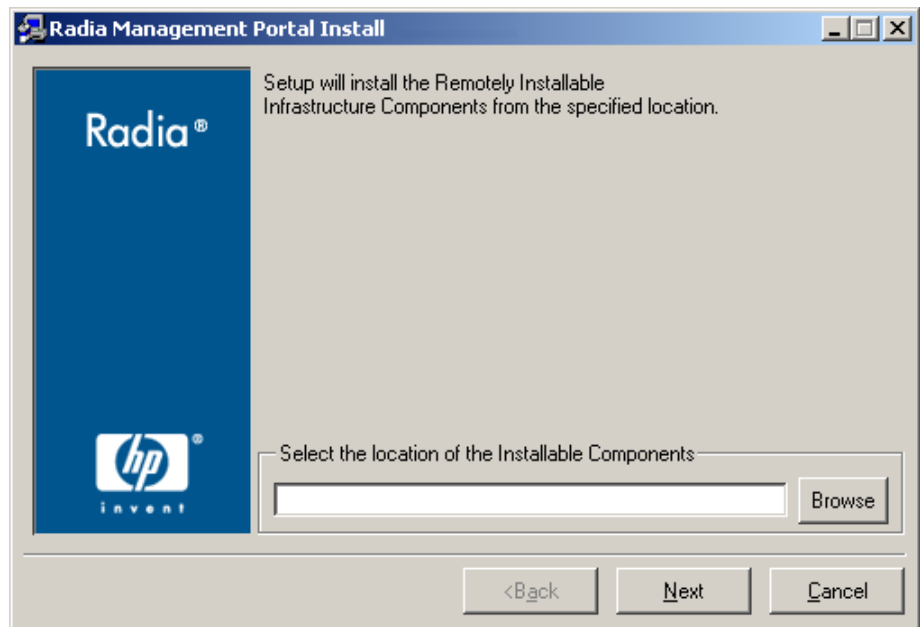
A summary window of the installation information opens.

- 17 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.

- 18 Click **Yes**.

The Remotely Installable Components Location window opens.



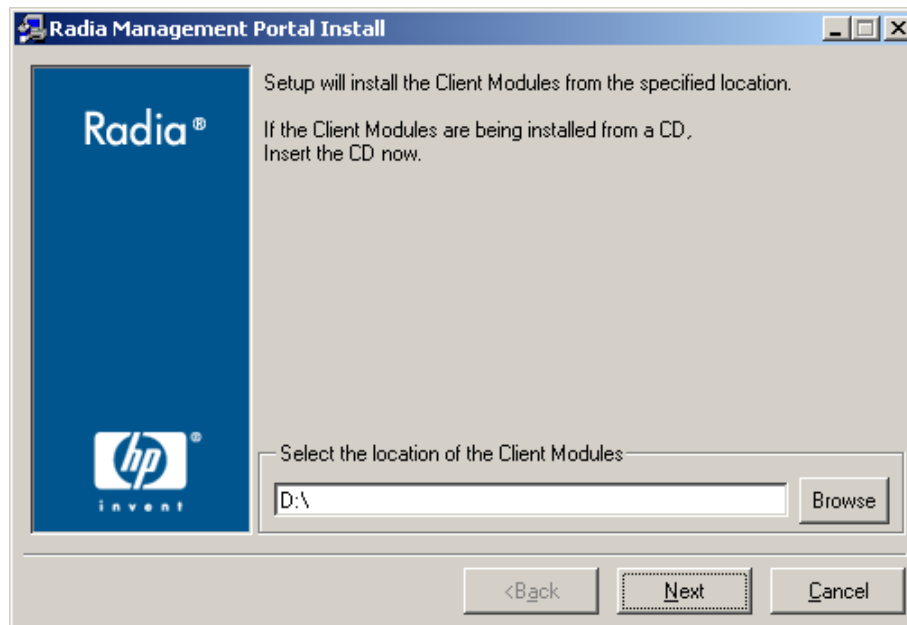
If necessary, click **Browse** to navigate to the location of the Management Infrastructure CD-ROM.

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

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

- 20 Click **Yes**.

The Client Modules Location window opens.

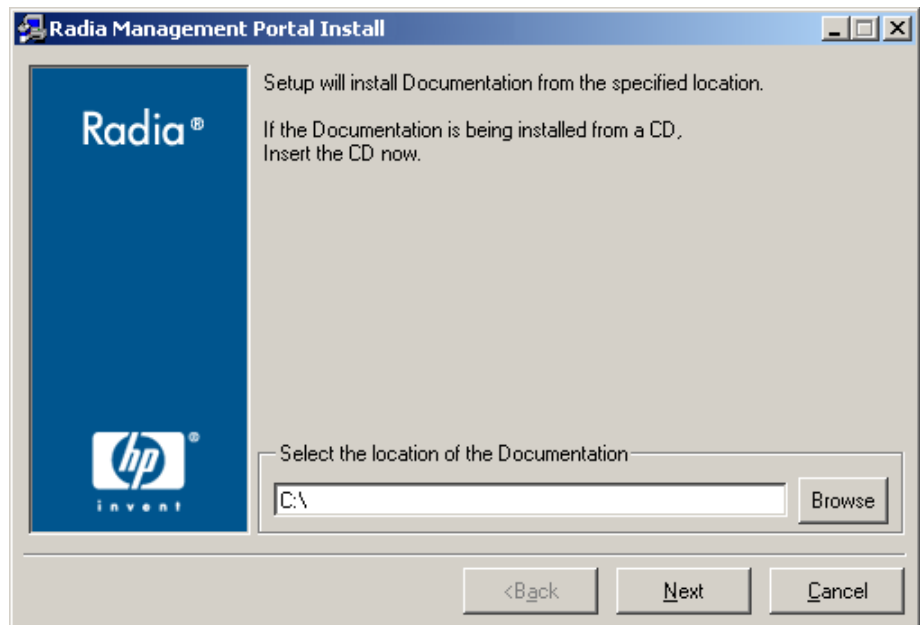


If necessary, remove the Management Infrastructure CD-ROM and insert the Management Applications CD-ROM.

- 21 Click **Browse** to navigate to the location of the Management Applications CD-ROM for the Radia Client modules.
- 22 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).

- 23 Click **Yes**.
The Publications Location window opens.



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

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

- 25 Click **Next**.

The Radia Publications Library is installed to the Management Portal.

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

Completing the installation automatically starts the Management Portal service as well as displays the Management Portal Welcome window, which prompts you to logon.



See Starting and Stopping the Management Portal on page 45 and Accessing the Management Portal on page 46 for information on performing these tasks manually.


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

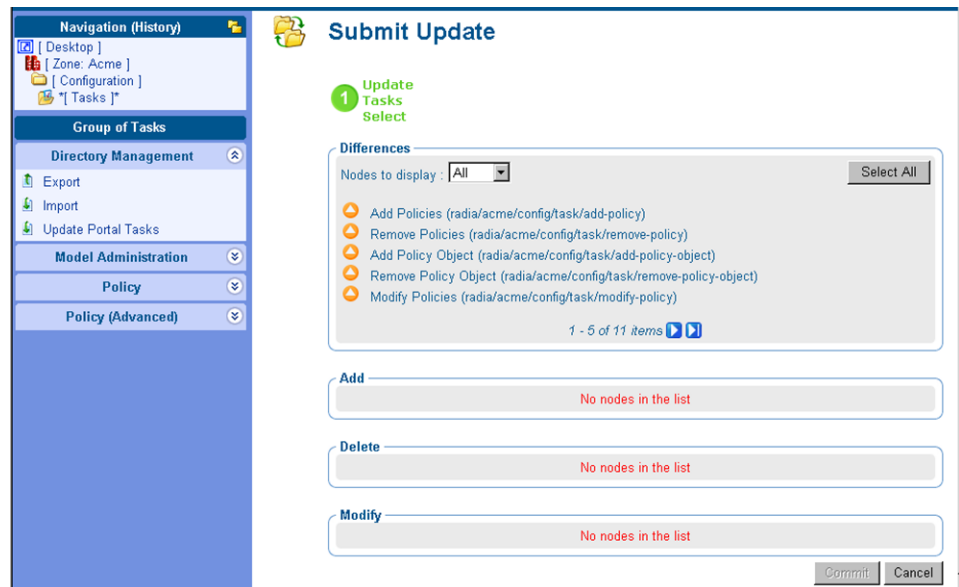
Updating Portal Tasks

- ▶ This task is not required the first time you install Management Portal Version 2.x.

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

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

- 1 If necessary, restart the Management Portal, (the Radia Integration Server [httpd] service).
 - 28 Logon as **Admin** (the password is **secret**) and run Update Portal Tasks. Details for running Update Portal Tasks follow.
 - 29 Use the Navigation aid to select **Directory → Zone → Configuration → Tasks**.
 - 30 In the Directory Management task group, click **Update Portal Tasks**.
 - 31 The Submit Updates dialog box opens.
 - 32 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.
-  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.



33 Click **Commit**.

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

To log off the Management Portal

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

Updating Management Portal Zones with a New Build

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

To update the subordinate Zones in your enterprise with a new build, the Management Portal includes an Update Management Portal task. For details, see Updating Subordinate Management Portal Zones on page 333.

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 Management Portal Zone as well all devices being managed by that Zone.

Specifying the IP Address for a Remote Management Portal

- ▶ When running the Configuration Server with the Messaging Server, it is no longer necessary to specify the IP address and port for the Management Portal in the MGR_RMP section of `edmprof.dat`.

Posting Client Objects to the Management Portal

As of Radia v4.x, all client objects collected by the Configuration Server are routed to external servers and databases by the Messaging Server. When a Messaging Server is installed, it may be configured to post objects to a Management Portal Zone or discard them.

For details on how to how to configure the Messaging Server to post client objects to a Management Portal Zone, refer to the *Messaging ServerGuide*.

- ▶ Notifying clients using Wake-On-Lan (WOL) from the Management Portal no longer requires you to route client objects to the Management Portal. The Radia Management Agent now collects the MAC address and Subnet information needed for WOL directly from any device which has a Radia client installed.

To verify that the Messaging Server is posting objects to the specified Management Portal, you can either monitor the posts in the Messaging Server log or check the Cross References container for Managed Services in the Management Portal (since each client's device will show the services that you deployed to it under the Cross References for Managed Services container).

Starting and Stopping the Management Portal

To start the 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, go to **Manage** → **Expand Services and Applications** → **Services**.
- 2 Right-click the Radia Integration Server and select Start.

To stop the Management Portal

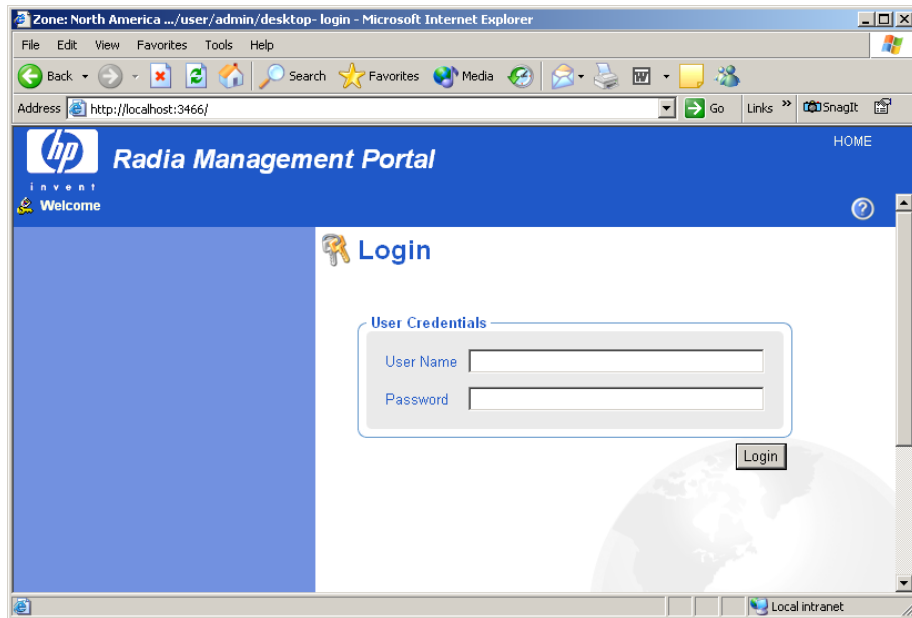
- 1 If necessary, go to the Windows Services. For example, in Windows 2000, right-click the **My Computer** icon on your desktop. Then, go to **Manage** → **Expand Services and Applications** → **Services**.
- 2 Right-click the Radia Integration Server and select **Stop**.

Accessing the Management Portal

To access the Management Portal

- 1 Open your Web browser.
 - ▶ See the Client topic of System Requirements on page 31 to review the Web browser requirements for the Management Portal.
- 2 In the Address bar, type the following:
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.
- 3 Press **Enter**.

The Welcome page for the Management Portal prompts you to Login.



The banner area of the Management Portal will display additional links (next to the top-right HOME link) when other HP OpenView using Radia products or publications are installed on the same computer. For details, see the Banner discussion on page 56.

Logging On

To log on to the Management Portal

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

— **Admin**

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

The password is **secret**.



Be sure to change your password before moving the Management Portal into your production environment. See Changing Passwords on page 48 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.
- 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 Management Portal on page 54 for more information.

To log off the 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 Management Portal user interface, see page 55.

- For information about performing tasks, see *Performing Any Task* in the Management Portal on page 54.

To change your password

- 1 Use the Navigation aid and workspace to go to the 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.

➤ The User Password field is not shown on the Properties dialog box for a Person, but can be changed from the Modify Properties dialog box for that Person.

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

The Modify Person dialog box opens.

 **Modify Person**

Properties

Description	This user has complete access to the system.
Display Name	Portal Administrator
User Password
External User ID	
External authentication?	<input type="checkbox"/>

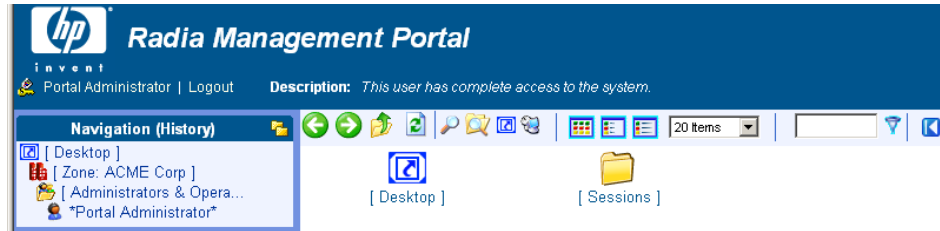
Group Membership

Available		Selected
Account Administrators (account_admins)	➤➤	
Auditors (audit_admins)	➤➤	
Infrastructure Administrators (infrastructure_admins)	⏪⏪	
Operations Staff (opsys)	⏪⏪	
Package Administrators (package_admins)		
Policy Administrators (policy_admins)		
RCS Administrators (rcs_admins)		
Service Administrators (service_admins)		


Modify Reset Cancel

- 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.



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

- ▶ To display the properties for any user, go to the **Zone** → **Administrators and Operators** container, select the user object, and then click the **View Properties** toolbar icon .

Summary

- Install an initial Management Portal 2.x, giving it a zone name. This installation becomes your enterprise's Master Zone.
- To install additional Management Portal zones, use the Install Management Portal 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 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 Portal Tasks** after obtaining a new build of the Management Portal to update the tasks available to you.
- Run **Update Management Portal** to update subordinate Zones in your enterprise with a new build, such as a Management Portal Service Pack.
- Optionally, the Messaging Server can be configured to route client-objects from the Configuration Server to the Management Portal.

3 Using the Management Portal

At the end of this chapter, you will:

- Be familiar with the 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 this version fo the Management Portal.
- 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 Management Portal Zone.
- Know how to navigate to locations that has been configured for access from the Management Portal, including Networks, the Radia Database on a 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 Management Portal

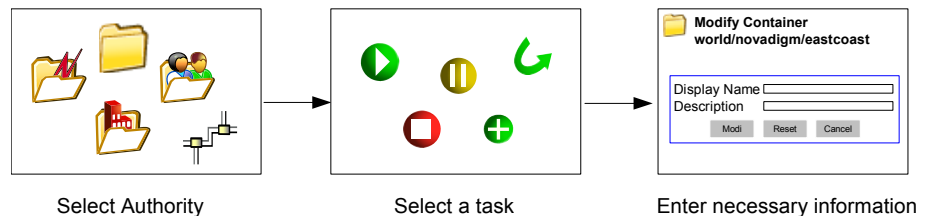
One of the benefits to using the Management Portal is consistency. Because of this consistency, you can use the same basic procedure whether you are notifying devices in your infrastructure or installing the Proxy Server on remote computers.

To perform any task in the Management Portal

- 1 Use the Workspace area and 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 70 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 275 for detailed information on completing tasks.



For detailed information about the user interface, see About the Management Portal 2.x Interface on page 55.

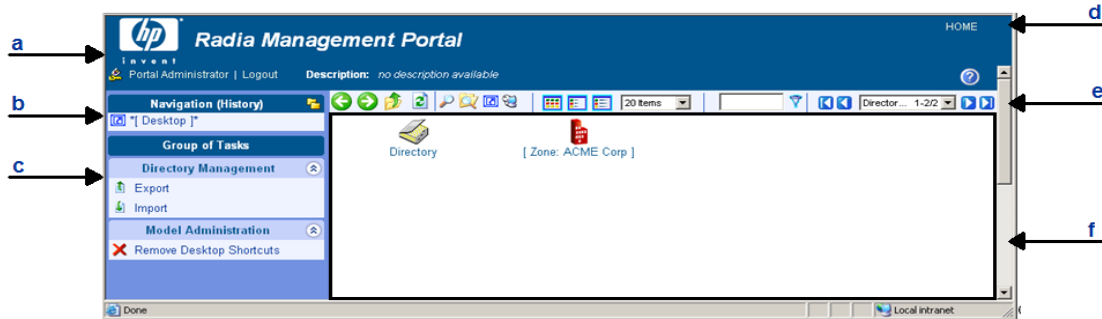
For detailed information about specific tasks, see the Administrative Functions and Operations Functions chapters.

For detailed information about using the RCS and Policy tasks, see the topics beginning with Using the RCS Administration Tasks on page 93.

About the Management Portal 2.x Interface

The Management Portal (RMP) user interface contains several distinct areas.

Figure 3 RMP 2.x User Interface



Legend

- a** Banner
- b** Navigation Aid
- c** Taskbar
- d** Links
- e** Toolbar
- f** Workspace

- **Banner area.** This area is discussed on page 56.
- **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 Management Portal 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 58.
- **New Desktop location.** When you log on to the Management Portal, you start at the level of your Desktop, in Navigation (History) mode. This starting location gives you quick access to the Management Portal Directory and the containers and objects in the current 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 62 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 70 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 82 for more information.
- **New Container objects** in your Radia Zone. See *Radia Directory and Zone Objects* on page 86.

Banner

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



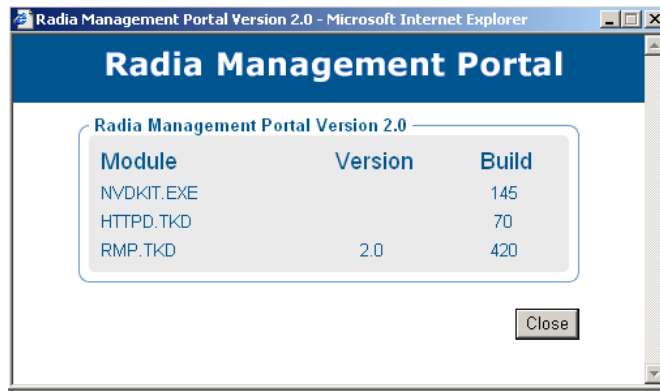
- Click **Logout** to log off the Management Portal (RMP).
- Click **HOME** to return to the RMP home page. This is the Directory location in Navigation (Location) mode.
- Rest the mouse pointer on the  button to display the Management Portal version number. For example, a display of RMP V2.1 indicates the Management Portal Version 2.1.
- After logging in, click the  button to view detailed version and build level information for the Management Portal component modules. A sample Version information window is shown in Figure 4 on page 57. Whenever this Version information window is displayed, the version and build information is also written to the Management Portal log file: `httpd-port.log`. Version and build information is helpful when you are contacting HP Technical Support. For more information, see *Viewing and Logging Version Information* on page 362.

Figure 4 Sample Version Information Window



If the Inventory Manager or Policy Server is installed on the same computer, click the appropriate link (**INVENTORY** or **POLICY**) in the banner of the Management Portal to access them.

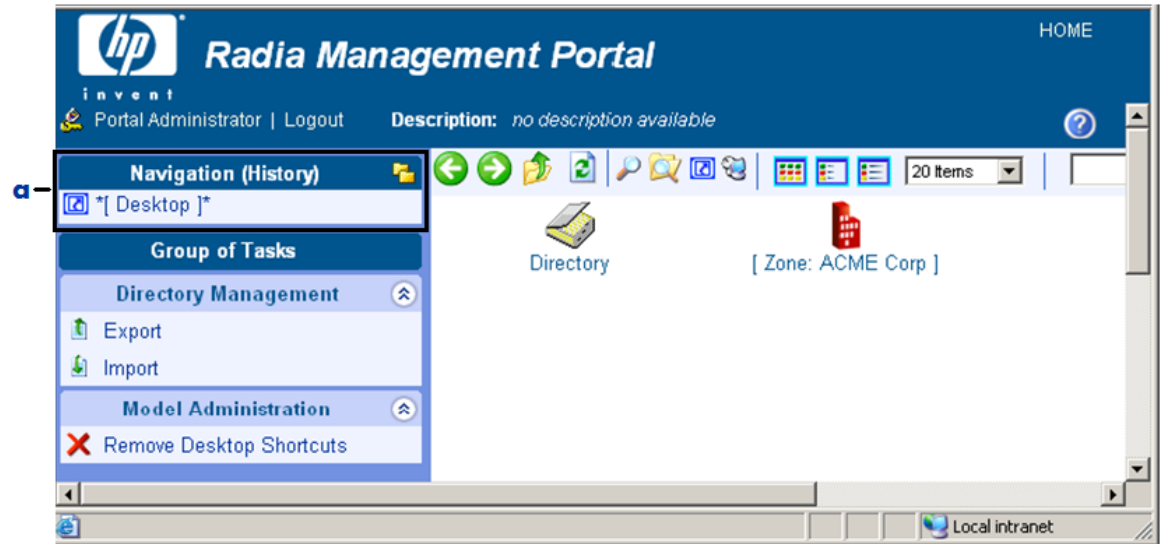
If the Radia Publications Library is installed on this computer, click the **PUBS** link in the banner of the Management Portal to access the library.

Using the Navigation Aid

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

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

Figure 5 Initial Desktop location in Navigation (History) mode





Legend



- History mode

This starting Desktop location gives you quick access to the Management Portal Directory and the containers and objects in the current 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 62 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.

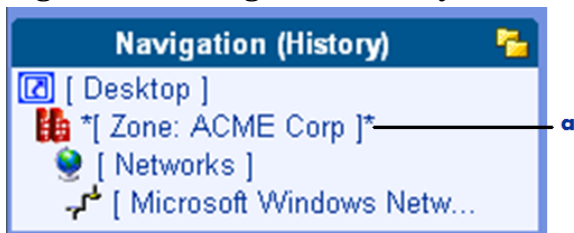
- **Navigation (History)** 
This is the default mode of navigation when you login to the Management Portal. To toggle to the Navigation (Location) mode, click .
The Navigation (History) aid provides a record of your navigation path. To quickly return to a previously visited location, just click any entry 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.

The figure that follows 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. This is used as an example only. Your screen may not look like this.


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


Figure 6 Navigation (History) records visited locations



Legend

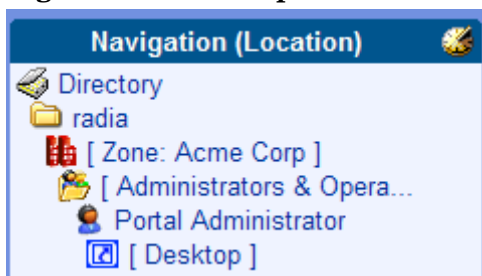
a *Current Location*

- **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 .

The next figure shows the Desktop location for a Portal Administrator when viewed in Navigation (Location) mode. The Desktop is under the current user's entry in the Zone Administrators & Operators container. This is used as an example only. Your screen may not look like this.

Figure 7 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 Management Portal Zone containers and viewing the objects automatically discovered in your networks.

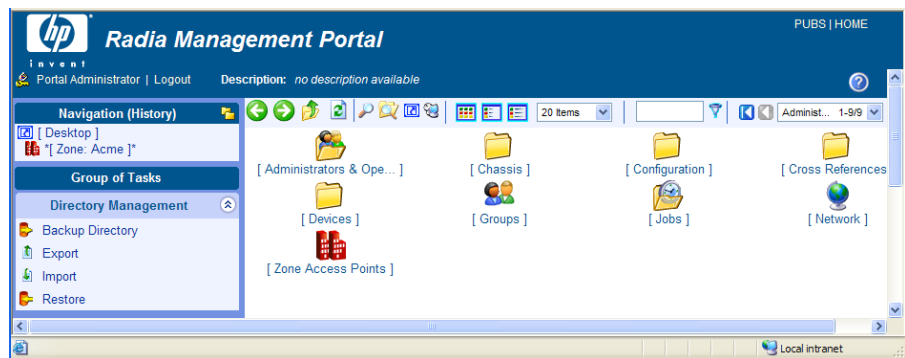
To access the Portal Directory and the Microsoft Windows Network

- 1 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 Management Portal Directory object appears in the workspace.

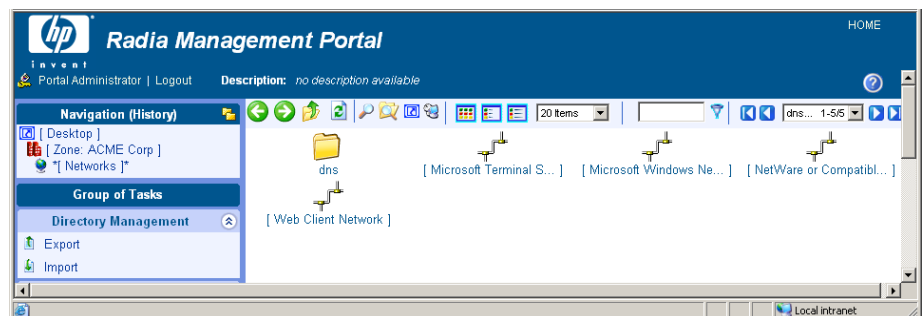
- 2 In the Workspace, click the **Zone** object.

The highest-level objects in the Zone appear in the workspace. See About the Zone Containers on page 88 for more information.






- 3 In the workspace, click the **Network** object.

Notice that the navigation aid now lists Desktop, your Zone object, 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 134.

- 4 In the workspace, click **Microsoft Windows Network**.
- 5 In large networks, use the filtering and paging options to locate objects by their common name:
 - For example, type ***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.

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



Legend

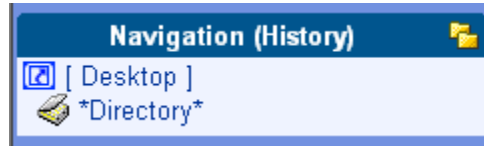
- a** Filter by name
- b** Browse or select a page
- 6** To return to the Desktop, click **[Desktop]** in the Navigation aid.

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:

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

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




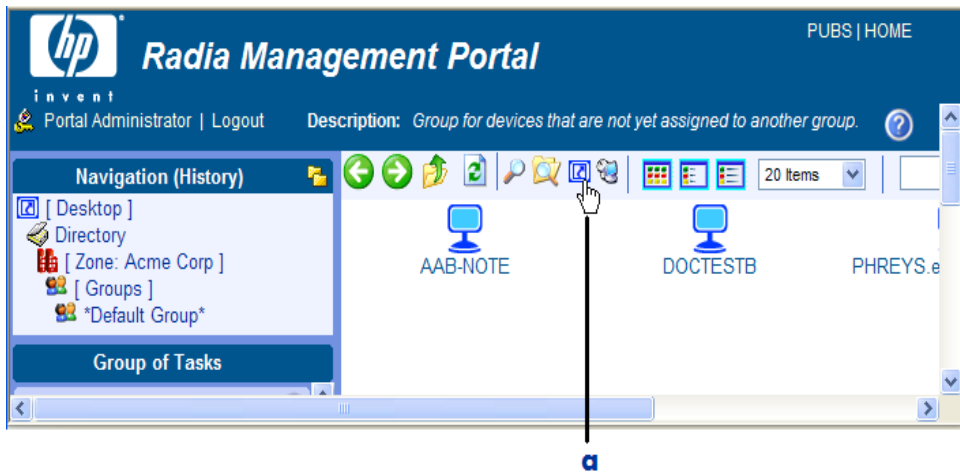
- 2 Click **Desktop** in the Navigation aid.

Adding Shortcuts to Your Desktop


This version of the 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


- 1 Start in Navigation (History) mode.
- 2 Navigate to the device or location for which you want to create a shortcut on the Desktop. For example, to create a shortcut to the **Default Group** of devices in a Zone, navigate to it from the Directory level by clicking the following entries in the Workspace area:
 - Zone
 - Groups
 - Default Group
- 3 After navigating to the location for which you want to create a shortcut, click the **Add Desktop Shortcut** icon  on the Toolbar.




Legend


- a Click  on the toolbar to add a desktop shortcut for current location.

The Add Shortcut to (selected location) window opens, requesting a confirmation.

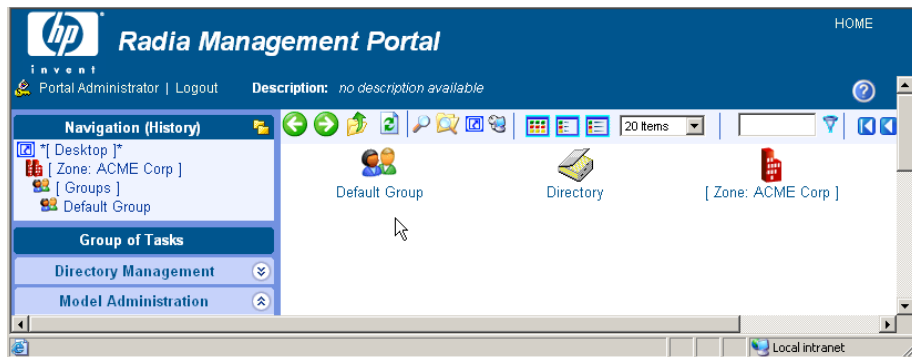
- 4 Click  to confirm that you want to add the shortcut.

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.



Removing Shortcuts from Your Desktop

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

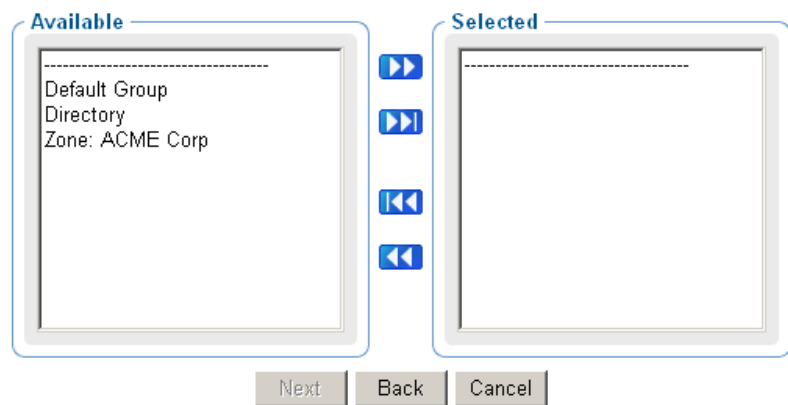
To remove shortcuts from the desktop

- 1 Return to your Desktop location. If you need help, see *Accessing and Returning to Your Desktop* on page 62.
- 2 In the Model Administration task group, click **Remove Shortcuts from Desktop**.

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

Remove Object

1 Select — 2 Summary



- 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.

Remove Object

1 Select – 2 Summary

Selected Audience

Default Group

Submit Back Cancel

- 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

- ▶ The term Authority Navigation Aid has been changed to Navigation Aid.

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

Below is an example of how to select an authority in the Management Portal. It includes step-by-step instructions on how to navigate to the Zone Devices container and the Zone Groups container of the Management Portal Directory.

To navigate the Zone Containers

- 1 Start in Navigation (History) mode.
- 2 Click the Desktop icon or label in the Navigation area.



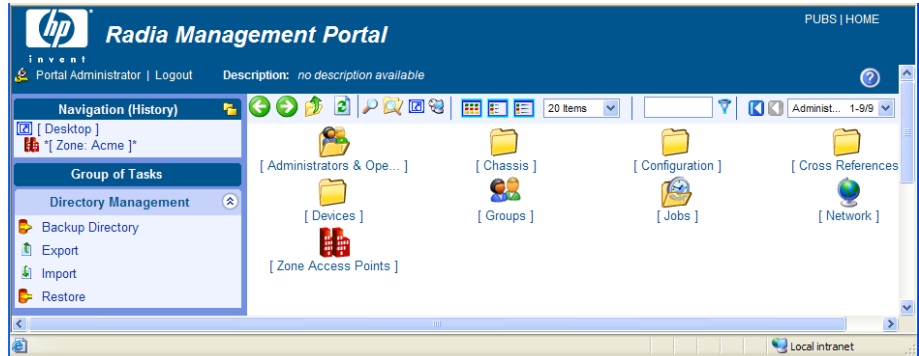
- ▶ In Navigation (History) mode, the Desktop is always the top entry.

Your current Desktop objects appear in the workspace to the right of the Navigation area.

- 3 In the workspace, click the Zone icon.



The Workspace displays the highest-level objects in the Zone Directory, as shown in the following figure.



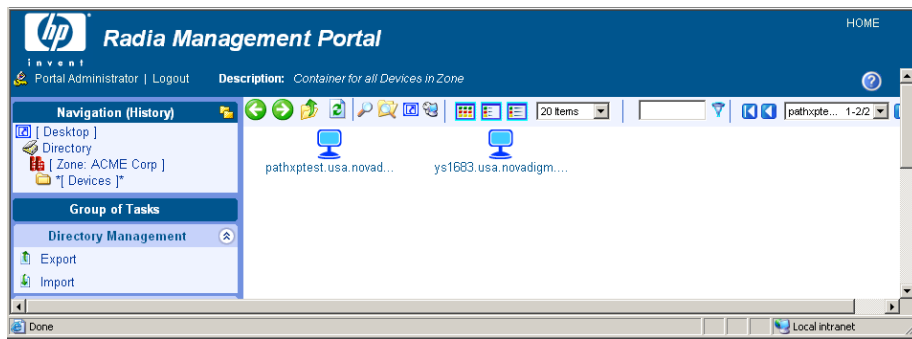
The Zone containers for Configuration, Cross References, Devices, Groups, and Zone Access Points were introduced with Management Portal version 2.0.

A Chassis container for the racks and enclosures of server blade devices was introduced to the Zone Directory as of version 2.1.

- 4 In the workspace, click the container named **Devices**.

The workspace displays up to one page of devices currently in the Devices container and being managed by the Management Portal Zone. The default page size is 20 items.

The figure below shows a sample Devices container with two devices under management.




Notice that the navigation aid now lists Desktop, Directory, Zone, and Devices, with only one with one entry, Devices, surrounded by asterisks. In Navigation (History) mode, the surrounding asterisks identify your *current location*, also known as your *selected authority*.

Each device being managed by this 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 159.

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

See *About the Zone Containers* on page 88 for detailed information on the Devices container and the other Zone containers.

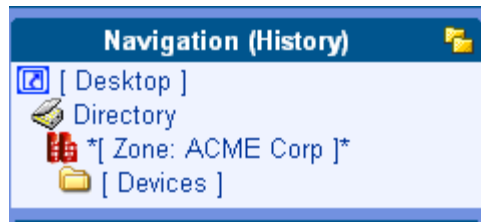
5 Now let's return to the Zone level containers. You can either:

- Click the toolbar icon  to go up one level in the Navigation path.
- or
- Click the [**Zone: name**] entry in the Navigation aid.

The workspace displays the Zone objects again.

The Navigation path continues to display your previously visited locations under the current location.

The following Navigation (History) example indicates the Devices container was visited, but the user is currently at the Zone level (as indicated by the surrounding asterisks).



- 6 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 Management Portal, only the Default Group object appears. If the Management Portal is not newly installed, you will also see any user-created groups in this container. The following example shows a Groups container that includes the Default Group entry as well as two user-created groups.



The Groups container is one of the most important containers in the 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 actually exist within the groups. The group memberships can be added or removed, at will.

See *Configuring the Zone Infrastructure* on page 175 for more information on how to create groups and add or import devices into the groups.

- 7 Click the **Default Group** object in the workspace, and then click the View Properties icon on the toolbar

The Group Properties page for the Default Group object opens.

Default Group Group Properties

Properties | Object Information

Properties

Create Time Stamp	2004/06/21 18:00
Is Critical System Object	true
Members	pathxptest.usa.nova.com ys1683.usa.nova.com sma_02
Modify Time Stamp	2004/06/28 18:59

[Back to top](#)

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

- 8 Click on a link in the Members area to go to the Device Properties page for that member. The following figure shows one example of a Device Properties page.


sma_02 Device Properties

Properties | Object Information

Properties

Create Time Stamp	2004/06/28 18:59
DNS Host Name	sma_02
Group Membership	Default Group cn=doc_dept_machines.cn=group.cn=acmecorp.cn=radia
Modify Time Stamp	2004/06/28 18:59

[Back to top](#)

-  If you switch from Navigation (History) to Navigation (Location) mode, you will see the Device Properties page is located within the Devices container.

Notice that the Device Properties page includes a Group Membership list. The sample Device shown in the previous figure lists two group memberships: one for the Default Group, and a user-created group named doc_dept_machines.

- 9 Click the **HOME** link in the top-right of the banner area to quickly return to your Desktop.
- 10 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
- Model Administration
- Operations
- Policy Management
- Policy (Advanced)
- RCS Administration

See [Toolbar Tasks](#) on page 82 for information about the tasks that can be initiated directly from icons in the Toolbar.






See [Configuring Task Groups](#) on page 213 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 Management Portal Directory. A sample set of tasks is shown below. The available tasks vary according to your navigation location.



•	Backup Directory  Click Backup Directory to backup the entire Management Portal Zone Directory. See Creating a Backup of the Portal Zone Directory on page 239 for more information.
•	Export  Click Export to export a subset of your Management Portal Zone Directory to an LDIF (LDAP Data Interchange Format) file. See Exporting Data from the Portal Directory on page 247 for more information.
•	Import  Click Import to import an LDIF (LDAP Data Interchange Format) file into your Management Portal Zone Directory. See Importing Data into the Portal Directory on page 249 for more information.
•	Restore  Click Restore to restore a backup of the entire Portal Zone Directory. See Restoring the Portal Directory on page 243 for more information.
•	Update Portal Tasks  Click Update Portal Tasks when you receive a new build of the Management Portal to update the tasks available to you. Available from the Zone, Configuration, Tasks container. See Updating Portal Tasks on page 253 for more information.

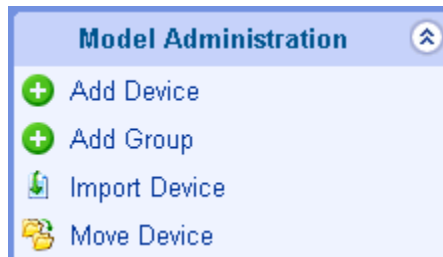
Infrastructure Task Group

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







2.2	Start Directory Service  Click Start Directory Service to connect to the Primary Database on the Configuration Server whose service is stopped, or start other directory service such as Active Directory. See Starting a Directory Service on page 150 for more information.
2.2	Stop Directory Service  Click Stop Directory Service to stop an external service, such as the Primary Database on the Configuration Server, or another directory service such as Active Directory. See Directory Service on page 152 for more information.






Model Administration Task Group







Use the Model Administration task group to manage the Management Portal Directory and a Zone. The available tasks vary according to your navigation location. The following figure shows a sample set of Model Administration tasks available from the Zone → Groups → Default Group location.



The following is a list of all potential Model Administration tasks available in the Management Portal.

•	<p>Add object-type </p> <p>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.</p> <p>As of version 2.1, you can also add objects types for racks, blade enclosures, enclosure configurations, and slots. See <i>Configuring Blades, Enclosures and Racks</i> for more information.</p>
2.0	<p>Add Device </p> <p>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 <i>Adding Devices to an RMP Zone</i> on page 159 for more information.</p>
2.0	<p>Add Directory Service </p> <p>Click the new Add Directory Service task to configure a connection between the Management Portal zone and another Directory Service, including the Configuration Server ZTOPTASK service. The task is available from the Zone → Configuration → Directory Service container. See <i>Adding a Directory Service</i> on page 135 for more information.</p>
2.0	<p>Add Group (of Devices) </p> <p>Click Add Group from the Devices container to create a new Group of Devices for organizing devices for operations. See <i>Adding Groups</i> on page 181 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 Device task.</p>
2.0	<p>Add Install Profile </p> <p>Click Add Install Profile to define a custom profile for selection during the Install Radia Client task. The Add Install Profile task is available from the following Navigation location: Zone → Configuration → Profiles → Radia Products → Client Installs. See <i>Adding, Modifying, and Deleting Install Profiles</i> on page 308 for more information.</p>
•	<p>Disable </p> <p>Click Disable to prevent a job or job group from being processed. See <i>Disabling Jobs or Job Groups</i> on page 262 for more information.</p>

•	<p>Enable </p> <p>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 262 for more information.</p>
2.0	<p>Import Device </p> <p>Click the Import Device 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 192 for more information.</p>
•	<p>Modify </p> <p>Click Modify to change an object. For example, you might want to change the areas of the Management Portal that an administrator can access, or change a job group's schedule. See Modifying Objects on page 198 or Modifying Job Groups on page 256 for more information.</p>
2.0	<p>Move Device </p> <p>Click the Move Device 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 Devices into a Group on page 186 for more information.</p>
•	<p>Query </p> <p>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 277 for more information.</p>
•	<p>Query Jobs </p> <p>Click Query Jobs to locate existing jobs, review their status, and make changes to them. See Querying Jobs or Job Groups on page 258 for more information.</p>
•	<p>Query User's Delegated Administration </p> <p>Click Query User's Delegated Administration to display information about a user's role. See Querying a User's Delegated Administration on page 228 for more information.</p>

•	<p>Remove </p> <p>Click Remove to remove an object and all of its children from the Management Portal Directory. See Removing Objects on page 199 or Removing Jobs or Job Groups on page 263 for more information.</p>
2.0	<p>Remove Shortcuts from Desktop </p> <p>Click Remove Shortcuts from Desktop to remove any previously added shortcuts from your Desktop location. See Removing Shortcuts from Your Desktop on page 64 for more information.</p>
•	<p>Restart Failed Jobs </p> <p>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 260 for more information.</p>
•	<p>Stop </p> <p>Click Stop to stop an active job group from running. See Stopping Job Groups on page 261.</p>
•	<p>View Properties </p> <p>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 264 for more information.</p>







Operations Task Group









Use the Operations task group to perform operations on your Radia infrastructure. A sample Operations task group listing is shown below.










The following describes all of the operations available in the Management Portal. Remember, the tasks available to you vary based on your selected

authority: therefore, the figure above above may not contain all of the tasks described here.

2.0	<p>Add Task Template </p> <p>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 Radia Proxy Server, as a saved Task Template. Task templates can be selected and applied during the ZoneJob task (which schedules Operations across multiple Zones at once). See Managing Task Templates on page 324 for more information.</p>
•	<p>Assign Proxy Server </p> <p>Use the Assign Proxy Server task to have a Proxy Server assist in the remote installation of Radia clients. Devices assigned to a Proxy Server will obtain their client installation scripts from that Proxy Server instead of from the Management Portal. See Assigning Proxy Servers on page 311 for more information.</p>
•	<p>Help Desk Notify </p> <p>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 286 for more information.</p>
•	<p>Install Management Agent </p> <p>Click Install Management Agent to install the Radia Management Agent on remote computers. See Installing the Radia Management Agent on page 295 for more information.</p>
2.0	<p>Install Management Portal </p> <p>Click Install Management Portal to remotely install another Management Portal Zone in your infrastructure. See Installing Additional Management Portal Zones (Subordinate Zones) on page 327 for more information. Also refer to the tasks: Update Management Portal, Open Subordinate Zone, and Schedule Zone Operation.</p>
•	<p>Install Proxy Server </p> <p>Click Install Proxy Server to install the Proxy Server on remote computers. See Installing the Proxy Server on page 315 for more information.</p>

	<ul style="list-style-type: none"> • Install Radia Client  Click Install Radia Client to install the Radia Client on remote computers. See Installing the Radia Client on page 302 for more information. Multiple Client Install Profiles are supported. For details, see Supporting Remote Installs Using Multiple Profiles on page 307.
	<ul style="list-style-type: none"> • Notify  Use the Notify tasks to perform an action on the selected audience. See Using the Notify Tasks on page 283 for more information.
2.0	<ul style="list-style-type: none"> • Open Subordinate Zone  Click Open Subordinate Zone to quickly access the Management Portal of another Zone in your enterprise from the Zone Access Points container. See Opening a Subordinate Zone on page 339 for more information.
	<ul style="list-style-type: none"> • Purge Proxy Server Dynamic Cache  Click Purge Proxy Server Dynamic Cache to purge the dynamic cache of one or more Radia Proxy Servers. See Purging the Dynamic Cache of the Proxy Server on page 322 for more information.
	<ul style="list-style-type: none"> • Restart  Click Restart to stop a service and then start it again. See Managing Services on page 323 for more information.
	<ul style="list-style-type: none"> • Resume  Click Resume to resume execution of a service that has been paused. See Managing Services on page 323 for more information.
2.2	<ul style="list-style-type: none"> • Schedule Zone Operation  Click Schedule Zone Operation from the Zone Access Points container to run a Notify or Install Proxy Server 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 334 for more information.
2.0	<ul style="list-style-type: none"> • Sequence Job  Use the Sequence Job task 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 341 for more information.







	<ul style="list-style-type: none"> • 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 345 for more information.
	<ul style="list-style-type: none"> • Start  Click Start to run a service. See Managing Services on page 323 for more information.
	<ul style="list-style-type: none"> • Start Viewer  Click Start Viewer to start a VNC session on a remote Radia client. See Using Remote Control on page 345 for more information.
	<ul style="list-style-type: none"> • Stop  Click Stop to stop a service. See Managing Services on page 323 for more information.
	<ul style="list-style-type: none"> • Synchronize Proxy Server  Click Synchronize Proxy Server to force the Proxy Server to connect to the Configuration Server to preload the files to the static cache on the Proxy Server. See Synchronizing the Proxy Server on page 320 for more information.
2.0.1	<ul style="list-style-type: none"> • Update Management Portal  Click Update Management Portal to remotely update the code delivered with a new build to the subordinate Management Portal Zones in your infrastructure. See Updating Subordinate Management Portal Zones on page 333 for more information.
2.2	<ul style="list-style-type: none"> • Zone Job  Click Zone Job from the Zone Access Points container to run a Notify or Install Proxy Server 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 334 for more information.

Policy Task Group

Use the Policy task group to assign policy using an LDAP Directory, such as Active Directory. Remember, the tasks listed will vary based on your selected authority. A sample Policy task group is illustrated below.



The following is a list of the available Policy tasks.





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 104 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 105 for more information.
2.0	Modify Policy Targets  Click Modify Policy Targets to specify members of a group to be targeted based on the policy assignments. See Modifying Policy Targets on page 107 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 105 for more information.
2.0	Refresh Managed Services Cache  Click Refresh Managed Services Cache to refresh the list of services displayed in the Management Portal. This list is created from information in the Radia Database. See Refreshing the Managed Services Cache on page 115 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 109 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.

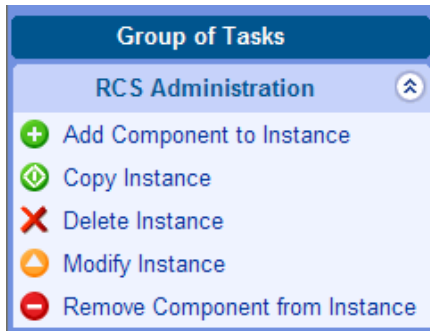
- ▶ Make sure that you have a good understanding of the Policy Server and the Radia Policy attributes before using these tasks.

The tasks available are:







2.0	Modify Policy Defaults  Click Modify Policy Defaults to set the defaults for the attributes in a service. Using this task modifies edmPolicyDefault. Refer to the <i>Policy Server Guide</i> for details. See Modifying Policy Defaults on page 119 for more information.
2.0	Modify Policy Dependencies  Click Modify Policy Dependencies to modify policy links. Using this task modifies the edmLink attribute. Refer to the <i>Policy Server Guide</i> for details. See Modifying Policy Dependencies on page 116 for more information.
2.0	Modify Policy Flags  Click Modify Policy Flags to limit the scope of policy resolution for specific objects. Using this task modifies the edmFlags attribute. Refer to the <i>Policy Server Guide</i> for details. See Modifying Policy Flags on page 118 for more information.
2.0	Modify Policy Overrides  Click Modify Policy 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. Refer to the <i>Policy Server Guide</i> for details. See Modifying Policy Overrides on page 121 for more information.

RCS Administration Task Group




Use the RCS Administration task group to manage instances in the Radia Database. Remember, the tasks listed will vary based on what you have selected in the navigation aid. A sample RCS Administration task group is shown below.



The following is a list of the RCS Administration tasks.

2.0	Add Component to Instance  Click Add Component to Instance to add a component connection to the selected instance. See Adding Components to Instances on page 96 for more information.
2.0	Copy Instance  Click Copy Instance to create a copy of the selected instance. See Copying Instances on page 98 for more information.
2.0	Create Instance  Click Create Instance to add a new instance to the current class. After adding the new instance, use the Modify Instance task to set the attributes, and the Add Component to Instance task to make connections for the instance. See Creating Instances on page 95 for more information.
2.0	Delete Instance  Click Delete Instance to remove the selected instance from the Radia Database. See Deleting Instances on page 99 for more information.
2.0	Modify Instance  Click Modify Instance 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 99 for more information.
2.0	Remove Component from Instance  Click Remove Component from Instance to remove a component connections from the selected instance. See Removing Components from Instances on page 100 for more information.

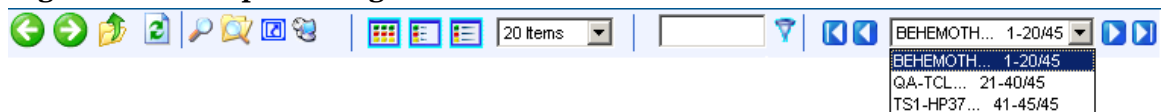
Toolbar Tasks

2.0	Add Shortcut to Desktop  Click Add Shortcut to Desktop to add a shortcut icon to the Desktop location within the 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 62 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 286 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 264 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 8 Sample Management Portal Toolbar







Some figures throughout this book show an earlier version of the toolbar. Disregard any earlier toolbar images and refer to this topic for toolbar usage information.

Navigation Icons


- Click  to go back one page.
- Click  to go forward one page.
- Click  to go up one level in the Management Portal Directory.
- Click  to refresh the information displayed in the workspace.

Task Icons

See Toolbar Tasks on page 82 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  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  to show the potential targets with large icons.
- Click  to show the potential targets in a list view (small icons).
- Click  to show the potential targets in a detailed view.

Paging and Filtering Icons

About LDAP Paging

For increased performance, the Management Portal immediately displays only the first 20 objects in any LDAP directory. To collect and view the rest of the objects:

- **Reset the items per page size.** Page sizes range from 20 to 1000 items. The Management Portal immediately retrieves up to one page of items using the revised page size.
- **Page forward**, if necessary, until all objects have been collected and displayed.
- When there are no more objects to collect, the **next page button turns gray and is disabled.**

The following image shows an example of using the paging icons to display all Management Portal Tasks on a single page. In this example, the page size was reset to 400, resulting in all 126 tasks being shown on a single page. The disabled next page button indicates there are no additional tasks to display.



To obtain an item count of LDAP objects

- 1 Reset the items per page to a very large number, such as 500 or 1000.
If the next page icon is gray, you have reached the end of the objects and the total items retrieved indicates the total item count.
- 2 If necessary, page forward until the next page icon turns gray.

When the next page icon is gray, the last page indicates the total item count.


- ▶ Once you have collected all LDAP items for a group, use the filter feature or a smaller page size to find specific items in the group.

Paging and Filter Icon Details


- Use the drop-down list box to reset the maximum number of items to retrieve for a single page:



Page sizes range from 20 (the minimum and initial value) to 1000.


- For increased performance, objects in LDAP directories are retrieved one page at a time. Click  to retrieve and go to the next page of objects.

- ▶ LDAP-paging applies to Management Portal Zone directories as well as external LDAP directories, such as an Active Directory.

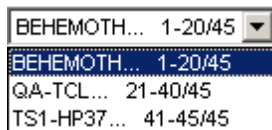
- In the filter text box, type a filter value and click  to filter the retrieved objects according to their display names, common names, and cn= values.







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 .
- Use the drop-down list box or the arrows to page through multiple pages of collected objects.

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



- Click  to go to the first page of collected objects. If only one page has been collected, this redisplay the current page.

- Click  to go to the previous page of collected objects.
- Click  to collect and display the next page of objects, or page forward to a previously-retrieved page of objects.
 - ▶ When the next page icon turns gray, all objects have been collected and counted. The final number of any page selection [for example: QA-TCL... 21-40/45] gives a total object count.
- Click  to go to the last page of retrieved objects. If only one page has been collected, this redisplay the current page.
- 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 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 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 Management Portal at this location. Other 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 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 Configuration Server, whose Common Name has been assigned cn=primary. Use the RCS Administration Tasks from the Management Portal to perform instance-level tasks on the Radia Database. To configure the Primary file, see Adding a Directory Service on page 135.
- **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 88. 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 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 Configuration Server.

A computer is a physical device that exists in your infrastructure. If you want it managed by this 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** 

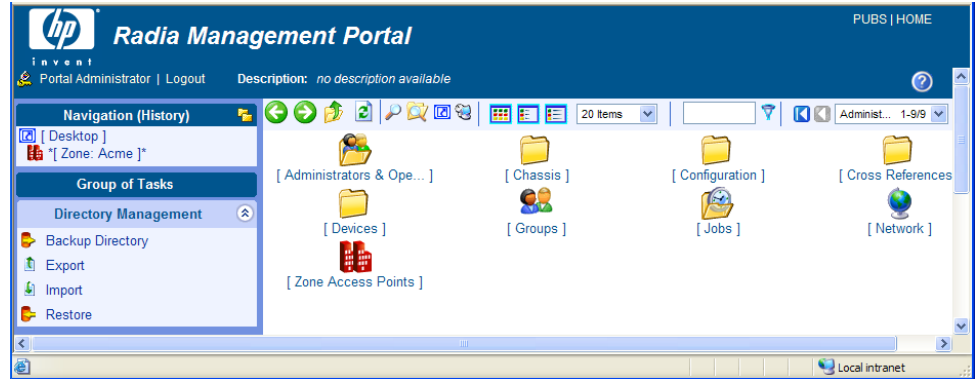
A network, such as Microsoft Windows Network, represents an external network directory that has been discovered by the Management Portal. Objects in a network can be selected for management by this Management Portal Zone.
- **Directory Service** 

External Services are defined to the Management Portal Zone to enable a connection to that service from within the Management Portal. An Active Directory, the Radia Database on the 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 Configuration Server or Proxy Server.

About the Zone Containers

This topic defines the 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.





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 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 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.
- Perform modeling and policy-based management of server blade devices in a Zone using the knowledge of their blade enclosures, racks, and enclosure configurations.

- **Administrators and Operators Container (cn=USER)**

The Administrators and Operators Container is the default, built-in source for authenticating users of the 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 Management Portal, Accounts, Infrastructure, the Network, Packages, Policy, Services, and the Configuration Server.

- **Chassis Container (cn=chassis)**

The Chassis container is used to manage and apply policy to the blade servers in a Zone using the (physical) enclosures and racks in which they are mounted, as well as their (logical) enclosure configurations. It contains three groups:

- Blade Enclosure Configurations
- Blade Enclosures
- Racks with Enclosures

- **Configuration Container (cn=config)**

The Configuration container holds the start-up configuration of the 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
- 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 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. Most 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 Management Portal for all devices under a zone's management:
 - **Device Manufacturers** – For example, Hewlett-Packard, Dell, and Gateway device groups.
 - **Device Architecture** – For example, HP Itanium, HP PA-RISC, and SUN Architecture.
 - **Enclosure Manufacturers** – For example, Hewlett-Packard and IBM are groups listed under the enclosure manufacturers for server blades.
 - **Infrastructure Services** – For example, Proxy Server, Radia Management Agent, and 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.

▶ The Managed Services groups are created and maintained using objects collected at the end of a client-connect session with a Configuration Server, and routed from a Messaging Server to the Management Portal Zone. For more information, see Posting Client Objects to the Management Portal on page 45.

- **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:



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

▶ As of RMP v2.1, subnet addresses for devices use the format `nnn.nnn.nnn.nnn`. Previously, they used the format `nnn_nnn_nnn_nnn`.

- **Devices Container (cn=device) Self Managed**

The Devices container holds the object properties for all devices being managed by this 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 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 Management Portal. Within the Jobs Container is the History container, holding daily records of completed jobs.
- **Network 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 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 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, the figure below shows the descriptions available for the objects at the Zone level of the Directory.

Figure 9 Details View includes descriptions

Display Name	Description	Modify Time Stamp
 [Administrators & Operators]	Default (builtin) source for authenticating users. (WHO)	2005/12/15 12:10
 [Chassis]	Container for Racks and Enclosures of Blade Devices	2005/12/15 12:10
 [Configuration]	Container for config objects	2005/12/15 12:10
 [Cross References]	Container for Cross Reference objects in Zone	2005/12/15 12:10
 [Devices]	Container for all Devices in Zone	2005/12/15 12:10
 [Groups]	Container for groups of managed computers.	2005/12/15 12:10

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

- To configure your Management Portal Zone and bring devices under management, go to Chapter 4: Administrative Functions.
- To perform operations on devices in your 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 below.
- To perform Policy using an LDAP directory, see Using RMP to Assign Policy through an LDAP Directory on page 102.

Using the RCS Administration Tasks

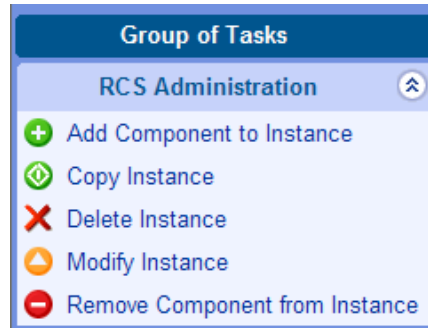
The Management Portal contains several tasks, stored in the RCS Administration task group, that allow you to manipulate instances in the Radia Database.

Prerequisites

- The Configuration Server service must be started on the machine where you want to make changes.
- A Configuration Server directory service must be defined and the RMP must be connected to that directory service. For details, see the following topics in Adding a Directory Service on page 135 and Starting a Directory Service on page 150.

About the RCS Administration Tasks

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



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 Component to Instance**
Click **Add Component to Instance** to add connection(s) to the selected instance.
- **Create Instance**
Click **Create Instance** to add a new instance to the current class. After adding the new instance, use the Modify Instance and Add Component to Instance tasks to set the attributes and make connections for the instance.
- **Copy Instance**
Click **Copy Instance** to create a copy of the selected instance.
- **Delete Instance**
Click **Delete Instance** to remove the selected instance from the Radia Database.
- **Modify Instance**
Click **Modify Instance** 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 Component from Instance**
Click **Remove Component from Instance** to remove connection(s) from the selected instance.

Creating Instances

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

To add an instance

- 1 Use the navigation aid and workspace to go to the class where you want to add a new instance. For example, go to the Accounts class in the Policy domain.
- 2 In the RCS Administration task group, click **Create Instance**.

The Create window opens.



Create

** Required fields*

New Accounts

Instance*	<input type="text"/>
Friendly name*	<input type="text"/>

- 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 **Create**.

The Properties window for the new instance opens.

Susan Fields User Properties

Basic | [Advanced](#)

[Properties](#) | [Connections](#)

Properties

Friendly name	Susan Fields
Created	2006/01/05 16:16
Last Modified	2006/01/05 16:16

[Back to top](#)

Connections

-  Susan Fields
 -  Application
 -  [Maint_40](#)
 -  Software Services
 -  [StratusPad](#)
 -  [Sales Information](#)
 -  [Redbox Organizer](#)
 -  Workgroups
 -  [\[Default\]](#)

[Back to top](#)

Adding Components to Instances

Use the Add Component to Instance task to add component connections to the selected instance.

To add a component to an instance

- 1 Use the navigation aid and workspace to go to the instance for which you want to create a connection.
- 2 In the RCS Administration task group, click **Add Component to Instance**.

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

Add Connections to 100_MGR

1 Select — 2 Add — 3 Summary

Type

- 3 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.

Add Connections to 100_MGR

1 Select — 2 Add — 3 Summary

Selection

Type: Services

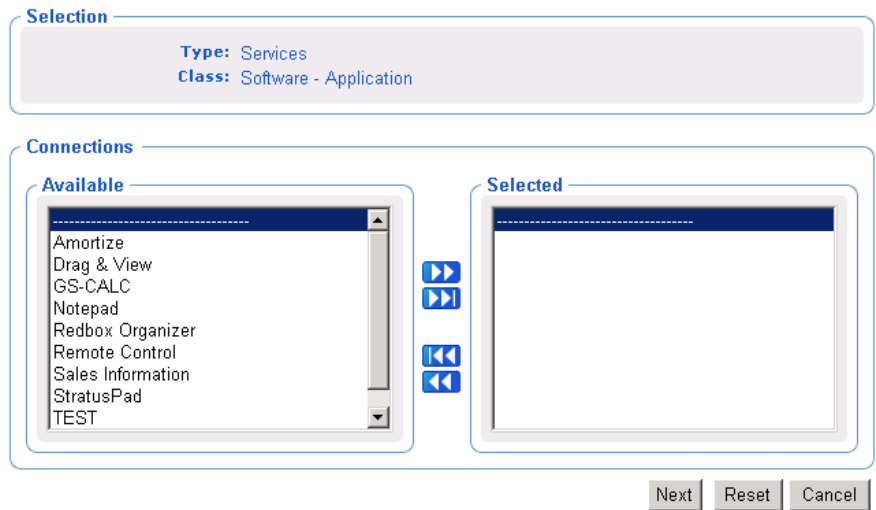
Class

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

The Connections area opens.

Add Connections to 100_MGR

1 Select — 2 **Add** — 3 Summary



Selection

Type: Services
Class: Software - Application


Connections

Available

- Amortize
- Drag & View
- GS-CALC
- Notepad
- Redbox Organizer
- Remote Control
- Sales Information
- StratusPad
- TEST

Selected

Next Reset Cancel

- 5 From the Available list, select one or more instances.
- 6 Click  to add the selected instances to the Selected list.
- 7 Click **Next**.

The Add Connections - Summary window opens.

- 8 Click **Commit**.
- The Properties window opens and displays the new connections.

Copying Instances

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

To copy an instance

- 1 Use the navigation aid and workspace to go to the instance that you want to copy.
- 2 In the RCS Administration task group, click **Copy Instance**.

The Copy window opens.

Copy 100_MGR



100_MGR

Instance

Friendly name



Copy Cancel

- 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 Instance task to remove the selected instance from the Radia Database.

To delete an instance

- 1 Use the navigation aid and workspace to go to the instance that you want to delete.
- 2 In the RCS Administration task group, click **Delete Instance**.
The Delete window opens, asking you to confirm the delete.
- 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 Instance task to modify the selected instance.

To modify an instance

- 1 Use the navigation aid and workspace to go to the instance that you want to modify.
- 2 In the RCS Administration task group, click **Modify Instance**.
The Modify window opens.

Modify Amortize

Basic | Advanced

Properties | Behavior Properties | Method Properties

* Default Values

Service Properties

Friendly name	Amortize
Service Name/Description	Amortize
Catalog Group Name	Demo Applications
Mandatory or Optional Service *	<input type="radio"/>
Local Repair *	<input type="checkbox"/>
Service Create Ordering *	<input type="checkbox"/>
Events to Report *	A=B,AD=B,AU=F,AR=N,VA=F,VD=F
Install/Update/Delete/Version Chang *	
Vendor Name	Parnes
WEB URL Name	http://www.novadigm.com
Author Name *	
Version Description	1.0

3 Make any necessary changes.

4 Click **Modify**.

The Properties window opens.

Removing Components from Instances

Use the Remove Component from Instance task to remove component connections from the selected instance.

To remove a connection

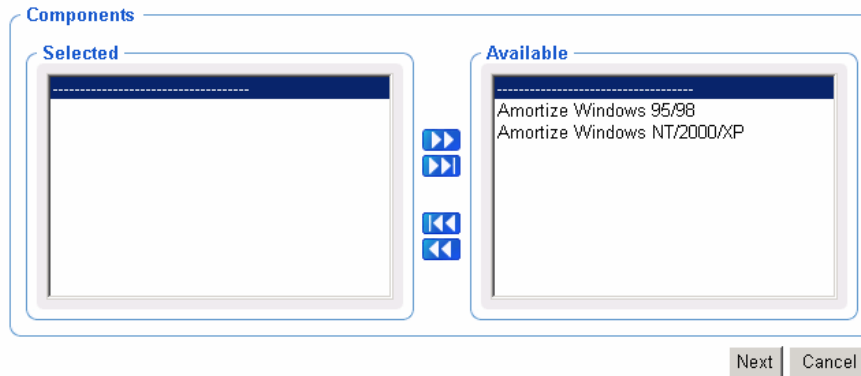
- 1 Use the navigation aid and workspace to go to the instance for which you want to remove a connection.
- 2 In the RCS Administration task group, click **Remove Component from Instance**.


The Remove Connections window opens.

⑤ Remove Connections from Amortize

Basic | Advanced

1 Remove — 2 Summary



- 3 From the Available list, select one or more instances.
- 4 Click  to move the instances to the Selected list.
- 5 Click **Next**.
The Summary window opens.
- 6 Click **Commit**.
The Properties window opens and the connections are removed.

Using RMP to Assign Policy through an LDAP Directory

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

Prerequisites

- A comprehensive understanding of the Policy Server and assigning policy.
- A connection to the *primary* Configuration Server service so you can access services.



The *primary* 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 143 for more information.

- A connection to the LDAP Directory service. See *Starting a Directory Service* on page 150 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 148.
- If you defined an LDAP Policy Extension with a prefix other than *edm* through the Policy Server, you must also define the custom policy prefix to the 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 156 for more information.



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. Refer to 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. A sample Policy task group is shown below. Remember, the available tasks vary based on your selected authority.



The following is a list of the available Policy tasks.

- **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 Policy Targets**
Click **Modify Policy 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 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 (DNNAME). 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 and workspace to go to the appropriate container in the directory service where you want to add a policy object.

For example, the following image shows a sample navigation path taken to go to a container named [Test] that exists in a directory service named [eng.test.com]. A policy object will be added to the [Test] container.



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

The Add Policy Object window opens.



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

The Add Group window opens.

Add Group

Properties

Common Name	<input type="text" value="MyGroup"/>
Display Name	<input type="text"/>
Description	<input type="text"/>



- 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.
- 7 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 and workspace 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, asking you to confirm the object removal.
- 3 Click  to confirm that you want to remove the object.
or
Click  to indicate that you do not want to remove the object.

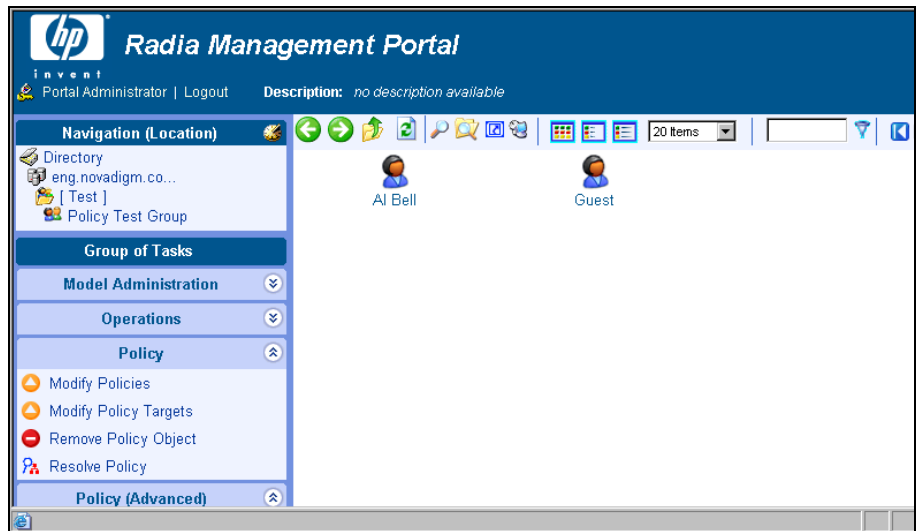
Modifying Policies

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

To modify policies

- 1 Use the navigation aid and workspace to go to the policy object that you want to modify.
- 2 Optionally, click  to the right of any task group's title to minimize the task list.

For example, the following figure shows a sample starting location to modify a policy object (your location will vary), and shows the Model Administration and Operations task groups have been minimized.



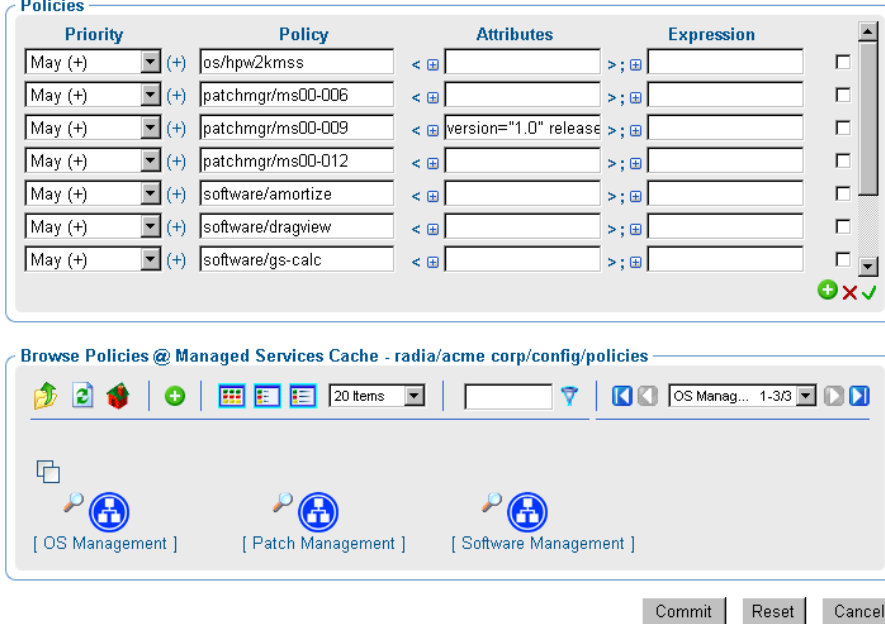
- 3 In the Policy task group, click **Modify Policies**.



If necessary use the Group of Tasks scroll bar to navigate to the Policy task group.

The Modify Policy window opens.

Modify Policy



The image shows two screenshots from a management portal. The top screenshot is titled 'Policies' and displays a table with columns for Priority, Policy, Attributes, and Expression. The bottom screenshot is titled 'Browse Policies @ Managed Services Cache - radia/acme corp/config/policies' and shows a navigation pane with icons for OS Management, Patch Management, and Software Management, along with a toolbar and buttons for Commit, Reset, and Cancel.

Priority	Policy	Attributes	Expression
May (+)	os/hpw2kmss		
May (+)	patchmgr/ms00-006		
May (+)	patchmgr/ms00-009	version="1.0" release	
May (+)	patchmgr/ms00-012		
May (+)	software/amortize		
May (+)	software/dragview		
May (+)	software/gc-calc		

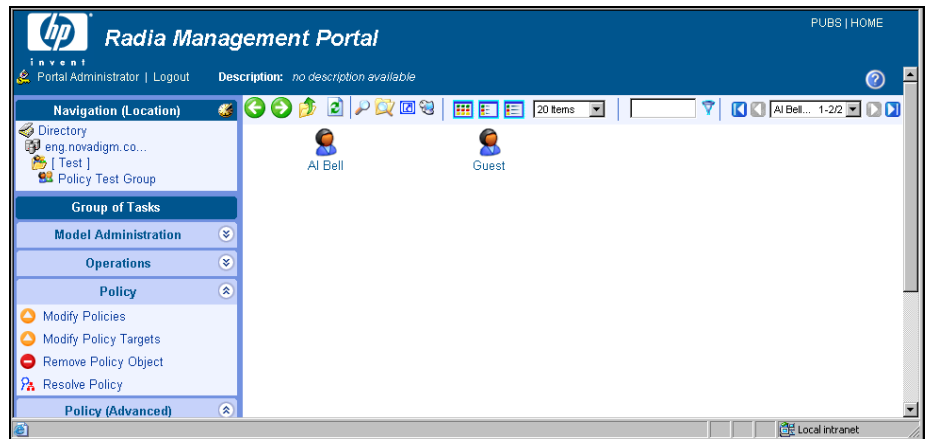
- 4 Use the Modify Policies window to modify existing policy or to select additional services to be assigned to the policy object. See Basic Procedures for Modifying Groups on page 161 for information on how to use this window. Within that section, see Using the Attribute Editor on page 166 for information on how to modify service attributes, and see Using the Expression Editor on page 169 for information on how to modify the constraints for a service using the expressions editor.
- 5 When you are done making changes, click **Commit**.

Modifying Policy Targets

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

To modify policy targets

- 1 Use the navigation aid and workspace to go to the appropriate policy object. The location shown in the following figure is an example; your starting location will vary.



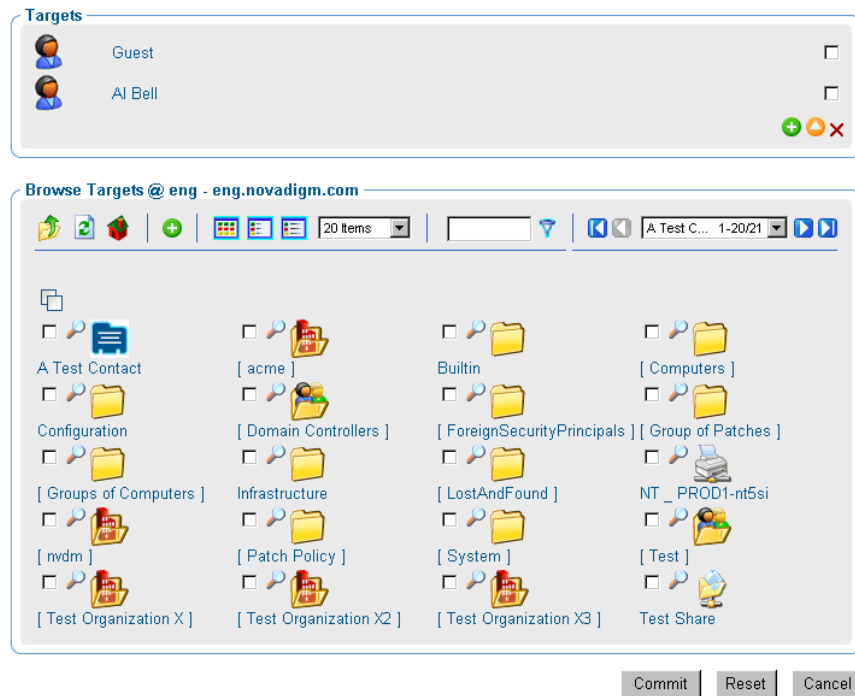
- 2 In the Policy task group, click **Modify Policy Targets**.



If necessary use the Group of Tasks scroll bar to navigate to the Policy task group.

The Modify Policy Targets window opens.

Modify Policy Targets



- 3 Use the Modify Policy Targets window to select the appropriate targets. See Basic Procedures for Modifying Groups on page 161 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.



If you customized the set of domain filters (DNAMES) in the Policy Server configuration file (`pm.cfg`), you can also customize the domain filters available in the Resolve Policy task of the Management Portal. See *Customizing Domain Filters (DNAMES) in the Resolve Policy Task* on page 114 for details.

To resolve policy entitlements

- 1 Use the navigation aid and workspace to go to the appropriate policy object. For example, go to a specific user object in your policy directory.



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



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

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 sources of indirect entitlements are listed on the left column. The figure below shows the direct policies for Patch Management, followed by the indirect policies inherited for three groups. The policies for the second and third groups have been hidden from view.




- 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.



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 114 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 below Zcontext 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.

The screenshot shows a web form titled "Attributes". It contains a dropdown menu for "Dname" with "PATCH" selected. Below this are five text input fields labeled "Host", "Os", "Uid", and "Zcontext". At the bottom of the form, there are two more empty text boxes for adding a new attribute. Below the form are two buttons: "Resolve Policy" and "Cancel Resolve Policy Task".

- 5 After specifying Attributes for the policy resolution, click **Resolve Policy** 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.

Resultant Policies

OS Management

- Policy Test Group OS.BEHAVIOR.X_X
- OS.ZSERVICE.HPW2KMSS

Attributes

Dname	<input type="text" value="OS"/>
Host	<input type="text"/>
Os	<input type="text" value="Win98"/>
Uid	<input type="text"/>
Zcontext	<input type="text"/>

Resolve Policy
Cancel Resolve Policy Task

- 6 To exit the Resolve Policy page, click an entry in the top-left Navigation area of the Portal. 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 Policy Server `pm.cfg` file, you can port your modified filter settings to the 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 Policy Server. Any custom filter settings must be properly defined in the Radia Policy Server configuration file, `pm.cfg` using the format:

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



Refer to Appendix C, Domain Filtering in the *Policy Server Guide* for details on domain filtering and syntax.

To port your custom domain filter settings to the Management Portal Resolve Policy task you must modify the `httpd.rc` file, which is located in the `etc` directory of where the 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. The Code sample below displays 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 }
}
```

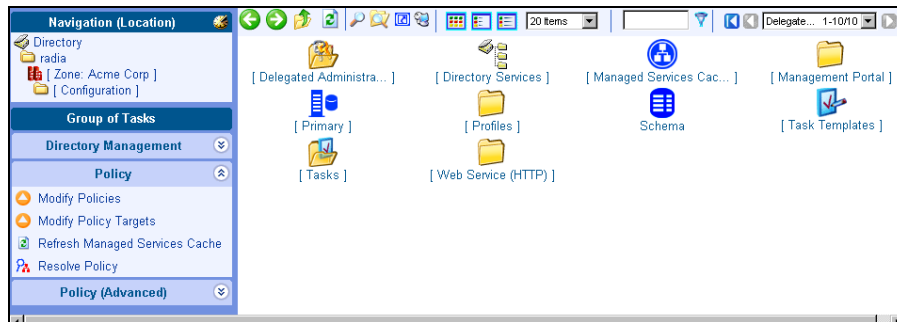
Save the changes to the `httpd.rc` file and restart the Management Portal service. The modified filter settings will be available from the Dname drop-down list box on the Resolve Policy task.

Refreshing the Managed Services Cache

Use the Refresh Managed Services Cache task to periodically refresh the list of services displayed in the Management Portal. This list is created from information in the Radia Database that is connected to the Portal using a Directory Service type of `ds-rcs`.

To refresh the managed services cache

- 1 Use the navigation aid and workspace to go to the Zone Configuration container.



- 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.

- ▶ 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 Policy Defaults**
Click **Modify Policy Defaults** to set the defaults for the attributes in a service. Using this task modifies edmPolicyDefault. Refer to the *Policy Server Guide* for details.
- **Modify Policy Dependencies**
Click **Modify Policy Dependencies** to modify policy links. Using this task modifies the edmLink attribute. Refer to the *Policy Server Guide* for details.
- **Modify Policy Flags**
Click **Modify Policy Flags** to limit the scope of policy resolution for specific objects. Using this task modifies the edmFlags attribute. Refer to the *Policy Server Guide* for details.
- **Modify Policy Overrides**
Click **Modify Policy 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. Refer to the *Policy Server Guide* for details.

Modifying Policy Dependencies

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

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

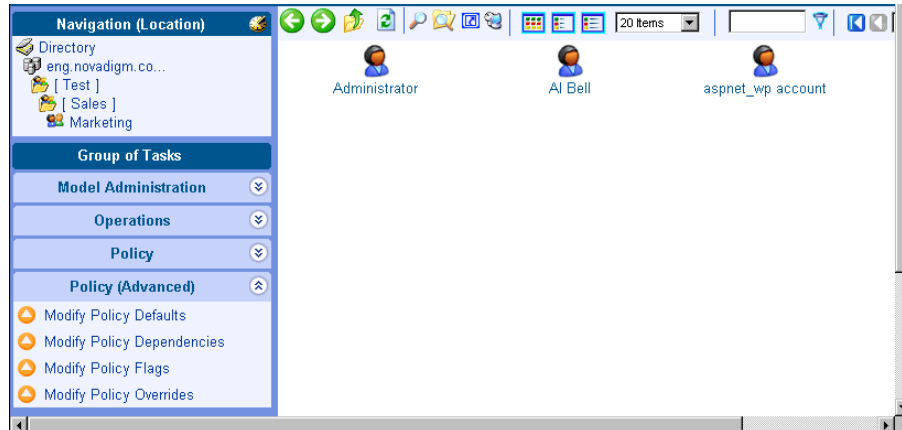
Example

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

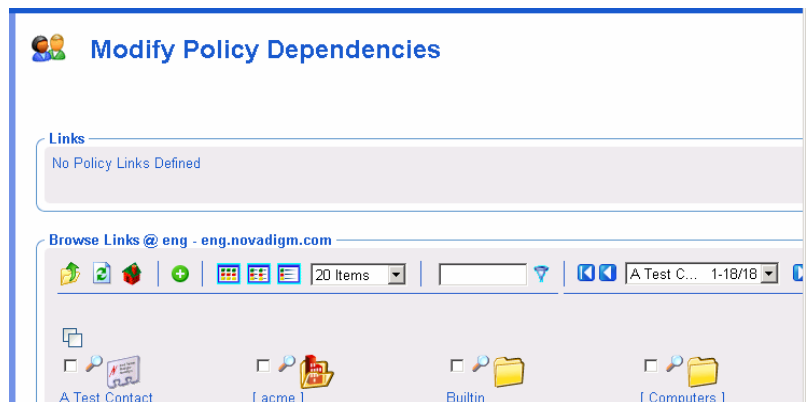
receive several services that are specifically for HP Compaq Notebook nc6000 machines. The following example shows how to create a dependency (also called a link) from the Marketing group to the HP Compaq Notebook nc6000 group.

To modify a policy dependency

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

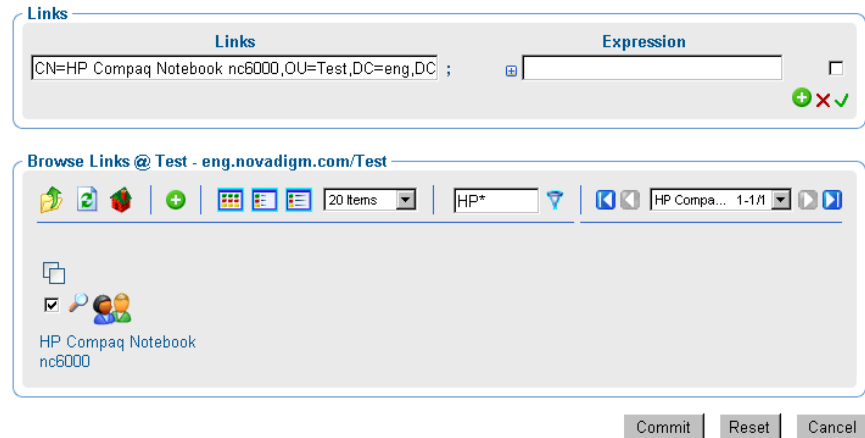


- 2 In the Policy (Advanced) task group, click **Modify Policy Dependencies**. The Modify Policy Dependencies window opens.



- 3 Use this window to select the policy link. See Basic Procedures for Modifying Groups on page 161 for information about how to use this window.

Modify Policy Dependencies



The screenshot shows the 'Modify Policy Dependencies' interface. It features a 'Links' section with a text input field containing the LDAP entry 'CN=HP Compaq Notebook nc6000,OU=Test,DC=eng,DC;' and an adjacent 'Expression' field. Below the 'Links' section is a browser window titled 'Browse Links @ Test - eng.novadigm.com/Test'. The browser window shows a search for 'HP*' and a result for 'HP Compaq Notebook nc6000'. At the bottom of the interface are three buttons: 'Commit', 'Reset', and 'Cancel'.

- 4 If you want to add any additional constraints use the Expression Editor. See Using the Expression Editor on page 169 for more information about how to use this window and the *Policy Server Guide* for more information about expressions.
- 5 Click **Commit** to save the changes to the policy dependencies.

Modifying Policy Flags

Use the Modify Policy Flags task to limit the scope of policy resolution for specific objects. Using this task modifies the edmFlags attribute. Refer to 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 policy flags


- 1 Use the navigation aid and workspace to go to the policy object for which you want to limit the scope of policy resolution.
- 2 In the Policy (Advanced) task group, click **Modify Policy Flags**.

The Modify Policy Flags window opens, showing the current status of the policy flags for the selected object:

- A check mark indicates that flag has been set for the policy object.
- An empty check box indicates that flag has not been set for the policy object.

Modify Policy Flags



- 3 Select the appropriate check box to set a flag, or to remove a previous flag setting.
 - **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.
- 4 Click  to accept the changes.
- 5 Click **Commit**.

Modifying Policy Defaults

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

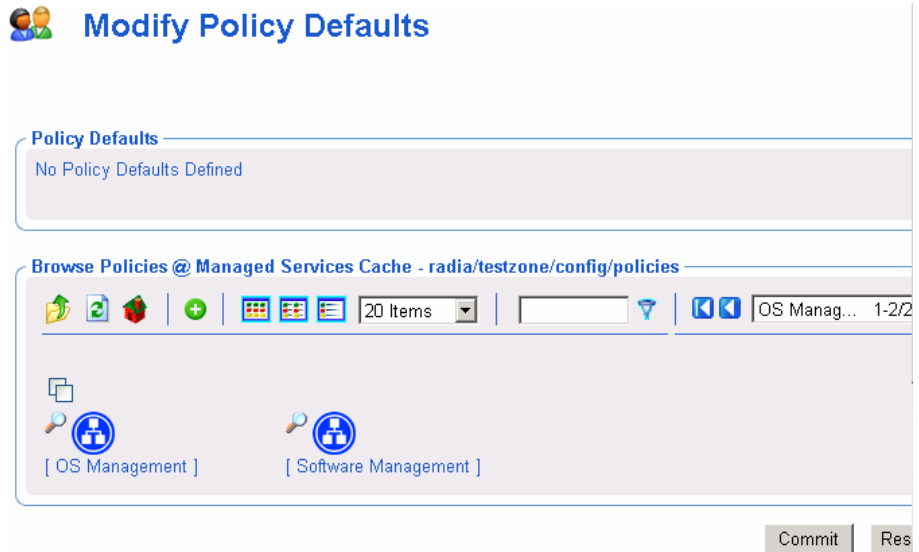
Example

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 policy defaults

- 1 Use the navigation aid and workspace to go to the appropriate policy object.
- 2 In the Policy (Advanced) task group, click **Modify Policy Defaults**.

The Modify Policy Defaults window opens.



- 3 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.
- 4 Once you have selected a service, use the Attribute Editor to specify the default values. See Using the Attribute Editor on page 166 for information about how to use this editor and the *Policy Server Guide* for details about attributes.
- 5 Use the Expression Editor to specify any additional constraints. See Using the Expression Editor on page 169 for information about how to use this editor and the *Policy Server Guide* for details about expressions.

Modifying Policy Overrides

Use the Modify Policy 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

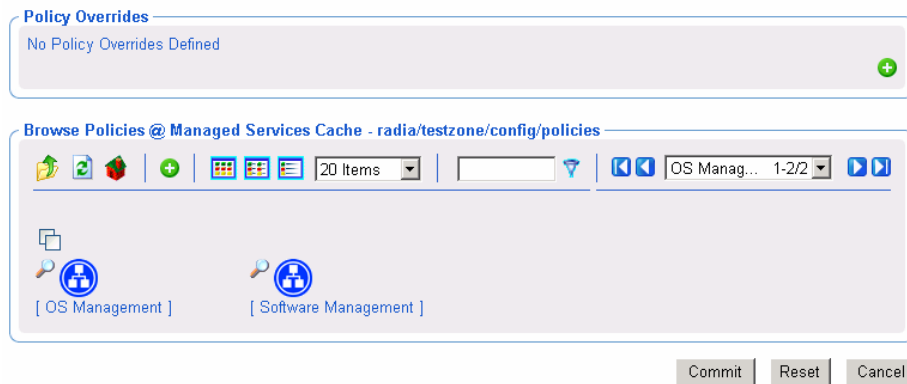
Bob Smith is entitled to the Sales application, version 1. You can use this task to override the version information for Bob alone, and entitle him to version 2.

To modify policy overrides

- 1 Use the navigation aid and workspace to go to the appropriate policy object.
- 2 In the Policy (Advanced) task group, click **Modify Policy Overrides**.

The Modify Policy Overrides window opens.

Modify Policy Overrides



- 3 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.
- 4 Once you have selected a service, use the Attribute Editor to specify the override values. See Using the Attribute Editor on page 166 for information about how to use this editor and the *Policy Server Guide* for details about attributes.

- 5 Use the Expression Editor to specify any additional constraints. See Using the Expression Editor on page 169 for information about how to use this editor and the *Policy Server Guide* for details about expressions.

Summary

- The Management Portal has a consistent user interface, which means that you can follow the same basic procedure to complete any task.
- The 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 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 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 Management Portal contains several tasks, stored in the RCS Administration task group, that allow you to manipulate instances in the Radia Database.
- The 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 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 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 Management Portal Directory.
- Be able to manage the 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 Management Portal.

Several administrative functions are available for configuring and managing your organization's infrastructure from the Management Portal. Administrative functions allow you to prepare your 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 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 134.

Also new for this release are the containers and tasks used to bring devices under management by the Management Portal Zone. For details, see *Establishing Devices and Device Groups* on page 159.

Configuring a 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 Management Portal to be able to connect, such as the Primary file on your Configuration Server or an existing LDAP Directory in your enterprise.
- **Network Discovery and Mount Points**
The 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 Management Portal Zone can be further clustered into different Groups to expedite common operations.
- **Subordinate Zones**
From the initial 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,

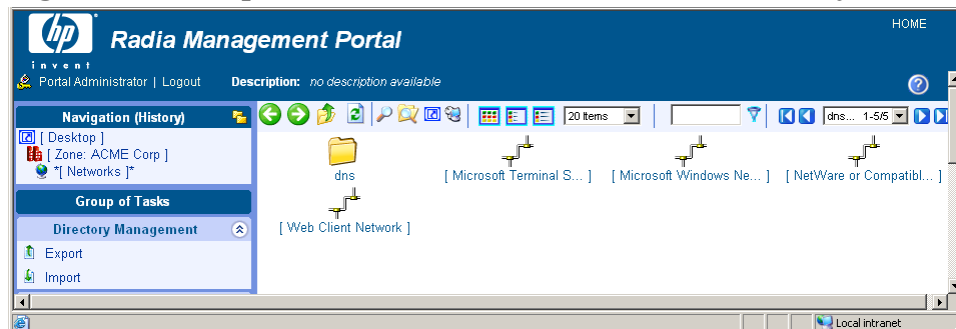
which can be used to schedule Zone Operations on devices in all zones in your enterprise.

- **Task Templates**
Task templates need to be added before scheduling jobs for Zone Operations.
- **Cross References Container**
The groups in the Cross References 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

If enabled during the install, the Management Portal runs the network discovery job 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 →Networks location, where they can be selected for management by the Management Portal Zone.

Figure 10 Sample Network containers with discovered objects



► The Network Discovery feature is not supported on a Windows NT 4.0 platform.

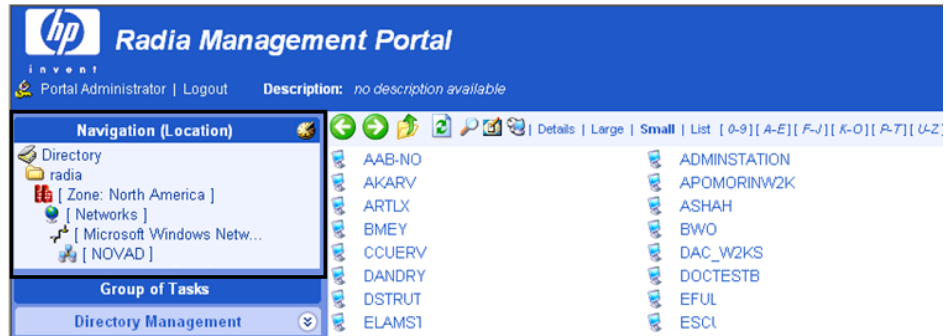
To view the objects discovered in a specific network, navigate to the Zone →Networks container and then click the specific network object in the Workspace. For example:

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

- Click **Network or Compatible Networks (cn=nrnw)** to view Network devices that you can manage.

Figure 11 below shows the objects discovered in a sample Microsoft Windows Network domain.

Figure 11 Sample Microsoft Windows Network domain



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

- 1 Stop the Radia Integration Server service.
- 2 Use a text editor to open the 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 (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
#

```

- 3 You can insert any of the parameters in Table 2 below into this file before the finishing curly bracket () as shown in the code sample above.
- 4 Use a space to separate the parameter and its value.

Table 2 Parameters to Configure Network Discovery

Parameters	Explanation
NETSCAN	<p>Enables or disables network discovery. Default is disabled. During the install the user can set this value to enabled or disabled.</p> <ul style="list-style-type: none"> • Type NETSCAN 0 to disable network discovery. • Type NETSCAN 1 to enable network discovery.

Parameters	Explanation
NETSCAN_START_DELAY	<p>The time to wait (in seconds) before starting network discovery when the Management Portal starts up. Default is 15 minutes or 900 seconds.</p> <p>You can specify this value as:</p> <pre>NETSCAN_START_DELAY 900</pre> <p>Another way to specify this value is by using a Tcl expression, which would read as follows:</p> <pre>NETSCAN_START_DELAY {15*60}</pre> <p>where 15 is the number of minutes. When multiplied by 60 seconds, the value becomes 900 seconds.</p>
NETSCAN_POLL	<p>Network Discovery Interval (in seconds). Default setting is 86400 seconds, or 24 hours.</p> <p>Optionally, specify this value using a Tcl expression in curly brackets. For example: to specify 12 hours, enter:</p> <pre>NETSCAN_POLL {12*60*60}</pre> <p>where 12 is the number of hours, multiplied by 60 minutes, multiplied by 60 seconds.</p>
NETSCAN_INCLUDE	<p>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.</p> <p>Use the following syntax:</p> <pre>NETSCAN_INCLUDE { object_class {object_list} object_classn {object_list} }</pre> <p>where:</p> <p><i>object_class</i> 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.</p> <p><i>object_list</i> is a space-separated list of common names within curly brackets. These are the only</p>

Parameters	Explanation
	<p>objects to be included in network discovery for the given object class. Unnamed objects in the specified class are excluded.</p> <p>All names are case insensitive.</p> <p>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.</p> <pre>NETSCAN_INCLUDE { network {lanmanredirector} domain {domain1 domain2} }</pre> <p>For additional examples, see Using NETSCAN_INCLUDE to Limit Network Discovery on page 131.</p>

- 5 Save and close the file.
- 6 Restart the Radia Integration Server and open the Management Portal.

Using NETSCAN_INCLUDE to Limit Network Discovery

- 1 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.
- 2 For general syntax, refer to the NETSCAN_INCLUDE entry in Table 2 on page 129. When using NETSCAN_INCLUDE, be aware of the following implications:
- 3 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
```
- 4 For a given class, if a class is not named in a NETSCAN_INCLUDE list, all objects are included. (This is subject to limits already processed for a higher-class object, discussed in Step 3 above)

- 5 Once you limit objects of a given class in a `NETSCAN_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. This is the 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 128) or LDAP authentication (see page 153).

Table 3 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 128 for detailed steps on how to modify parameters in the `rmp.cfg` file.

Table 3 Additional RMP Configuration Parameters

Parameter	Definition
LINKS	<p>Specifies the policy configuration links to enable when policy has been applied to the objects in the Chassis container and related Cross-Reference containers for server blade devices.</p> <p>See <i>Enabling Policy Configurations for Blades, Enclosures and Racks</i> on page 211 for the details on specifying the attributes for this parameter.</p>
LISTENING_ADDRESS	<p>Specifies a valid network address (either an IP address, hostname, or DNS address) that is to be passed to Radia Management Agents, and then used by them to connect back to the Management Portal.</p> <p>Use a LISTENING_ADDRESS when the Management Agents are experiencing communication failures with the Management Portal and are successful in registering back to the Portal or performing remote tasks on behalf of the Portal. This can occur when the RMP resides on a machine with dual-NIC cards or is using a dynamic IP address. Specify a network address using the format that works best in your environment:</p> <pre>LISTENING_ADDRESS IPaddress or LISTENING_ADDRESS hostname Or LISTENING_ADDRESS DNS</pre> <p> Ensure the network address you enter points to the current RMP Zone. If it does not, results are unpredictable.</p>

Parameter	Definition
USE_FQDNHOST_NAME	<p>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.</p> <ul style="list-style-type: none"> • Type USE_FQDNHOST_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_FQDNHOST_NAME 1 to return to the use of fully qualified domain names (the default).
WOL_MCAST_ADDR	<p>Permits Wake-on-LAN (WOL) support in multicast-enabled environments. Default is no support for multicast WOL.</p> <ul style="list-style-type: none"> • Type WOL_MCAST_ADDR <IP_address> where the <i><IP address></i> 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 start or stop another Directory Service, such as the service for the Configuration Server hosting the PRIMARY database or an Active Directory service in your enterprise. For details, see Adding a Directory Service on page 135.

Figure 12 Example of 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 Management Portal's Zone directory service to another directory service. You can add any 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, NDS, or Netscape Iplanet.
- **LDAPS**
Use this type to connect to another LDAP directory over SSL (Secure Socket Layer). This type requires the server hosting the LDAP directory to be SSL enabled. See Preparing for an LDAPS Directory Service Connection on page 136 for more information.
- **RCS**
Use this type to connect a Configuration Server and access the PRIMARY file in the Radia Database.
- **DSML**
Use this type to connect to another Management Portal zone in your enterprise.
 - ▶ When you install another Management Portal Zone using the Install Management Portal task, this type of Directory Service connection 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 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 Management Portal startups.
 - A manual connection requires the user to connect each time they want to access the defined directory. For details, see *To start a predefined Directory Service* on page 183.
 - 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 183.

Preparing for an LDAPS Directory Service Connection

Prior to adding an LDAPS directory service, review the requirements and SSL-related files needed to support an LDAPS directory service connection, which are listed below.

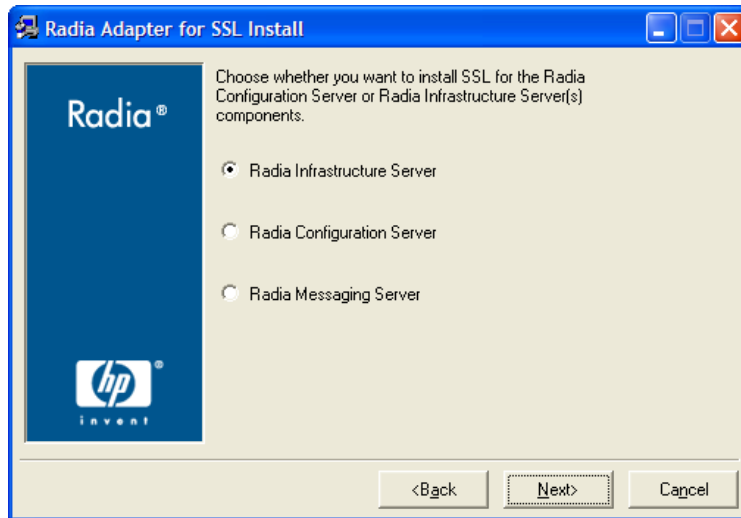
- Management Portal Version 2.1.1 or above.
- The target server hosting the LDAP directory requires an installed X.509 SSL server certificate and must be SSL enabled. Obtain the SSL port number from the server administrator; the default LDAPS port number is 636.
- Prior to installing the HP OpenView Adapter for SSL using Radia, delete any copies of `ldap82.dll` currently found in the Management Portal folders within its root install directory:
`C:\Novadigm\IntegrationServer.`

This is required to make sure the latest version of the `ldaps82.dll` distributed with the SSL Adapter is used.

- Install the SSL Adapter for HP OpenView using Radia, Version 2.1.1 or above, on the Management Portal server. During the SSL Adapter

installation for the Radia Integration Server, select **Radia Integration Server** as shown in Figure 13 below.

Figure 13 Adapter for SSL Install



Selecting **Radia Integration Server** provides the Management Portal with both HTTPS and LDAPS support. For additional details on installing the Adapter for SSL, refer to the *Installation and Configuration Guide* for that product.

- If the server hosting the LDAP directory is using a certificate authority other than Entrust, VeriSign or G.E., obtain and place the CA root certificate (the public key) on a local drive of the Management Portal. By default, the Adapter for SSL installs a folder and certificate file which can be used to store the public key:

```
CACertificate File      cacert.pem
CACertificate Directory RMP_dir/etc/CACertificates
```

You can either add the contents of the public key to the top of the default `cacert.pem` file, or copy the CA root certificate file to a local directory on the Management Portal.

To allow for multiple LDAPS connections, multiple keys may be added to the top of this `cacert.pem` file.

You will need to reference this file and its location when you add an LDAPS Directory Service in the CA Certificate File and CA Certificate Directory properties on the Add Directory Service page.

- Open the certificate file on the LDAP server to learn how the host is specified in the CN= value of the Subject line. For example, the certificate may specify the LDAP host using its fully-qualified DNS hostname. When entering the URL property in the Add Directory Service task, you must specify the LDAP hostname using the common name specified in its certificate file or the connection will fail.

Once you have met these LDAPS requirements, continue with the task To add a directory service below.

To add a directory service

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



Legend

- a** Browse to Directory Services
 - b** Click Add Directory Service
- 2 Click **Add Directory Service** from the Model Administration task group. The Add Directory Service page opens, where you specify the properties.
 - 3 Begin by selecting the Type of directory service from the Type drop-down list.

Table 4 Adding a Directory Service by Type

Type	Directory Service Connection
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 and NDS.
ds-ldaps	LDAPS: an LDAPS Directory Service using LDAP over SSL.
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 or LDAPS Directory Service Properties, on page 140
- Specifying RCS Directory Service Properties on page 143
- Specifying DSML Directory Service Properties on page 146
- Specifying Metakit Directory Service Properties on page 146

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

The Directory Service definition is added to the Directory Services container.

- If the Startup type is automatic and the service is active, the Workspace displays the directory objects at its mount point, which is defined by the USE parameter of its Directory Service properties.
- If the Startup type is manual, or the service is not active, use the Start Directory Service task to start the service. See Starting a Directory Service.

Specifying LDAP or LDAPS Directory Service Properties

Use Table 5 below to complete the Directory Service Properties for a Type of ds-ldap (LDAP) or ds-ldaps (LDAP over SSL).



Review the topic [Preparing for an LDAPS Directory Service Connection](#) on page 136 prior to adding an LDAPS directory service.

Table 5 Directory Service Properties

Field	Description
Common Name	Common name for the Directory Service. Must be unique among Directory Service objects and follow X500 standards. Example: <code>eng.acme.com</code> is assigned to the LDAP Directory Service known as <code>dc=eng,dc=acme,dc=com</code>
Display Name	Display Name of the object in the Directory Service container.
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 Start Directory Service task from the Infrastructure task group 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. ds-ldaps Type required for an LDAP over SSL directory service. See prerequisites on page 136.

Field	Description
URL (Web Page Address)	<p>LDAP Format and Examples:</p> <p>ldap://<IP address or qualified computer name>:<LDAP port>/<qualified username></p> <p>ldap://10.10.10.1:389/administrator@eng.acme.com</p> <p>ldap://svr209.usa.mycompany.com:389/admin@usa.mycompany.com</p> <p>Novell Directory Server (NDS) Format and Examples:</p> <p>ldap://<IP address or qualified computer name>:<LDAP port>/<full dn of binding User></p> <p>ldap://10.10.10.55:389/cn=rpolicymgr,ou=pcbadm,o=pcb</p> <p>LDAPS Format and Examples:</p> <p>ldaps://<LDAP hostname in certificate>:<LDAP secure port>/<bind User>@<domain></p> <p>ldaps://svr3.eng.acme.com:636/administrator@eng.acme.com</p>
Password	Password for the username entered in the URL
Used for Policy	<p>Default: false</p> <p>False indicates this LDAP directory service is not to be used for policy tasks.</p> <p>True enables the use of this Directory Service for all policy tasks. To set this field, use the Modify task from the Model Administration task group.</p>

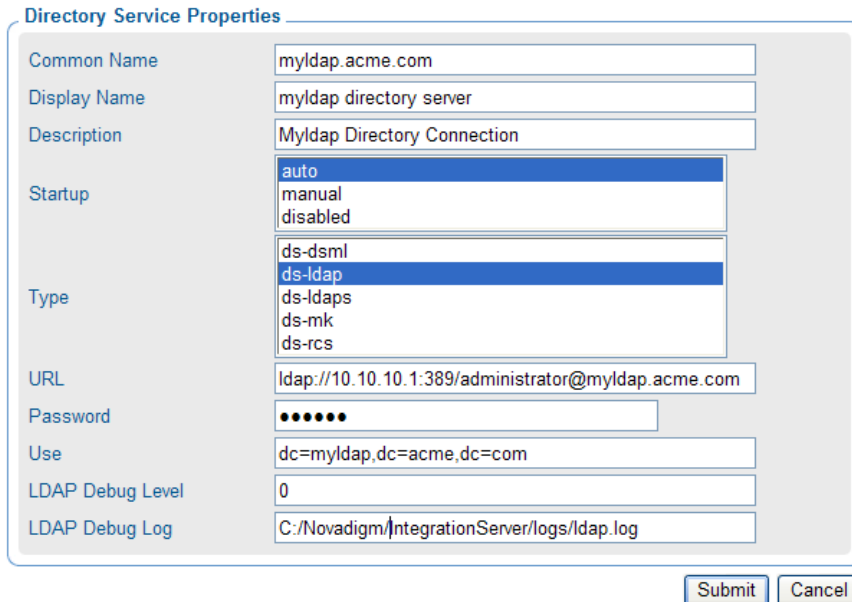
Field	Description
Use	<p>Specifies a fully-qualified domain at which to mount the directory service. This mount point becomes the highest level of the directory structure that can be accessed from the Management Portal. For example, to mount and limit the use of the eng.acme.com directory to the Computers domain, specify the properties for this Directory Service with a Use value of:</p> <p>cn=computers,dc=eng,dc=acme,dc=com</p> <p>For NDS, a typical Use value is:</p> <p>cn=pcb</p> <p>If left blank, the common name is used to mount the directory service at the highest level.</p>
CA Certificate Directory	<p>Available with Type ds-ldaps only.</p> <p>Default: <code><RMP dir>/etc/CACertificates</code></p> <p>Local, fully-qualified path to the required certificate file containing the public key of the LDAP host server. See Preparing for an LDAPS Directory Service Connection on page 136 for more information.</p>
CA Certificate File	<p>Available with Type ds-ldaps only.</p> <p>Default: <code>cacert.pem</code></p> <p>Filename containing the CA Certificate public key for the LDAP host server. See Preparing for an LDAPS Directory Service Connection on page 136 for more information.</p>
LDAP Debug Level	<p>Default: 0 (no LDAP logging)</p> <p>HP does not recommend enabling LDAP logging unless you are directed to by HP technical support. For example, a log level such as 5 may be requested to troubleshoot an LDAP connection problem.</p>
LDAP Debug Log	<p>Default: <code><RMP dir>/logs/ldap.log</code></p> <p>The path and filename used for logging LDAP debug entries when the LDAP Debug Level is greater than 0.</p>

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 14 Add Directory Service Properties for LDAP

Add Directory Service



Directory Service Properties	
Common Name	myldap.acme.com
Display Name	myldap directory server
Description	Myldap Directory Connection
Startup	auto
Type	ds-ldap
URL	ldap://10.10.10.1:389/administrator@myldap.acme.com
Password	••••••
Use	dc=myldap,dc=acme,dc=com
LDAP Debug Level	0
LDAP Debug Log	C:/Novadigm/IntegrationServer/logs/ldap.log

Submit Cancel

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

- ▶ To specify an LDAP or LDAPS Directory Service being used for policy, see [Modifying Directory Service Properties](#) on page 148.
- To specify an LDAP or LDAPS 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 156.

Specifying RCS Directory Service Properties

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

Table 6 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 Start Directory Service task from the Infrastructure task group 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 Configuration Server directory service.

Field	Description
URL (Web Page Address)	<p>Default entry: <code>rcs://localhost:3464/RAD_MAST</code></p> <p>Format: <code>rcs://<hostname or IP address>:<port #>/<Username></code></p> <p>Example: <code>rcs://myserver600:3464/RAD_MAST</code></p> <p>Change <code><localhost></code> to specify the qualified host name or IP address of your 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.</p>
Password (User Password)	Password for the username entered in the URL.
Path (see Modify task)	<p>Optional entry for expediting a connection to the RCS Primary file.</p> <p>Specifies the fully qualified path of ZTOPTASK.EXE on the RCS. For example:</p> <p><code>C:/Novadigm/ConfigurationServer/bin/ztop task.exe</code></p>
Timeout	<p>Period of inactivity (defined in seconds) after which an RCS connection will timeout and the connection will be dropped. 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.</p>

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 Configuration Server.

Figure 15 Sample Directory Service Properties for an RCS



Add Directory Service

Directory Service Properties

Common Name	<input type="text" value="primary"/>
Display Name	<input type="text" value="RCS Database"/>
Description	<input type="text"/>
Startup	<input type="list" value="auto"/> manual disabled
Type	<input type="list" value="ds-dsml"/> ds-ldap ds-ldaps ds-mk ds-rcs
URL	<input type="text" value="rcs://localhost:3464/RAD_MAST"/>
Password	<input type="password"/>
DS Prefix	<input type="text" value="cn=config,cn=acme corp,cn=radia"/>
Path	<input type="text"/>
Timeout	<input type="text" value="0"/>

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 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.



Examples of ds-mk directory services include the 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 7 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.
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 run the Start Directory Service task during each Management Portal session. Disabled Restricts any connection to or mounting of this Directory Service. The startup must be changed to auto or manual before anyone can connection to this Directory Service can take place.
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

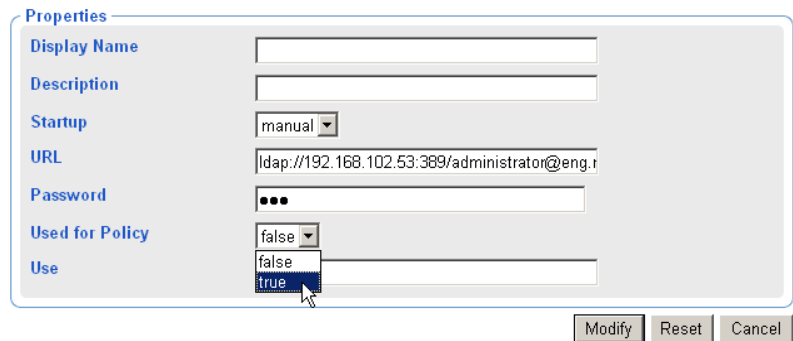
- 1 Display the Directory Service Properties for the service you want to modify.

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

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

The Modify page for the specific object type opens. The next figure shows a sample Modify LDAP page.

Modify LDAP



The screenshot shows a web form titled "Properties" for modifying an LDAP service. The form contains several fields: "Display Name" (text input), "Description" (text input), "Startup" (dropdown menu set to "manual"), "URL" (text input with value "ldap://192.168.102.53:389/administrator@eng.t"), "Password" (password input field with masked characters "•••"), "Used for Policy" (dropdown menu set to "false"), and "Use" (dropdown menu with "false" selected and "true" highlighted by a mouse cursor). At the bottom right of the form are three buttons: "Modify", "Reset", and "Cancel".

- 3 Change any entries to reflect the modified properties. For details on these fields, refer to the appropriate table in Adding a Directory Service on page 135.
- 4 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.

► 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 156 for more information.

- 5 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.

► 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

► 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 Management Portal:

- 1 Display the object properties by navigating to the **Zone** → **Configuration** → **Directory Services** container, and click on the directory service to be removed.
- 2 Click **Remove** from the Model Administration task group.
The Remove Directory Service dialog asks you to confirm this delete.
- 3 Click the green check mark to confirm the delete, or the red X to cancel the delete.

Starting a Directory Service

Use the Start Directory Service task in the Infrastructure task group to start the service for an external directory service that is currently stopped or is defined with a Startup mode of *manual*.



To start an RCS Service connection from its Device location in your Zone Directory, use the procedure starting on page 151. This access will prompt you to add the service to the Directory Services container if it does not currently exist.

For details on defining or modifying a directory service mount point, see Adding a Directory Service on page 135 or Modifying Directory Service Properties on page 148.

To start a predefined Directory Service

- 1 Display the Properties page for the directory service with which you want to connect.
 - Go to the **Zone** → **Configuration** → **Directory Services** container. In the Workspace, click the Directory Service object.
- 2 Click **Start Directory Service** from the Infrastructure task group.

The directory service connection starts immediately. The Workspace displays the objects at the mount point of the directory. The mount point is defined by the USE value of the Directory Services properties.

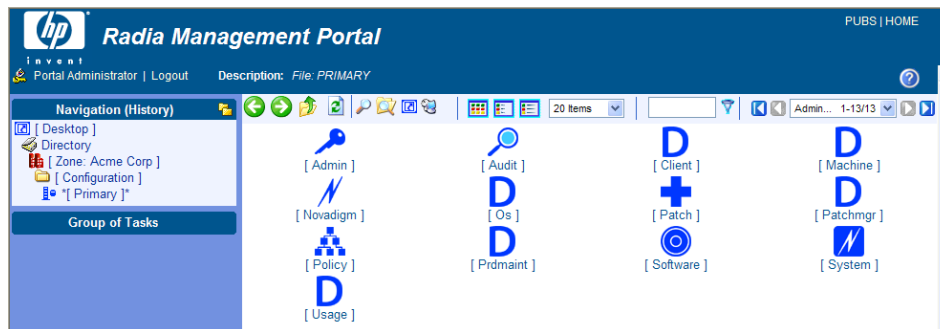
Your navigation location changes to where that type of directory service is accessed, and the tasks available for working with the objects also display as you navigate through the structure. See the following table for a list of where each type of Directory Service is accessed from in the Directory.

Table 8 Locations for Accessing Directories and Mount Points

Object	Directory Locations
Active Directory, other LDAP Directory	Directory level; at the same level as the Zone
Primary file of RCS	Zone → Configuration → Primary object
Network mount point	Zone → Networks container

Object	Directory Locations
DSML (Subordinate Zone)	Zone → Zone Access Points container
Metakit directory service (Advanced User)	Defined by Template

The next figure shows a sample connection to an RCS Database defined with a common name of Primary. The Workspace displays the class objects in the Primary file of that database; the class objects in your RCS Database may vary.



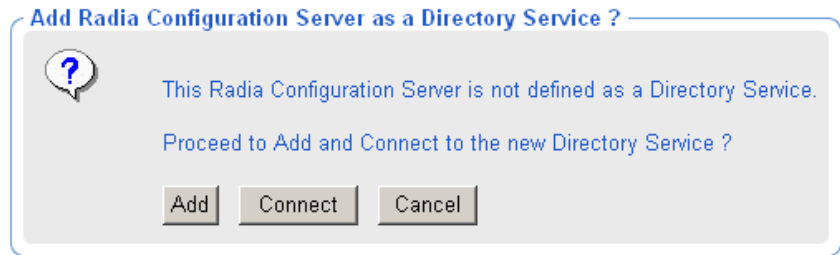
To connect to a service defined for a Device

- 1 Use the Navigation aid and workspace to go to the Zone → Devices container.
- 2 Select the Device containing the service to which you want to connect.
- 3 In the Workspace, select the service to which you want to connect.

The Service Properties page opens. The following figure shows a sample Service Properties page for the `Ztoptask.exe` service of the Configuration Server.

- 4 Click **Start Directory Service** from the Infrastructure task group.
- 5 If you are starting 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.

Connect Directory Service



- Click **Add** to first add the RCS as a Directory Service to the Zone Configuration container, and then connect (start) the directory service.

Adding a Directory Service entry allows an automatic connection to this RCS directory whenever the 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 143.

- Click **Connect** to connect to the RCS Primary directory for this session only.

Stopping a Directory Service


Use the **Stop Directory Service** task in the Infrastructure task group to stop an external service defined as a Directory Service to the Portal. After stopping the directory service, the objects in that Directory Service are no longer available for performing Management Portal operations until the directory service is started again.

- To stop a service defined as a Directory Service, use the following procedure *To stop a Directory Service*.
- To stop an RCS Service from its Service Properties page within the Device container, use the procedure *To stop a service defined for a Device* on page 153.

To stop a Directory Service

- 1 Display the Directory Service Properties page for the service you want to stop.

To navigate to a Directory Service Properties page:

- a Use the Navigation aid and workspace 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 .
- 2 Click the **Stop Directory Service** task within the Infrastructure task group.

The directory service connection is terminated immediately.

To stop a service defined for a Device

- 1 Use the Navigation aid and workspace to go to the Zone Devices container.
- 2 Select the Device containing the service from which you want to disconnect.
- 3 In the Workspace, select the service to which you want to disconnect.

The Service Properties page opens.

- 4 Click **Stop Directory Service** from the Infrastructure task group.

The directory service is stopped 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 Management Portal. The `LDAP_AUTH` parameters specify:

- the default external authentication setting for all users of the Management Portal (on or off)
- the domain a user will bind to
- the hostname and port of the LDAP server



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 88. To disable LDAP authentication for individual users, see Modifying the Default LDAP Authentication for Specific Users on page 156.

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 Management Portal

- 1 Stop the Radia Integration Server service.
- 2 Use a text editor to open the Management Portal configuration file, `rmp.cfg`, located by default in `SystemDrive:\Novadigm\IntegrationServer\etc`.
- 3 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 the bold face portion of the sample code below.

```
# RMP Module (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
#

```



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 156.

- 4 Use one or more spaces to separate the parameter and its value. See Table 9 below for details.

Table 9 rmp.cfg parameters for external LDAP authentication

Parameter and Value	Definition and Examples
LDAP_AUTH 1 <i>or</i> LDAP_AUTH 0	<p>Sets the default value of external authentication for all users logging onto the Management Portal. Use the External Authentication? field on on the Person properties page to override the default value for any user.</p> <ul style="list-style-type: none"> • 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>	<p>Defines the domain that a user will bind to. Replace <i>mydomain.com</i> with the domain that users will bind to. The <<user>> portion will be substituted with the value entered on the login page.</p> <pre>LDAP_AUTH_DN <<user>>@mydomain.com LDAP_AUTH_DN <<user>>@domainA.com</pre>
LDAP_AUTH_HOST hostname:389	<p>The hostname and port of the LDAP server. Where "myldaphostname" is the hostname of the LDAP server.</p>

- 5 Save and close the file.
- 6 Restart the Radia Integration Server and open the Management Portal.

Modifying the Default LDAP Authentication for Specific Users

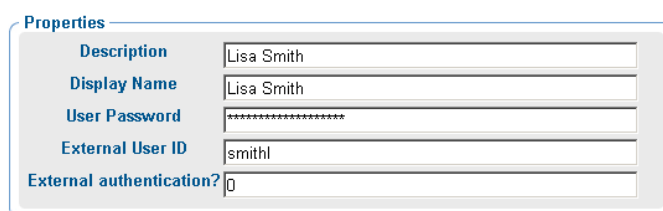
To change the default LDAP authentication value for specific users, use the Modify Person task and reset the value of External authentication for that person to the desired value.

- 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 230 and Modifying Users on page 233.

Figure 16 Modify Person dialog box

Modify Person



The screenshot shows a 'Properties' dialog box with the following fields:

Description	Lisa Smith
Display Name	Lisa Smith
User Password	*****
External User ID	smithl
External authentication?	<input type="checkbox"/>

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 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 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 Management Portal for a Custom LDAP Policy Prefix (other than edm)

- 1 Stop the Radia Integration Server service.
- 2 Use a text editor to open the Management Portal configuration file, `rmp.cfg`, located by default in `SystemDrive:\Novadigm\IntegrationServer\etc`.
- 3 Insert the `PREFIX` parameter (must be uppercase) into this file before the finishing curly bracket (`}`) as shown in the code sample here.

```
#
# 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 (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

}
#
# END OF CONFIG
```

#

- 4 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 10 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 Policy Server. For example: PREFIX rad defines a Policy prefix of rad instead of edm.

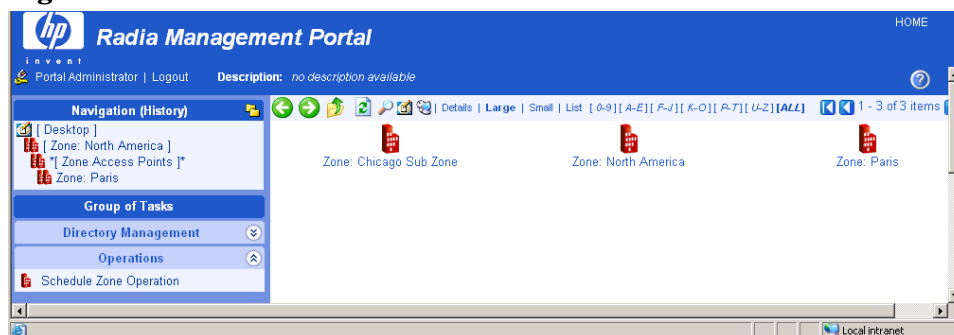
- 5 Save and close the file.
- 6 Restart the Radia Integration Server and open the Management Portal.

Configuring Zone Access Points

Access Points to other Management Portal Zones in your enterprise are automatically configured whenever you install multiple portal zones using the Install Management Portal 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 17 Zone Access Points container



Establishing Devices and Device Groups

There are a number of ways to bring devices under the control of a 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.
 - ▶ 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 181.
- 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 295.

Adding Devices to an RMP Zone

There are various ways to add devices to your RMP Zone. Table 11 on page 160 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 11 Methods to Add Computers to a Zone Devices Container

Method	Description and Reference
Network Selection	<p>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.</p> <p>Or</p> <p>Browse to computers in your Networks container and select Manage Computer from the Operations task group. For details, see <i>Managing Computers in Your Management Portal Zone</i> on page 272.</p>
Active Directory Selection	<p>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.</p> <p>or</p> <p>Browse to a computer in your LDAP directory and select the Manage Computer task in the Operations task group. For details, see <i>Managing Computers in Your Management Portal Zone</i> on page 272.</p>
Hostname List	<p>Prepare a list of hostnames and use the Import Devices task. For details, see <i>Importing Devices</i> on page 192.</p>
Individual Entry	<p>Browse to a group in the Groups container and click Add Device from the Model Administration task group. For details, see <i>Adding a Single Device</i> on page 175.</p>
Installed Radia Management Agent	<p>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 Management Portal.</p>

Several of the tasks used to bring devices under control of the 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 below.

Basic Procedures for Modifying Groups

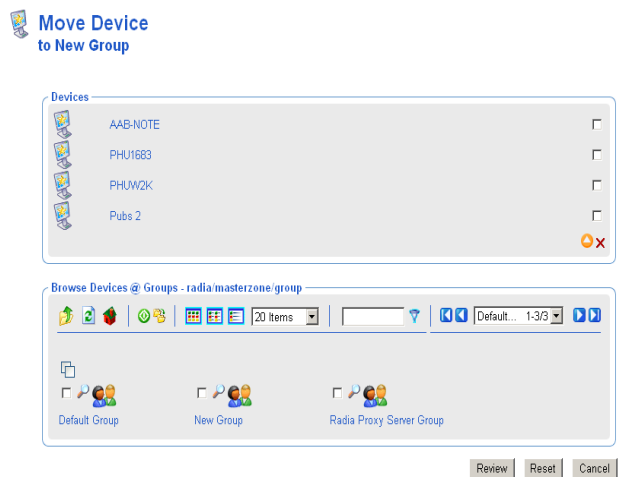
Many tasks in the Management Portal use a similar set of windows to browse and modify items in a group. This topic describes how to use these windows. The same procedures apply regardless of the exact task you are performing.

Use the task summary below as a guide.

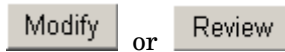
Task 1 Navigate to the target group and click the appropriate Portal task.



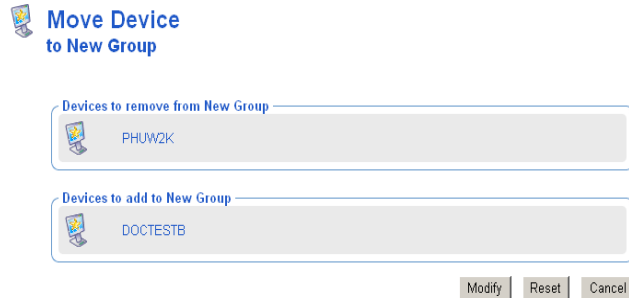
Task 2 Change the items in the group.



Task 3 Modify/Commit/Review changes.



Task 4 After Review, click **Modify**.

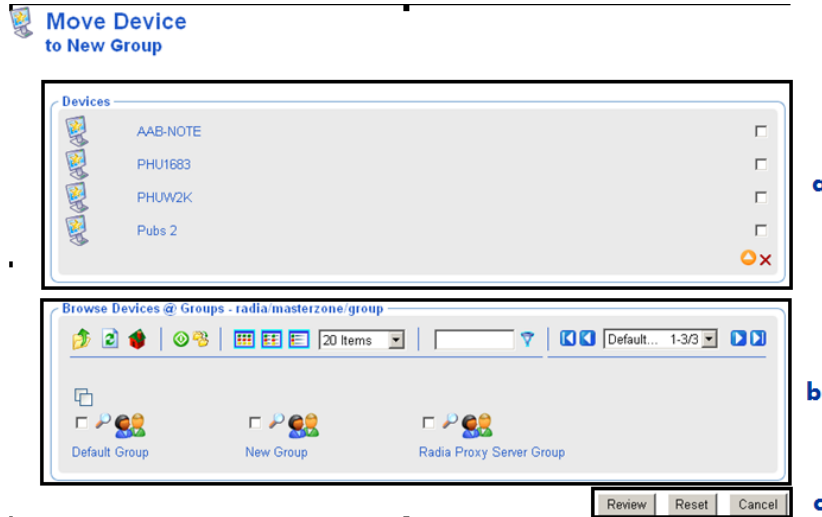


Using the Browse and Modify Window

The next figure shows a sample Browse and Modify window. The Move Device window opens when you select the Move Device task from the Model Administration task group.


Figure 18 on page 163 illustrates the three main areas of this window: the group list area, the browse area, and the buttons area. If you are working with Services or Policy objects, the group list area will also contain editors for service attributes and expressions. The following topics discuss how to use these areas.

Figure 18 Move Device task



Legend

- a** Group list: Delete or change using icons
- b** Browse area: Select items to add, move, or copy to group list
- c** Buttons: Click Review to continue

 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, the figure above 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 Using the Group List Area on page 164.

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 166 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 169 for more information.

- **Browse area**
The bottom area allows you to browse your 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 173.
- **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

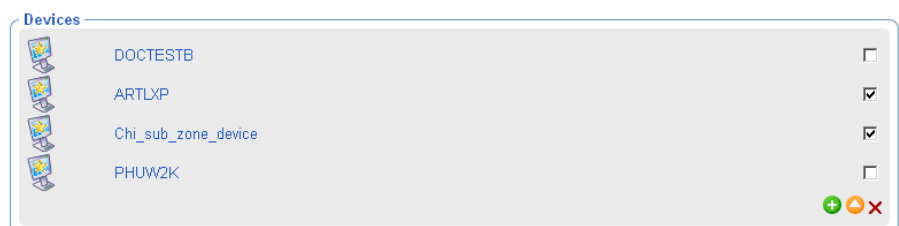
Use the group list area of the Browse and Modify window to delete items from the group and manually modify or add an item. To manually modify or add an item, you must specify its X500 Distinguished Name.



The X500 Distinguished Name is listed in the Object Information area of an item's Properties page. It is also available when you place the mouse over an object's name in the Workspace or the Navigation area.

To delete one or more items in the list

- 1 Click the check box to the right of each item in the group list area to be removed.



- 2 Click **X** to delete the items from the list.
- 3 Click the **Modify** or **Commit** button below the Browse group area to save the modified list.

▶ 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

- 1 Click the check box to the right of each item in the group list area to be modified.
- 2 Click **▶** to modify the checked items.



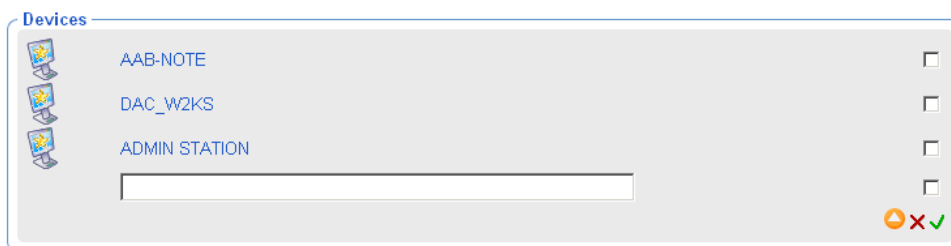
- 3 In the text box, modify the X500 Distinguished Name for the item.
- 4 Click **✓** to accept the changes.
- 5 Click **Modify** at the bottom of the page to save the modified list.


▶ Some tasks include a Review button. In this case, click **Review** and then click **Modify** after reviewing the changes.

To manually add an item to the list

- 1 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.



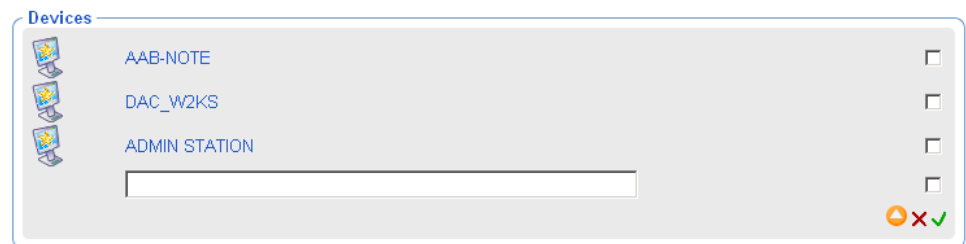
►  The X500 Distinguished Name is listed in the Object Information area of an item's Properties page. It is also available when you place the mouse over an object's name in the Workspace or the Navigation area.


- 2 In the text-box, 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`

- 3 Click  to accept the changes.
- 4 Click **Modify** or **Commit** below the Browse area to save the modified list.

► Some tasks include a Review button. In this case, click **Review** and then click **Modify** after reviewing the changes.



- 5 In the text box, type the X500 Distinguished Name entry for the item.
- 6 Click  to accept the changes.
- 7 Click **Modify** or **Commit** below the Browse area to save the modified list.

► 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

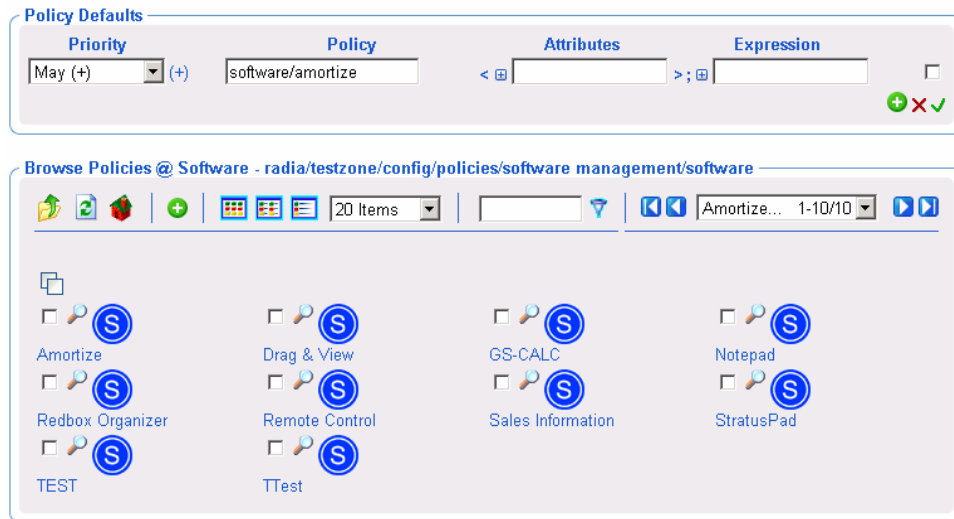
After selecting a service in the Browse and Modify window, use the Attribute Editor to specify values for the attributes for Radia services. The values that you are specifying are for policy (see Modifying Policies on page 105), defaults (see Modifying Policy Defaults on page 119) or overrides (see Modifying Policy Overrides on page 121).

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

- 1 After selecting the appropriate task from the Policy (Advanced) task group, use the Browse window to select the appropriate service, such as Amortize.

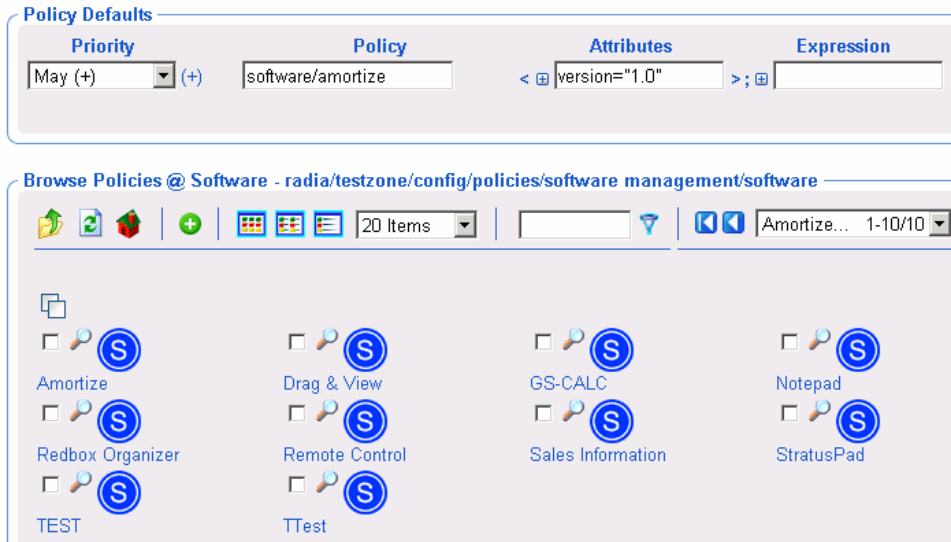
Modify Policy Defaults



The screenshot shows two windows from a software management interface. The top window, titled "Policy Defaults", has four tabs: "Priority", "Policy", "Attributes", and "Expression". The "Priority" tab is selected, showing a dropdown menu with "May (+)" and a "+" button. The "Policy" tab shows the text "software/amortize". The "Attributes" and "Expression" tabs are empty. There are green, red, and checkmark icons at the bottom right of this window. The bottom window, titled "Browse Policies @ Software - radia/testzone/config/policies/software management/software", shows a list of 20 items. Each item has a checkbox, a magnifying glass icon, and a blue circle with an 'S'. The items listed are: Amortize, Drag & View, GS-CALC, Notepad, Redbox Organizer, Remote Control, Sales Information, StratusPad, TEST, and TTest. The "Amortize" item is highlighted.

- 2 Click the  to the left of the Attributes text box.
The Attributes Editor area opens.

Modify Policy Defaults



The screenshot shows two windows from a management console. The top window, titled "Policy Defaults", has four columns: "Priority" with a dropdown set to "May (+)", "Policy" with the text "software/amortize", "Attributes" with the text "< version='1.0' >", and "Expression" which is empty. The bottom window, titled "Browse Policies @ Software - radia/testzone/config/policies/software management/software", shows a list of services in a grid. Each service has a checkbox and a blue circle with an 'S'. The services listed are: Amortize, Drag & View, GS-CALC, Notepad, Redbox Organizer, Remote Control, Sales Information, StratusPad, TEST, and TTest. The "Amortize..." service is selected, and the breadcrumb shows "Amortize... 1-10/10".

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.

- 7 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 105), defaults (see [Modifying Policy Defaults](#) on page 119) or overrides (see [Modifying Policy Overrides](#) on page 121).


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](#) on page 166), this service will only be deployed to machines with a Windows NT operating system.

To use the Expression Editor

- 1 After selecting the appropriate task from the Policy (Advanced) task group, use the Browse window to select the appropriate service, such as Amortize.



In the example shown in this procedure, the version attribute has also been set to 1.0.

- 2 Click  to the left of the Expression text box.

The Expression Editor area opens.




Modify Policy Defaults

Policy Defaults

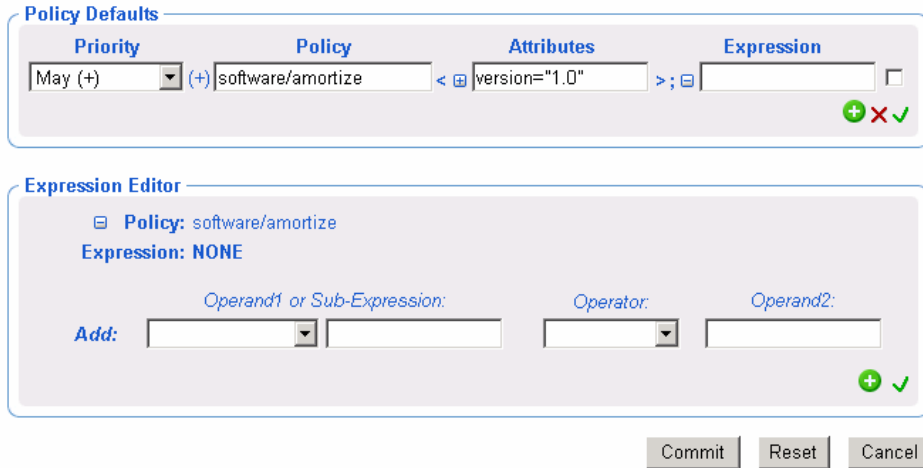
Priority	Policy	Attributes	Expression
May (+) <input data-bbox="738 724 763 745" type="button" value="+"/>	software/amortize <input data-bbox="657 724 682 745" type="button" value="<"/>	version="1.0" <input data-bbox="1031 724 1055 745" type="button" value=">"/>	<input type="text" value=""/> <input type="checkbox"/>

Expression Editor

Policy: software/amortize
Expression: NONE

- 3 In the Expression Editor area, click  to add a new expression.

Modify Policy Defaults




The screenshot shows two main sections: "Policy Defaults" and "Expression Editor".

Policy Defaults: This section contains four fields: "Priority" (set to "May (+)"), "Policy" (set to "software/amortize"), "Attributes" (set to "version='1.0'"), and "Expression" (empty). There are plus, minus, and checkmark icons for each field. A green plus icon, a red X icon, and a green checkmark icon are located at the bottom right of this section.

Expression Editor: This section shows "Policy: software/amortize" and "Expression: NONE". Below this are three fields: "Add:" (a dropdown menu), "Operand1 or Sub-Expression:" (a text field), "Operator:" (a dropdown menu), and "Operand2:" (a text field). A green plus icon and a green checkmark icon are at the bottom right of this section.

At the bottom of the interface are three buttons: "Commit", "Reset", and "Cancel".

- 4 From the Add drop-down list, select one of the following pre-defined operands:

 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 *Installation and Configuration Guide for the HP OpenView Application Manager using Radia* 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.

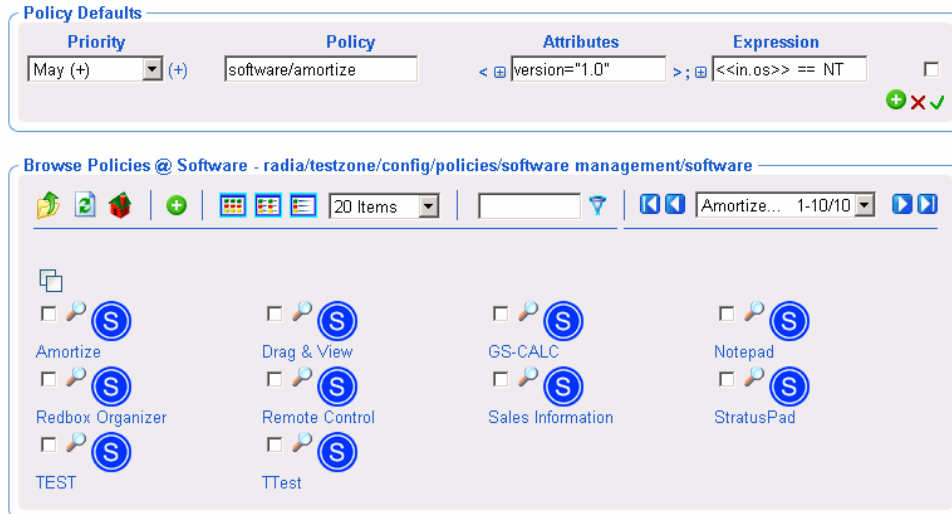
- 5 If necessary, select an operator from the Operator drop-down list, such as ==.

Table 12 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.

- 6 In the Operand2 text box, type the appropriate value, such as **NT**.
- 7 Click  to accept the changes to the expression.

Modify Policy Defaults



The screenshot shows two windows from a management console. The top window, titled "Policy Defaults", has four columns: "Priority" with a dropdown set to "May (+)", "Policy" with the text "software/amortize", "Attributes" with a field containing "< version='1.0'" and a plus icon, and "Expression" with a field containing "<<in.os>> == NT" and a checkbox. The bottom window, titled "Browse Policies @ Software - radia/testzone/config/policies/software management/software", features a toolbar with icons for home, refresh, add, and search, a "20 Items" dropdown, a search bar, and navigation buttons. Below the toolbar is a grid of 12 items, each with a checkbox and a blue circle containing an 'S'. The items are: Amortize, Drag & View, GS-CALC, Notepad, Redbox Organizer, Remote Control, Sales Information, StratusPad, TEST, and TTest.

8 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 Devices into a Group* on page 175.



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 19 Browse area label identifies current navigation location






Navigation Icons

- Click  to go up one level in your Zone directory.
- Click  to refresh the view.
- Click  to return home to the browse location when you started the task.
- Click  (a group or container icon) to browse the items in that group.

Action Icons

- Click  to add selected objects to the top area.
- Click  to move selected objects to the top area.
- Click  to copy selected objects to the top area.

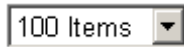
View Icons


- 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 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 161.

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 181, and then use the **Add Device** task, below.

To add a single device

- 1 If necessary, set the Navigate aid to Location mode.



- 2 Navigate to the **Groups** container in the Zone.



- 3 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.
- 4 From the Model Administration task group, click **Add Device**.

The Add Device dialog box opens.



Add Device

Add Device

Display Name	<input type="text"/>
DNS Host Name	<input type="text"/>
IP Address	<input type="text"/>

- 5 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 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.

6 Click **Add**.

The 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.
- 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 Management Portal must generate a unique Common Name for a device. A generated Common Name is illustrated below:

Figure 20 Sample Common Name generated for a device



The screenshot shows a window titled "New Device 2 Device Properties". At the top right, there are two tabs: "Properties" (selected) and "Object Information".

Properties

Create Time Stamp	2004/05/04 19:21
Group Membership	Default Group
IP Address	192.168.104.194
Modify Time Stamp	2004/05/04 19:21


Back to top

Object Information

Display Name	New Device 2
Common Name	20040504T232118ZD
X500 Distinguished Name	cn=20040504t232118z0, cn=device, cn=northamerica, cn=radia
Object Class	top computer device

Back to top

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 21 on page 179 shows the Device Properties for a new device when no RMA is installed.

Figure 21 Device Properties for new device

 **QA1-2 in QA Lab**
Device Properties

Properties | Object Information

Properties

Create Time Stamp	2004/04/14 12:01
DNS Host Name	qa1-2
Group Membership	Default Group
Modify Time Stamp	2004/04/14 12:01

[Back to top](#)

Object Information

Display Name	QA1-2 in QA Lab
Common Name	20040414T160136ZD
X500 Distinguished Name	cn=20040414t160136z0, cn=device, cn=mahwah, cn=radia
Object Class	top computer device

[Back to top](#)

After a Radia Management Agent is installed on a Device, the next figure. The 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 22 Device Properties after installing the RMA



pathxptest.usa.mycompany.com
Device Properties

Properties | Object Information

Properties

Create Time Stamp 2004/04/27 18:06

DNS Host Name pathxptest.usa.novadigm.com

Enclosure Manufacturer Dell
 Computer Corporation

Group Membership [Default Group](#)

Link to Operating System Object [cn=windows_xp_cn=operatingsystem_cn=xref_cn=northamerica_cn=radia](#)

Link to OS Service Pack Object [cn=service_pack_1_cn=windows_xp_cn=operatingsystem_cn=xref_cn=northamerica_cn=radia](#)

Link to System Manufacturer Object [cn=dell_cn=smsystemmanufacturer_cn=xref_cn=northamerica_cn=radia](#)

Link to System Product Name Object [cn=optiplex_cn=dell_cn=smsystemmanufacturer_cn=xref_cn=northamerica_cn=radia](#)

Modify Time Stamp 2004/05/01 21:16

Operating System Windows XP

Operating System Service Pack Service Pack 1

OS Platform windows

SMBIOS Enclosure S/N HPKHP11

SMBIOS Machine Unique UID 4C4C4544C6504B108048C8C04F503131

SMBIOS Manufacturer Dell
 Computer Corporation

SMBIOS Product OptiPlex
 GX400

SMBIOS System S/N HPKHP11

Zone [Zone: North America](#)

Back to top

Object Information

Display Name pathxptest.usa.mycompany.com

Common Name pathxptest.usa.novadigm.com

X500 Distinguished Name [cn=pathxptest.usa.novadigm.com_cn=device_cn=northamerica_cn=radia](#)

Object Class top
 computer
 device

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 183.
- 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 192.

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.

- 1 If necessary, set the Navigate aid to Location mode.



- 2 Navigate to the **Zone** → **Groups** container.



- 3 From the Model Administration task group, click **Add Group**.
The Add Group dialog box opens.
- 4 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.



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.

5 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.

 **Modify Group**
Test Group

The screenshot shows the 'Modify Group' dialog box for 'Test Group'. It is divided into three main sections:

- Properties:** Contains two text input fields. The 'Display Name' field contains 'Test Group' and the 'Description' field contains 'Test Group of Devices'.
- Devices:** A section titled 'No Devices Defined' with a green plus icon in the bottom right corner, indicating where to add devices.
- Browse Devices @ Groups - radia/masterzone/group:** A list view showing four groups: 'Default Group', 'New Group', 'Radia Proxy Server Group', and 'Test Group'. Each group has a search icon and a group icon. The 'Test Group' is highlighted.

At the bottom right of the dialog are three buttons: 'Modify', 'Reset', and 'Cancel'.

6 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 or import devices into it. Refer to the Import Devices or Move Device 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.

► Use this sample procedure to become familiar with using the Browse area.

To add devices to a new group

- 1 If necessary, set the Navigate aid to Location mode.



- 2 Go to the the **Groups** container for your Zone.



- 3 From the Model Administration task group, click **Add Group**.
The Add Group dialog box opens.
- 4 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.

➤ 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 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.


 **Modify Group**
Test Group



The screenshot shows the 'Modify Group' dialog box for 'Test Group'. It is divided into three main sections:

- Properties:** Contains two text input fields. The 'Display Name' field contains 'Test Group' and the 'Description' field contains 'Test Group of Devices'.
- Devices:** A section with the text 'No Devices Defined' and a green plus sign icon on the right.
- Browse Devices @ Groups - radia/masterzone/group:** A list view showing four groups: 'Default Group', 'New Group', 'Radia Proxy Server Group', and 'Test Group'. Each group has a search icon and a checkbox. The 'Test Group' is highlighted. Above the list is a toolbar with various icons, a search bar, and a dropdown menu showing 'Default...' and '1-4/4'. Below the list are three buttons: 'Modify', 'Reset', and 'Cancel'.

➤ Your groups listed in the Browse area will vary, but they will always include the Default Group and the newly created Test Group.


- 6 In the Browse Devices area, click the **Default Group** icon. 
- 7 The Browse area refreshes to display all devices that are members of your Default Group.

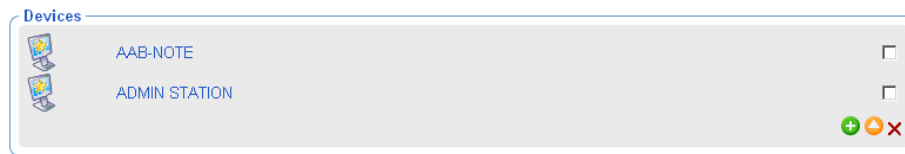
Typically, there will be a large number of devices in the Default Group, since all devices are automatically added to this group unless specified otherwise.

At a minimum, the Default Group includes the device hosting your Management Portal.

- 8 Click the check box next to at least one device in the browse area.

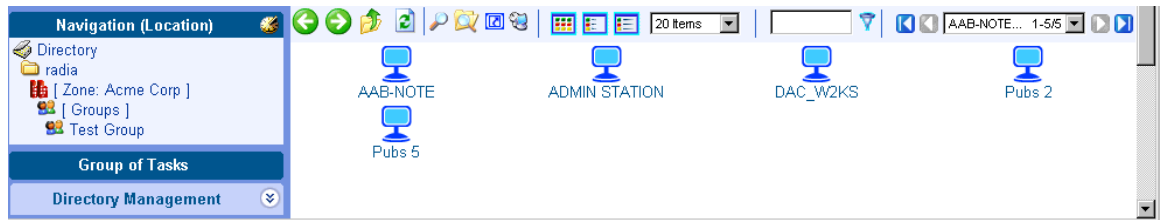


- 9 Click  on the Browse toolbar to add the selected devices to the group list.



- 10 Click the **Modify** button below the Browse toolbar to complete the task.

The devices are added to the Test Group, and the Modify Group dialog box closes. The Management Portal indicates the new location of the Test Group within the Groups container, and the Workspace lists the current devices in the group.



Moving Devices into a Group

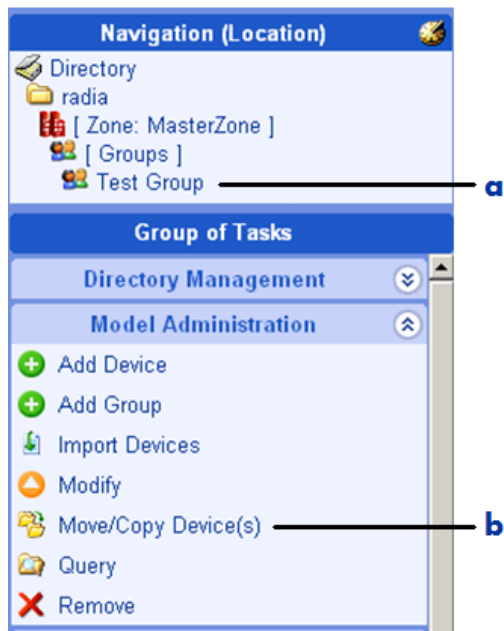
Use the Move Device task in the Model Administration task group whenever you need to switch members of an existing device group. The task is flexible and allows you to switch device group memberships, copy devices that are members of another group, or remove devices from a group's membership.

▶ To create a new group for devices, see [Adding User Groups](#) on page 183.

To remove devices from a group, see the procedure [To remove devices from a Group](#) on page 189.

To move devices into a group

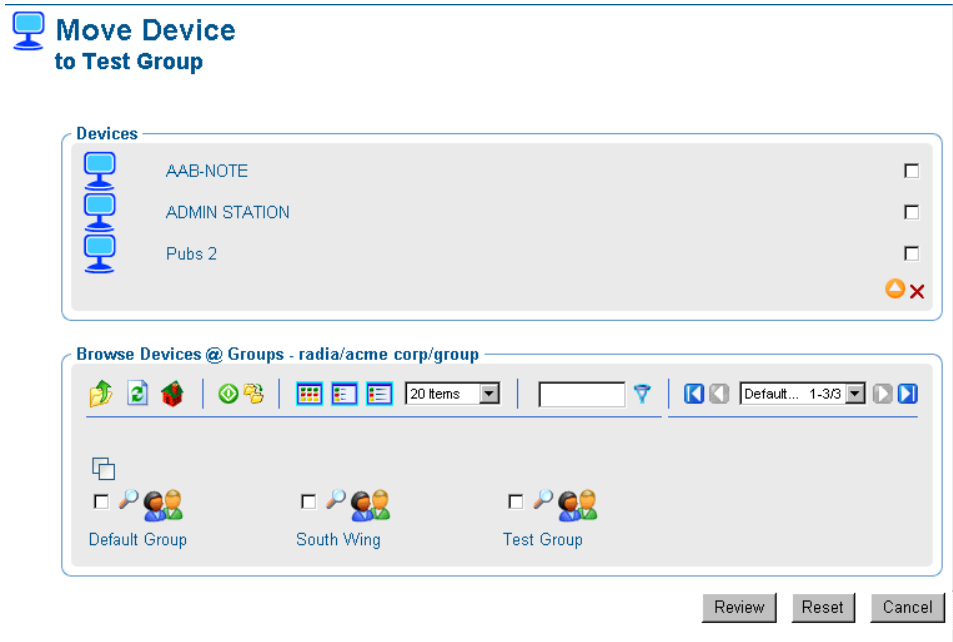
- 1 Use the Navigation aid and workspace to select the group in the Zone Groups container whose members you want to change.
- 2 In the Model Administration task group, click **Move Device**.



Legend

- a** Locate target Group requiring device changes.
- b** Click Move Device task.

The Move Device to <<selected>> Group window opens. Use this window to make any changes to the device membership for this group.



For general instructions on how to navigate and use this window, see the topic *Basic Procedures for Modifying Groups* on page 161.

3 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.



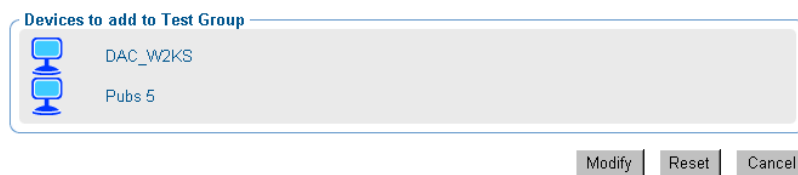
You cannot move or copy devices into Groups until they have been added to the *Devices* and *Groups* containers of your Zone. For example, you cannot move or copy devices accessed from the *Network* container—they first must be added to your Zone. This is done automatically when you use any of the *Install* 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 192, or the *Add Device* task.

4 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.
- 5 If necessary, repeat the browse and move steps until all devices and groups are listed in the Devices area.
 - 6 Click the **Review** button on the bottom of the page.

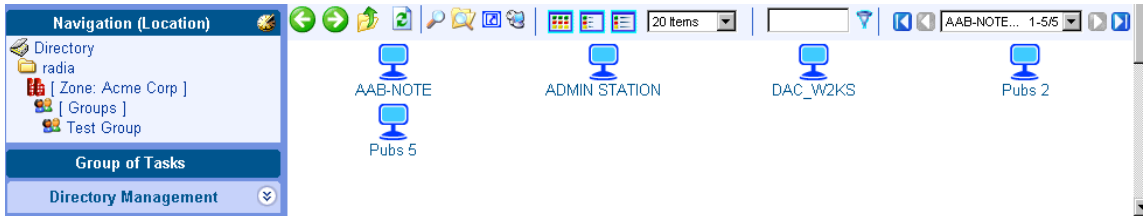
A page listing the summary of devices being added or removed from the current group opens. The following figure illustrates the devices DAC_W2KS and Pubs 5 are to be added to the Test Group.

Move Device to Test Group



- 7 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 Move Device task ends, and the workspace displays the current group members.



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 Device**.
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.

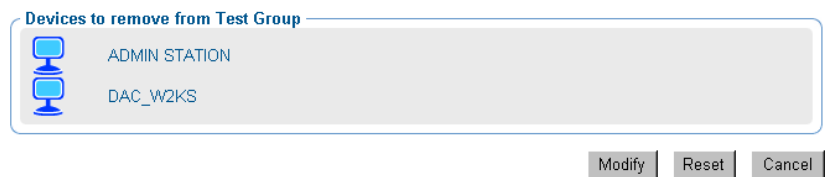
Move Device to Test Group



- 4 After selecting the devices to be deleted, click **X** to delete the checked items.
- 5 Click **Review** to review the changes.

A window opens to list the devices to remove from the group.

Move Device to Test Group



- 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 and workspace to go to the appropriate group in the Groups container.

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

The Remove Group window appears, asking you to confirm the object removal.

- 3 Click  to confirm that you want to remove the group from the 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

- 5 To first review the Child Objects, click **Selective Delete of Child Objects**. Indicate which group members are to be deleted, and click **OK**.
- 6 Click  to confirm that you want to remove the group and any groups that are selected members of it from the Management Portal Directory.

or

Click **X** 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 Device 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

- 1 Outside the 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.



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 193, 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
```

- 2 From the 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 181.

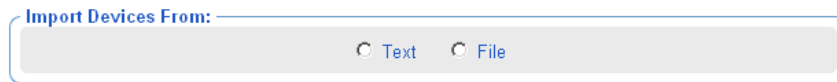


All imported devices automatically become members of the Default Group. If you import the devices into a group other than the Default Group, they will hold memberships in both groups.

- 3 Navigate to the Zone Groups container and select the Group to hold the imported devices.
- 4 From the Model Administration task group, click **Import Device**.

The Import Devices dialog box opens, prompting you to select an input method.

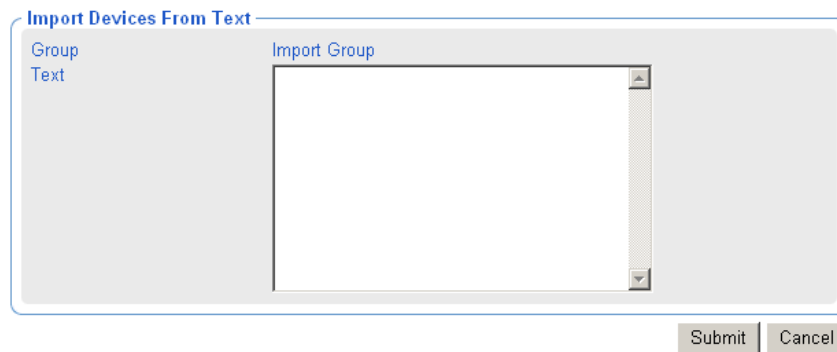
Import Devices



Import Devices From: Text File

- 5 Choose how you want to import the members of the group using one of the following methods:
 - Click **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.

Import Devices



Import Devices From Text

Group: Text

Import Group

Submit Cancel

Use the Import Group text box to type (or cut and paste) the members of the group. Enter DNS hostnames for the devices separated by one or more spaces. You can remove members from this import list in the next step.

- Click **File** on the Import Devices dialog box to select a `txt` file that you have prepared and placed in the `\etc\group` folder of the Management Portal installation directory. The following dialog box opens.



Import Devices

Import Devices From File

Group Import Group

Filename *filename.txt to be found in c:\RMPwithZones\etc\group

prod_devices.txt

qa_devices.txt

Submit Cancel

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.



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.

- 6 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 Devices into a Group](#) on page 186.
 - To move some of the devices into a new group, see [Adding Devices to a New Group](#) on page 183.

Dynamic Job Scheduling Against Groups of Devices

Jobs scheduled for the following Operations tasks are dynamic when used against a group of devices:

- Install Radia Client
- Install Management Agent
- Install Proxy Server
- Notify
- Synchronize Proxy Server
- Purge Proxy Server Dynamic Cache

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

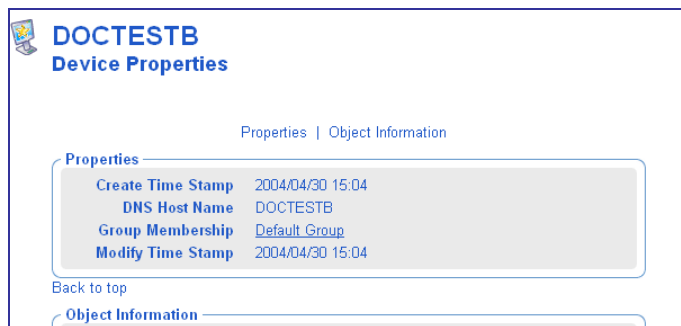
Use the Add Service task to manually add a service to a Device within your Zone. This can be done before a Radia Management Agent is installed on the Device to manually enable a connection to the service, or to enable the Management Portal tasks available for the specific service.

For example, if you manually add a service for a Proxy Server to a Device, then the Synchronize Proxy Server and Purge Proxy Server Dynamic Cache tasks become available from the Operations task group when you navigate to the service. See the following procedure for an example of how to add a service for a Proxy Server to a Device.

► Once the Radia Management Agent has been installed on a Device, its Radia-managed services will be detected automatically.

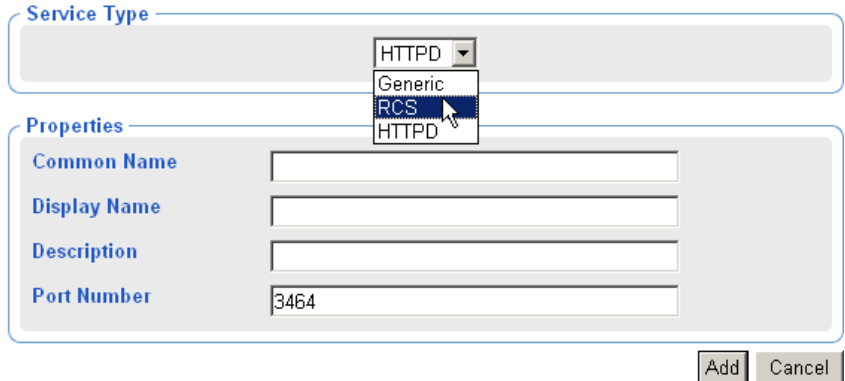
To add a service

- 1 Use the Navigation aid and workspace 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.



- In the Model Administration task group, click **Add Service**.
The Add Service dialog box opens.

Add Service




The screenshot shows the 'Add Service' dialog box. It has two main sections: 'Service Type' and 'Properties'. The 'Service Type' section has a dropdown menu currently open, showing four options: 'HTTPD', 'Generic', 'RCS', and 'HTTPD'. The 'Properties' section contains four text input fields: 'Common Name', 'Display Name', 'Description', and 'Port Number'. The 'Port Number' field contains the value '3464'. At the bottom right of the dialog, there are two buttons: 'Add' and 'Cancel'.

- 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 Configuration Server.
 - Select **HTTPD** to add a service running under the Radia Integration Service {httpd}, such a service for the Proxy Server or the 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 Proxy Server, type **rps**.

 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.

- 6 In the Description text box, type a description that will appear in the Details view of the infrastructure representation.
- 7 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 Proxy Server.


Add Service

Service Type

HTTPD ▾

Properties

Common Name	<input type="text" value="rps"/>
Display Name	<input type="text" value="RPS"/>
Description	<input type="text" value="Radia Proxy Server"/>
Port Number	<input type="text" value="3466"/>

 The following fields apply to a Service Type of RCS, only. If you are not adding a Service Type of RCS, skip to Step 12.

- 8 In the Path text box, type the exact path of `ztoptask.exe` on the RCS machine. For example:
`C:/Novadigm/ConfigurationServer/bin/ztoptask.exe.`
- 9 In the User text box, type the Username needed to use to connect to the RCS.
- 10 In the User Password text box, type the password for the user to connect to the RCS.
- 11 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.
- 12 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, click the **Start Directory Service** task in the Infrastructure task group. For details, see Stopping a on page 152.

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 161.

To modify an object

- 1 Use the Navigation aid and workspace 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.



Modify Device

Properties	
Display Name	Friendly Device Name
Description	
IP Address	
Operating System	Windows XP
Operating System Version	

Modify Reset Cancel

- 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.

- ▶ 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 and workspace to go to the appropriate object.
- 2 In the Model Administration task group, click **Remove**.
A confirmation appears in the workspace.
- 3 Click  to confirm that you want to remove the object from the 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

- 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 Management Portal Directory.

or

Click **X** 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 Blades, Enclosures and Racks

The Chassis container extends the device-based Radia infrastructure zone architecture to include the server blades, blade enclosures (both stand-alone and rack-mounted), and racks in a zone. The Chassis container also includes enclosure configurations, whose set of pre-defined entries can be extended, as necessary, to permit logical groupings of the blade enclosures in any enterprise.

Figure 23 Chassis Container Contents

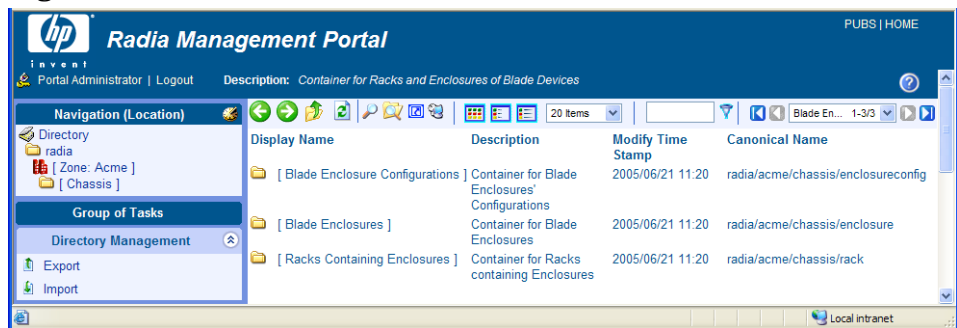


Table 13 below lists the Chassis container contents and Table 14 on page 201 lists the related Cross-References containers for these objects.

Table 13 Chassis Container Objects

Chassis Container Group	Contents and Notes
Racks Containing Enclosures	<p>Rack instances containing enclosures.</p> <ul style="list-style-type: none"> Physical racks IDs must be unique within all racks in a Zone. Multiple enclosure instances may be linked to a single rack.

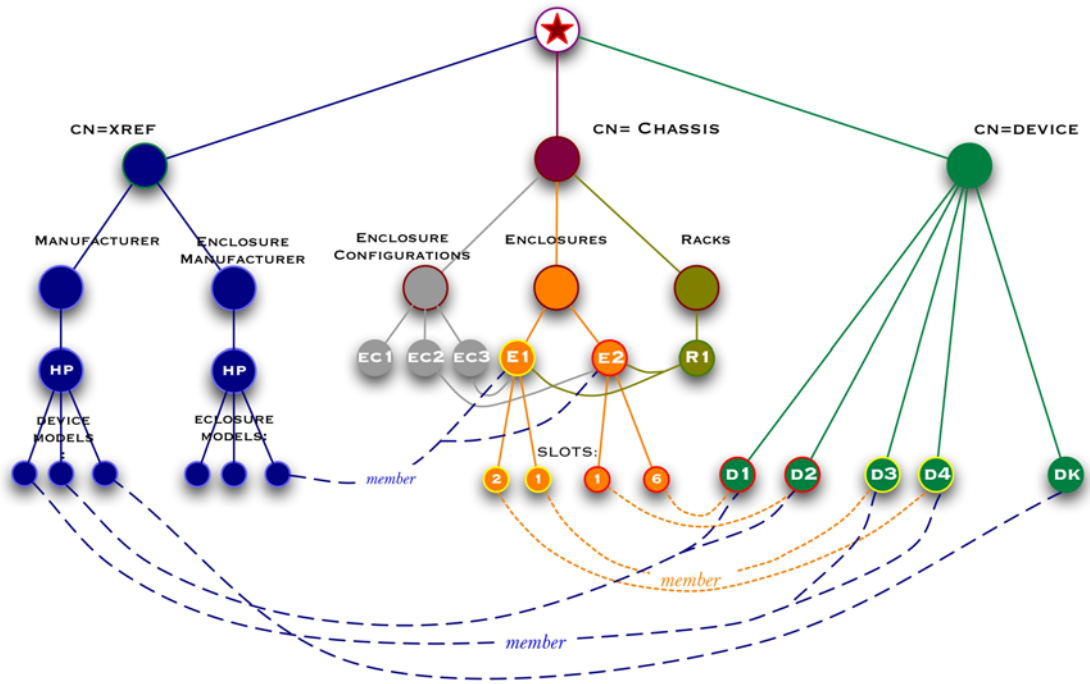
Chassis Container Group	Contents and Notes
Blade Enclosures	<p>Planned or actual enclosure instances.</p> <p>Each instance contains a set of slots. Slots are either <i>occupied</i> by a server blade or <i>empty</i>.</p> <ul style="list-style-type: none"> • Enclosure instance names must be unique within a zone. HP recommends using names that are independent of their rack location, to allow for relocation. • Enclosures can be linked to an Enclosure Manufacturer and Model Number (in the Cross References groups). • Enclosures can be linked to a single enclosure configuration and a single rack instance. • Occupied slots are linked to a managed blade device.
Blade Enclosure Configurations	<p>Predefined enclosure configurations (an enclosure model number and a predefined set of slots and server blades).</p> <ul style="list-style-type: none"> • To add configurations, see the Add Enclosure Configuration task on page 203.

Table 14 Cross References Container Groups for Blade Enclosures

Cross References Group	Group Objects	Description
Enclosure Manufacturer	Manufacturers of blade enclosures, such as HP, IBM	Members include enclosure instances made by that manufacturer.
Enclosure Models	Models of blade enclosures, such as: HP Signal Blade	Members include enclosure instances with that model number.

Figure 24 on page 202 presents an architectural model for the server blade devices, containers, and racks in a zone. Notice the model emphasizes the relationships between these entities, allowing for a variety of policy assignment types. For example, policy assignments can be based on physical groupings (rack policies), logical configurations (policies for pre-defined enclosure configurations), as well as the manufacturers and model numbers of the enclosure instances. The openness of the underlying architecture allows solution architects to assign policies practically anywhere, and enables implementations that fit the particular requirements of any modern enterprise.

Figure 24 Architectural model for server blades, enclosures and racks



- 1 Server blades in your Zone are devices with membership links to their respective enclosure slots within the Chassis → Enclosures container. For example, Device D1 is linked to Slot 6 of the enclosure E2.
- 2 Server blade devices also hold membership links to the appropriate Manufacturer group in the Cross References containers. Device D1 is a member of the HP Device Models listed in the Cross-References → Manufacturers container.
- 3 The enclosures defined in the Chassis container can hold memberships in a single enclosure configuration, enclosure model, or rack. For example, enclosure E2 is linked to the configuration EC2, an HP Enclosure Model (within the Cross References → Enclosure Manufacturers container) and rack R1.

About the Predefined Blade Enclosure Configurations

The Blade Enclosure Configurations container includes several predefined configurations for the HP Signal Backplane enclosures as described in Table 15 below.

To view these configurations, navigate to the **Zone → Chassis → Blade Enclosure Configurations** location in the Management Portal.

Table 15 Provided Blade Enclosure Configurations

Displayname	Description
HP Sgnl Backplane/BL20	8 HP/BL20 Blade Slots
HP Sgnl Backplane/BL30	16 HP/BL20 Blade Slots
HP Sgnl Backplane/BL40	2 HP/BL40 Blade Slots

If your environment uses different blade enclosure configurations, add the configurations you require. For details, see [Adding an Enclosure Configuration](#) below.

Adding an Enclosure Configuration

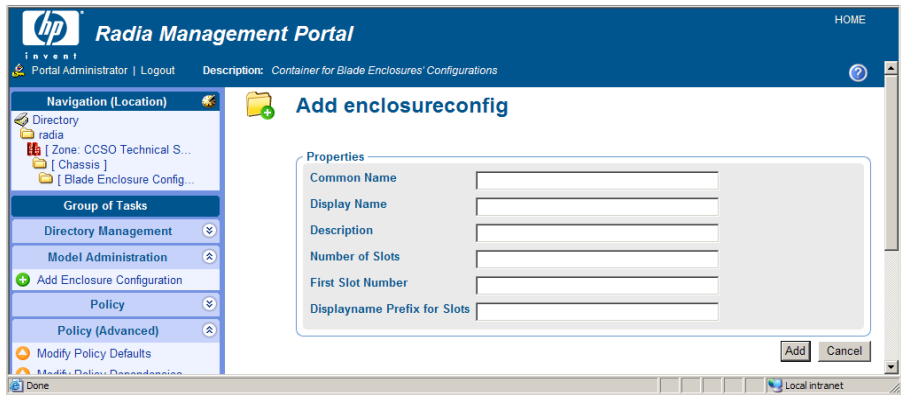
Use the Add Enclosure Configuration task in the Model Administration task group to define a new configuration for a blade enclosure in the **Zone → Chassis → Blade Enclosure Configurations** container.

Policy may be assigned to individual slots of the enclosure or to the enclosure configuration as a whole. The enclosure instances in your Zone that have an enclosure configuration added to their properties will be members of the Enclosure Configuration group, and will inherit the policy applied to the configuration. Likewise, enclosure slots will inherit policies that are applied to their respective slots of their assigned enclosure configuration.

To add an enclosure configuration

- 1 Navigate to the **Zone → Chassis → Blade Enclosure Configurations** group container.
- 2 Click **Add Enclosure Configuration** from the Model Administration task group.

The Add enclosure config window opens.



- 3 Complete the Properties for the enclosure configuration using the following guidelines.

Common Name – Required. Common names must be unique among all enclosure configurations in the same Zone.

Display Name – Name that displays next to the object in the Portal. Defaults to the common name. HP recommends using display names that are also unique among all enclosure configurations in the same Zone.

Description – Optional description of the enclosure configuration, such as the number of slots of each server type.

Number of Slots – Defines the number of slots to create for this enclosure configuration.

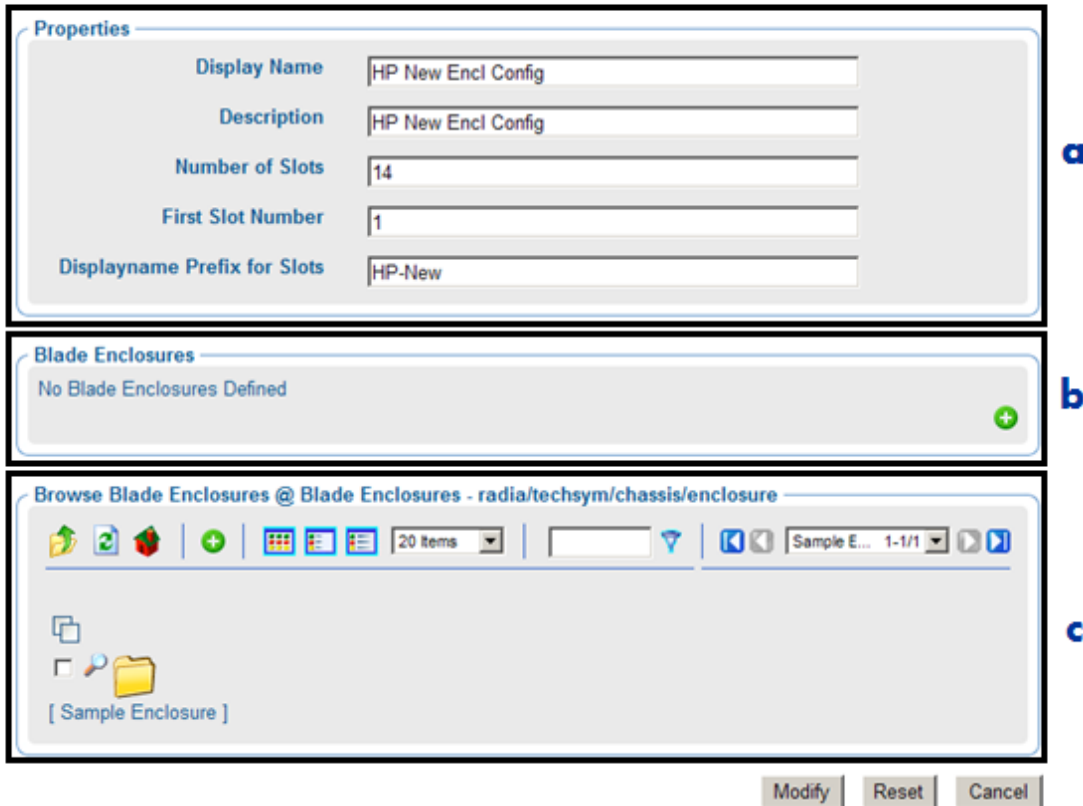
Fist Slot Number – The first slot number of an enclosure is either 1 or 0 (zero). The default value is 1. Enter 0 if this enclosure assigns 0 to the first slot number.

Displayname Prefix for Slots – Enter a prefix to easily identify each slot number for this configuration. Each slot for the configuration will be identified as the prefix entered here followed by a slot number. The figure below shows an example of slot display names which were given a prefix of "HP-New".

- 4 Click **Add**.

The Modify Enclosure Configuration window opens.


Modify Enclosure Configuration HP New Encl Config



Properties

Display Name	HP New Encl Config
Description	HP New Encl Config
Number of Slots	14
First Slot Number	1
Displayname Prefix for Slots	HP-New

Blade Enclosures

No Blade Enclosures Defined 

Browse Blade Enclosures @ Blade Enclosures - radia/techsym/chassis/enclosure

20 Items | Sample E... 1-1/1

[Sample Enclosure]

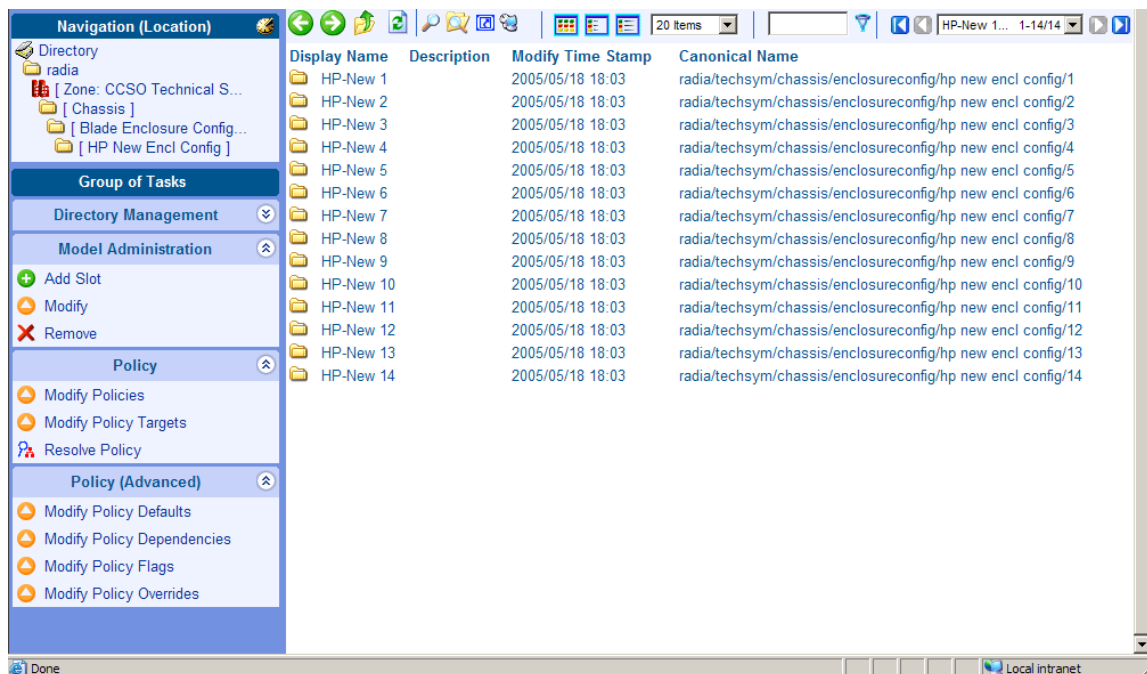
Modify Reset Cancel

Legend

- a** Properties displayed in the top area reflect your previous entries, and can be modified here, if necessary.
- b** Blade Enclosures area displays Blade Enclosures in your Zone that are defined as members of this configuration. Currently, this configuration has no members.
- c** Browse Blade Enclosures area is used to select blade enclosures to define as members of this configuration.
 - 5 If desired, modify the values of any of the properties.
 - 6 To define existing enclosures in your Zone as members of this configuration, use the Browse Blade Enclosures area (c) to add members to the Blade Enclosures area (b). See Using the Browse and Modify Window on page 162 for more information on how to use this area.

- Click **Modify** to create the Blade Enclosure Configuration.

The new configuration is added to the Blade Enclosure Configuration container. The configuration contains instances of each slot defined in the previous task. In the image below, a configuration was added with 14 slots.



- From this location, you can also add slots to the configuration. To do this, click **Add Slot** from the Model Administration task group.

The task to add an enclosure configuration is complete.

Adding an Enclosure

Use the Add Enclosure task in the Model Administration task group to create instances for the existing and/or planned enclosures in your Zone. This is performed from the **Zone → Chassis → Enclosures** group container.

When defining an enclosure, be aware of the following:

- If you base the enclosure on a predefined enclosure configuration, the new enclosure automatically includes the same number of slots as the Enclosure Configuration. (This is done on the Modify Enclosure window.)

Defining an enclosure configuration for the enclosures in your zone is the recommended approach for applying policies.

- If you add manufacturer and model details for the enclosure, you will be able to cross-reference the enclosure from the **Cross References** → **Enclosure Manufacturers** groups. In general, applying policies to the groups within the enclosure manufacturers containers have limited use, since all enclosures of a specific model will have the same set of policies.
- Defining a configuration for the enclosure also makes the enclosure a member of the selected enclosure configuration group. The membership enables any policies applied to the configuration to be inherited by the enclosure instance, as well as any policies applied to a slot number of the configuration to be applied to the same slot number of the enclosure instance.



Blade enclosure names must be unique within a zone.
Enclosure names should be independent of the racks in which they are mounted.

To add an enclosure

- 1 Navigate to the **Zone** → **Chassis** → **Blade Enclosures** container.
- 2 Click **Add Enclosure** in the Model Administration task group.

The Add enclosure window opens.



Add enclosure

Properties

Common Name	<input type="text"/>
Display Name	<input type="text"/>
Description	<input type="text"/>
Enclosure Manufacturer	<input type="text"/>
Enclosure Model	<input type="text"/>
Number of Slots	<input type="text"/>
First Slot Number	<input type="text"/>

- 3 Complete the Properties group fields using the following guidelines.

Common Name – Required. Common names for enclosures must be unique among all enclosures in the same Zone. HP recommends using

names that are independent of the racks where the enclosures are mounted.

Display Name – Name that displays next to the object in the Portal. Defaults to the common name.

Description – Optional description of the enclosure.

Enclosure Manufacturer – The manufacturer of the enclosure, such as HP or IBM. Enter this field to create a link to the Cross References container for Enclosure Manufacturers. Match the name exactly if the manufacturer is already listed in the Cross References containers.

Enclosure Model – The specific model of enclosure for the given manufacturer. To manually create a link to the Cross References container for Enclosure Manufacturers, enter a model name for the enclosure. Match the name exactly if the model is already listed in the Cross References containers.

Number of Slots – Defines the number of slots to create for this enclosure. Leave blank to have the slot numbers automatically defined from an enclosure configuration (defined on the next Modify Blade Enclosure dialog).

First Slot Number – The first slot number of an enclosure is either 1 or 0 (zero). The default value is 1. Enter 0 if this enclosure assigns 0 to the first slot number.

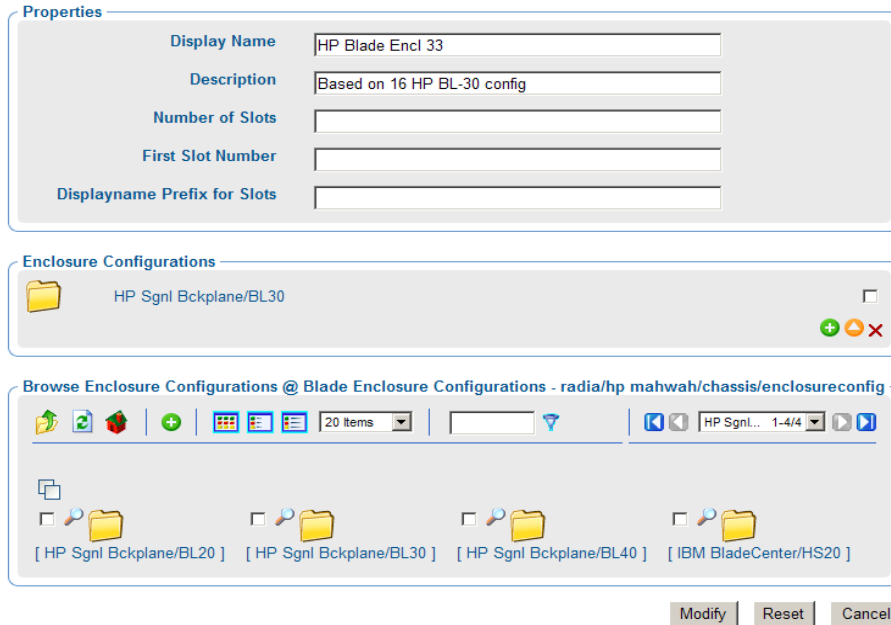
4 Click **Add**.

The Modify Blade Enclosure window opens.

5 Optionally, modify any entry in the Properties area for Display Name, Description, Number of Slots, or First Slot Number. Definitions for these fields are given earlier in this procedure.

6 Slot names are automatically generated using the format "Slot n". To add a prefix to these slot names, enter the prefix in the Displayname Prefix for Slots text area.

Modify Blade Enclosure HP Blade Encl 33



Properties

Display Name: HP Blade Encl 33

Description: Based on 16 HP BL-30 config

Number of Slots:

First Slot Number:

Displayname Prefix for Slots:

Enclosure Configurations

HP Sgnl Bckplane/BL30


Browse Enclosure Configurations @ Blade Enclosure Configurations - radia/hp mahwah/chassis/enclosureconfig

20 Items | HP Sgnl... 1-4/4

[HP Sgnl Bckplane/BL20] [HP Sgnl Bckplane/BL30] [HP Sgnl Bckplane/BL40] [IBM BladeCenter/HS20]

Modify Reset Cancel


The lower areas on the Modify dialog box allow you to define an enclosure configuration for this enclosure instance. Defining a configuration:

- Adds the Slots defined in the configuration to the enclosure instance.
 - Makes this enclosure a member of the selected Enclosure Configuration group. The membership enables any policies applied to the configuration to be inherited by the enclosure instance.
- 7 To optionally define an enclosure configuration for the enclosure, use these steps:
- a Slot names are automatically generated using the format "Slot n". To add a prefix to these slot names, enter the prefix in the Displayname Prefix for Slots text area.
 - b Use the Browse Enclosure Configurations area to select the target configuration on which to base this enclosure. See Using the Browse and Modify Window on page 162 for more information on how to use the Browse area features.
 - c After selecting a configuration from the Browse area, click  to add it to the Enclosure Configurations area.

- Click **Modify** at the bottom of the page.

The Enclosure configuration instance is created in that group. If Slot numbers were entered or defined from an existing configuration, the workspace displays the slots created for the enclosure.



- Click  on the toolbar to view the Blade Enclosure Properties.



HP Blade Enclosure 33 Blade Enclosure Properties

Properties | Object Information

Properties

Create Time Stamp	2005/05/19 17:42
ds.enclosuremodeldn	HP_Blade_Enclosure
Enclosure Configuration	HP_Sgnl_Bckplane/BL30
Enclosure Manufacturer	HP
Enclosure Model	sgnl bckplane
Modify Time Stamp	2005/05/19 18:03

Back to top

Object Information

Display Name	HP Blade Enclosure 33
Description	Based on 16 HP BL-30 config
Common Name	HP_BE_033
X500 Distinguished Name	cn=hp_be_033, cn=enclosure, cn=chassis, cn=hp mahwah, cn=radia
Object Class	top container enclosure

Back to top

Notice the properties for an enclosure indicate the Enclosure Configuration defined for it. Optionally, click on the linked entry to view the configuration.

This completes the entry for the enclosure instance of HP Blade Enclosure 33. Its configuration of 16 slots is based on the Enclosure Configuration named HP Sgnl Bckplane/BL30.

This enclosure instance is linked to that enclosure configuration, and will inherit any policies applied to the configuration.

Applying Policy to Blades, Enclosures and Racks

Policy may be applied to many entities related to the blades, enclosures and racks in your zone. There are several approaches that are discussed on the topics that follow.

- Before applying policy, however, you must first add a LINKS entry to the Management Portal configuration file, `rmp.cfg`, as discussed in [Enabling Policy Configurations for Blades, Enclosures and Racks](#) below.
- After enable the LINKS in the `rmp.cfg` file, use the tasks in the Policy and Advanced Policy tasks groups to assign policy that will apply to the server blade devices in your zone. For details on how to perform these tasks, see [Using RMP to Assign Policy through an LDAP Directory](#) on page 102.

Enabling Policy Configurations for Blades, Enclosures and Racks

Resolution of policy applied to the objects related to blades, enclosures and racks in a Zone requires a LINKS entry in the `rmp.cfg` file, as shown below:

```
rmp::init {
    LINKS { enclosureslotnumberdn enclosuremodeldn
           enclosureconfigdn rackdn osdevicearchitecturedn }
}
```

The specific set of links to include in the LINKS entry will vary for each enterprise, depending on which entities and containers have been used for policy. Table 16 on page 212 describes the policy link that is enabled when the value is added to the LINKS list. For example, if you have not assigned policy to the rack instances in your Zone, `rackdn` may be omitted from the set of LINKS shown above.

Table 16 Policy Resolution Links to Define in RMP.CFG

LINKS Parameter	Description
enclosureslotnumberdn	Links the blade device to the enclosure slot.
enclosuremodeldn	Links the blade device to the enclosure model.
enclosureconfigdn	Links the enclosure to its enclosure configuration.
osdevicearchitecturedn	Links the device to its device architecture (which is added by default).
rackdn	Links the enclosure to its rack (when policies are assigned to racks).

Assigning Policy Based on Enclosure Model Types

To assign policies based on enclosure manufacturer model types, do the following:

- 1 Modify the `rmp.cfg` file to include the necessary policy links. See [Enabling Policy Configurations for Blades, Enclosures and Racks](#) on page 211.
- 2 If available, enable the server blade devices in your Zone to report the model of the enclosure in which the blade occupies. When this attribute is reported, it is used for cross-referencing of the enclosures in the Enclosure Manufacturer cross-references container.
- 3 Optionally, add slots to the models in the Enclosure Manufacturer containers. This allows you to define policy for some or all slots for a given Enclosure Manufacturer model number.
- 4 Establish a set of enclosure configurations for your Zone.

Assigning Policy Based on Enclosure Configurations

To assign policies based on predefined enclosure configurations, do the following:

- 1 Modify the `rmp.cfg` file to include the necessary policy links. See [Enabling Policy Configurations for Blades, Enclosures and Racks](#) on page 211.

- 2 Establish a set of enclosure configurations that reflect the various configurations of server-blades in the enclosures in your enterprise. Use the predefined configurations or add your own.
- 3 For each enclosure instance in your enterprise, define it as member of an enclosure configuration. This can be done from the Modify Enclosure Configuration window using the Browse Blade Enclosures area. See the Modify Enclosure Configuration window on page 205 for details.
 - ▶ Once an enclosure is defined as a member of the enclosure configuration instance, all the slots of the enclosures have member of/member connections to the corresponding slots of the respective configuration.
- 4 Apply policy to the Enclosure Configuration itself, or to a Slot of the Configuration.

The enclosure instances and slot instances will inherit the policies of the enclosure configuration to which it is linked. A server that occupies a slot number in the enclosure will also inherit policy that is applied to the same-numbered slot in the enclosure configuration.

Configuring Task Groups

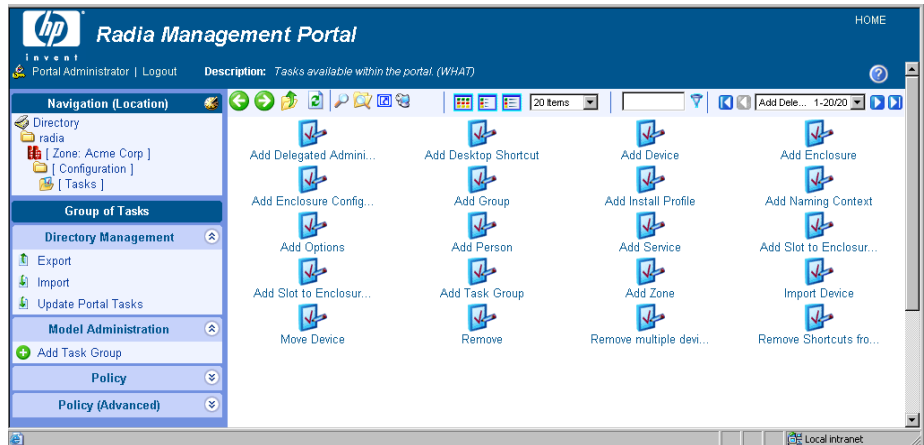
The Taskbar contains logical groups of tasks (called task groups). A task is an activity that a person performs to initiate a job. The available tasks vary based on the selected Authority, as well as your role. In addition to the standard task groups (see Taskbar on page 70 for more information), you can create your own task groups.

Adding Task Groups

To add a task group

- 1 Use the Navigation aid and workspace to go to **Directory** → **Zone** → **Configuration** → **Tasks** location.

The workspace displays the current set of Tasks and Task Groups. Task Groups are represented by the yellow folder icons; individual Tasks by blue page icons.



- In the Model Administration task group, click **Add Task Group**.
The Add Task Container dialog box opens.


 **Add tasks**

Properties

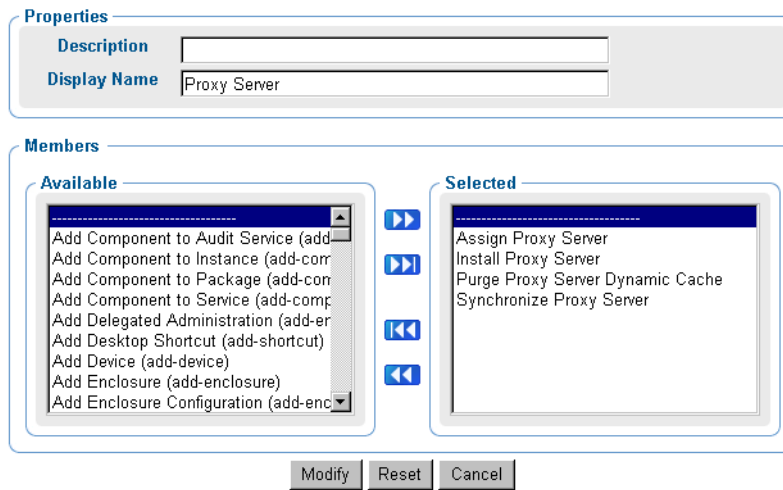
Common Name

Description

Display Name

- In the Common Name text box, type a name for the task group object.
 -  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 Description text box, type a description that will appear in the Details view.
- In the Display Name text box, type a name for the task group. If omitted, the Common Name is used.
- Click **Add**.
The Modify Task Container dialog box opens.

Modify Task Container



Properties

Description

Display Name

Members


Available

- Add Component to Audit Service (add-
- Add Component to Instance (add-corr
- Add Component to Package (add-con
- Add Component to Service (add-comp
- Add Delegated Administration (add-er
- Add Desktop Shortcut (add-shortcut)
- Add Device (add-device)
- Add Enclosure (add-enclosure)
- Add Enclosure Configuration (add-enc

Selected

- Assign Proxy Server
- Install Proxy Server
- Purge Proxy Server Dynamic Cache
- Synchronize Proxy Server

Modify Reset Cancel

- 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 task group.

- 10 In the toolbar above the workspace, click the View Properties icon .

The Task Container Properties for the new task group opens. As an example, the following figure shows the properties for a new Proxy Server task group.

Proxy Server Task Container Properties

Properties | Object Information

Properties

Create Time Stamp	2005/12/16 19:06
Members	Assign Proxy Server Install Proxy Server Purge Proxy Server Dynamic Cache Synchronize Proxy Server
Modify Time Stamp	2005/12/16 19:10

[Back to top](#)

Object Information

Display Name	Proxy Server
Common Name	Proxy Server Tasks
X500 Distinguished Name	cn=proxy_server_tasks, cn=task, cn=config, cn=acme corp, cn=radia
Object Class	top groupOfNames nvdTaskGroup

[Back to top](#)

- 11 To see this new Task Group, use the Navigation aid and workspace to go to the **Zone** → **Groups** → **Default Group** location.

In the Taskbar, your new task group, such as Proxy Server (as shown in the next figure), is available. Task Groups are listed alphabetically.



If you would like to configure the 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 and workspace 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.



Modify Task Container

Properties

Description

Display Name

Members

Available

- Add Component to Audit Service (add-cor...
- Add Component to Instance (add-compon...
- Add Component to Package (add-compor...
- Add Component to Service (add-compone...
- Add Delegated Administration (add-entitle...
- Add Desktop Shortcut (add-shortcut)
- Add Device (add-device)
- Add Enclosure (add-enclosure)
- Add Enclosure Configuration (add-enclosu...

Selected

- Assign Proxy Server
- Install Proxy Server
- Purge Proxy Server Dynamic Cache
- Synchronize Proxy Server

Modify Reset Cancel

- 4 Make any necessary changes. For detailed information about configuring task groups, see [Adding Task Groups](#) on page 213 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

- 1 Use the Navigation aid and workspace to go to **Directory** → **Zone** → **Configuration** → **Tasks**.
- 2 In the workspace, select the task group that you want to remove.
- 3 In the Model Administration task group, click **Remove**.

The Remove Task Container dialog box opens, asking you to confirm the object removal.

- 4 Click  to confirm that you want to remove the task group from the Management Portal Directory.

or


Click  to indicate that you do not want to remove the task group.

Configuring Delegated Administration

Use the 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 Management Portal contains several standard roles. To view the existing roles in the navigation aid go to **Directory → Zone → Configuration**. Then, in the workspace, click **Delegated Administration**.

The following roles are used to perform Core Management Portal operations:

- **Global Default Policy**
Allows the 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 Management Portal administrator to access all tasks in all Scopes of Action.
 This role cannot be modified in order to prevent you from being locked out of the 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

 The Figures in this procedure do not reflect the latest changes to the Management Portal.

- 1 Use the Navigation aid and workspace to go to the **Directory → Zone → Configuration** location.
- 2 In the workspace, click **Delegated Administration**.
- 3 In the Model Administration task group, click **Add Delegated Administration**.

The Add Delegated Administration dialog box opens.

Add Delegated Administration

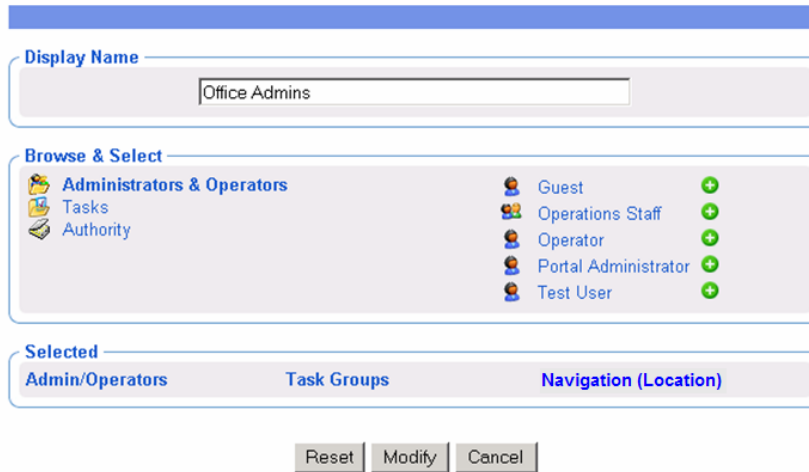


The dialog box has a title bar with the word "Properties" in blue. Below the title bar, there is a label "Display Name" in blue next to a text input field. At the bottom right of the dialog box, there are three buttons: "Add", "Reset", and "Cancel".

- 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.

Modify Delegated Administration



Display Name: Office Admins

Browse & Select


- Administrators & Operators
- Tasks
- Authority

- Guest
- Operations Staff
- Operator
- Portal Administrator
- Test User

Selected

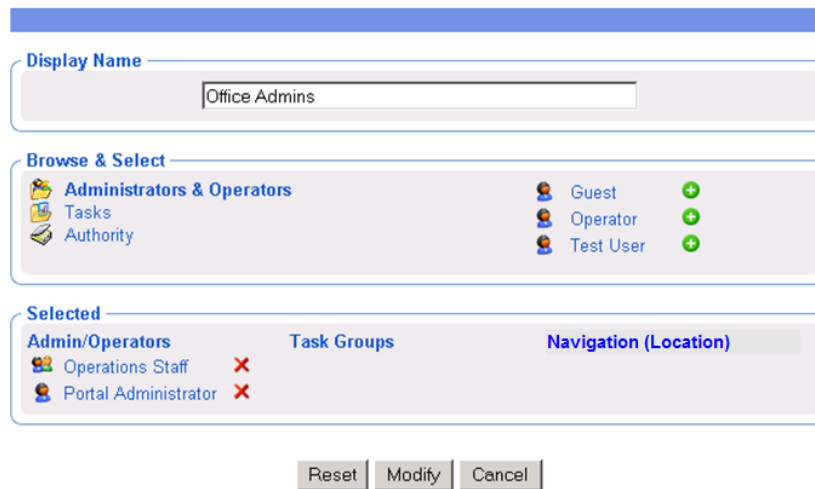
Admin/Operators Task Groups Navigation (Location)

Reset Modify Cancel

- 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 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.

Modify Delegated Administration



Display Name: Office Admins

Browse & Select

- Administrators & Operators
- Tasks
- Authority

- Guest
- Operator
- Test User

Selected

Admin/Operators Task Groups Navigation (Location)

Operations Staff ✗

Portal Administrator ✗

Reset Modify Cancel

If you want to remove an administrator or operator from the list of selected items, click .

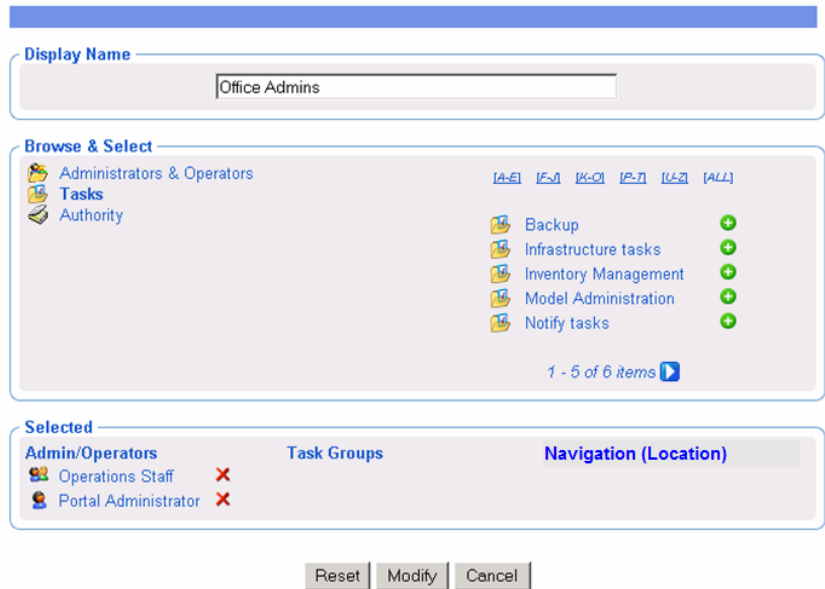
Next, select the tasks that you want to include in this role.

- 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.



Modify Delegated Administration



Display Name: Office Admins

Browse & Select

Administrators & Operators [A-E] [F-I] [K-O] [P-T] [U-Z] [ALL]

Tasks

Authority

Backup +

Infrastructure tasks +

Inventory Management +

Model Administration +


Notify tasks +


1 - 5 of 6 items

Selected

Admin/Operators	Task Groups	Navigation (Location)
Operations Staff		
Portal Administrator		

Reset Modify Cancel

- 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 in the Task Groups column.



Modify Delegated Administration

Display Name

Browse & Select

Administrators & Operators	Backup
Tasks	Infrastructure tasks
Authority	Inventory Management
	Model Administration

Selected

Admin/Operators	Task Groups	Navigation (Location)
Operations Staff	Notify tasks	
Portal Administrator	Operations	

Reset Modify Cancel

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.



Modify Delegated Administration

Display Name

Browse & Select

Administrators & Operators [A-E] [F-I] [K-O] [P-T] [U-Z] [ALL]

Tasks

Authority

- Administrators & Operators +
- Delegated Administration +
- Entire Network +
- Jobs +
- Radia Subscriber Information +

1 - 5 of 6 items ▶

Selected

Admin/Operators	Task Groups	Navigation (Location)
Operations Staff <input checked="" type="checkbox"/>	Notify tasks <input checked="" type="checkbox"/>	
Portal Administrator <input checked="" type="checkbox"/>	Operations <input checked="" type="checkbox"/>	







Reset Modify Cancel

- 12 If you do not see the container that you want to select, click below the list. 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**.





Modify Delegated Administration

Display Name

Browse & Select

<ul style="list-style-type: none">  Administrators & Operators  Tasks  Authority  Entire Network 	<ul style="list-style-type: none">  Microsoft Windows Network +  Novadigm-managed Infrastructure +
--	--

Selected











Admin/Operators	Task Groups	Navigation (Location)
 Operations Staff ✗	 Notify tasks ✗	
 Portal Administrator ✗	 Operations ✗	



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**.

Modify Delegated Administration





Display Name

Browse & Select

<ul style="list-style-type: none">  Administrators & Operators  Tasks  Authority  Entire Network <li style="padding-left: 20px;"> Microsoft Windows Network 	<div style="font-size: small; margin-bottom: 5px;"> [A-Z] [A] [B] [C] [D] [E] [F] [G] [H] [I] [J] [K] [L] [M] [N] [O] [P] [Q] [R] [S] [T] [U] [V] [W] [X] [Y] [Z] [ALL] </div> <ul style="list-style-type: none">  BETADOMAIN +  CLARIZIOWG +  CLTLAB +  CONNECTIONS2001 +  EDUCATION1 +
---	---


1 - 5 of 12 items  

Selected

Admin/Operators	Task Groups	Navigation (Location)
 Operations Staff ✗	 Notify tasks ✗	
 Portal Administrator ✗	 Operations ✗	

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 in the Authority column.

Modify Delegated Administration

Display Name
Office Admins

Browse & Select

Administrators & Operators
Tasks
Authority
Entire Network
Microsoft Windows Network


BETADOMAIN
CLARIZIOWG
CLTLAB
CONNECTIONS2001
EDUCATION1

1 - 5 of 12 items

Selected

Admin/Operators	Task Groups	Navigation (Location)
Operations Staff	Notify tasks	
Portal Administrator	Operations	

Reset Modify Cancel

If you want to remove an Authority from the list of selected items, click .

- 15 Click **Modify**.

The Delegated Administration Properties dialog box opens.

View Properties Delegated Administration

Office Admins

Who	What	Navigation (Location)
Operations Staff	Notify tasks	world/microsoft/betadomain
Portal Administrator	Operations	

Modifying Delegated Administration Roles

To modify a delegated administration role

- 1 Use the Navigation aid and workspace 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.



Modify Delegated Administration

Display Name: Office Admins

Browse & Select

Administrators & Operators | Tasks | Authority | Entire Network | Microsoft Windows Network

CLARIZOWG +
CLTLAB +
CONNECTIONS2001 +
EDUCATION1 +
NOVADIGM +

1 - 5 of 11 items

Selected

Admin/Operators	Task Groups	Navigation (Location)
Operations Staff ✖	Notify tasks ✖	BETADOMAIN ✖
Portal Administrator ✖	Operations ✖	

Reset Modify Cancel

- 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 and workspace 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.
- 4 Click  to confirm that you want to remove the Delegated Administration role from the 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 and workspace 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.

Delegated Administration Properties

Properties		
Name	What	Navigation (Location)
 Infrastructure Administration	 Infrastructure	 radia/northamerica  radia/northamerica/user  radia/northamerica/config/task

- 4 Click any link in the table to view the properties for that object.

Configuring Administrators and Operators

The Administrators & Operators container in the 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 227 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.



External LDAP Authentication is disabled for all users by default. To enable it, see [Configuring for External LDAP Authentication](#) on page 153 for details.

To add a user

- 1 Use the Navigation aid and workspace to go to the **Directory** → **Zone** location.
- 2 In the workspace, click the **Administrators & Operators** container.
- 3 In the Model Administration task group, click **Add Person**.


The Add Person dialog box opens.




Add person



Properties

User ID	<input type="text"/>
Description	<input type="text"/>
Display Name	<input type="text"/>
User Password	<input type="password"/>
External User ID	<input type="text"/>
External authentication?	<input type="radio"/> on <input type="radio"/> off


- 4 In the User ID text box, type the user name.
 -  The User ID for the person must be unique. If you attempt to create an object for a person 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 Management Portal.
- 7 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 \.
- 8 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.
 -  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 153.
- 9 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 Portal.
 - Click **off** to disable external authentication for this user.
 - Click **on** to enable external authentication for this user.
- 10 Click **Add**.

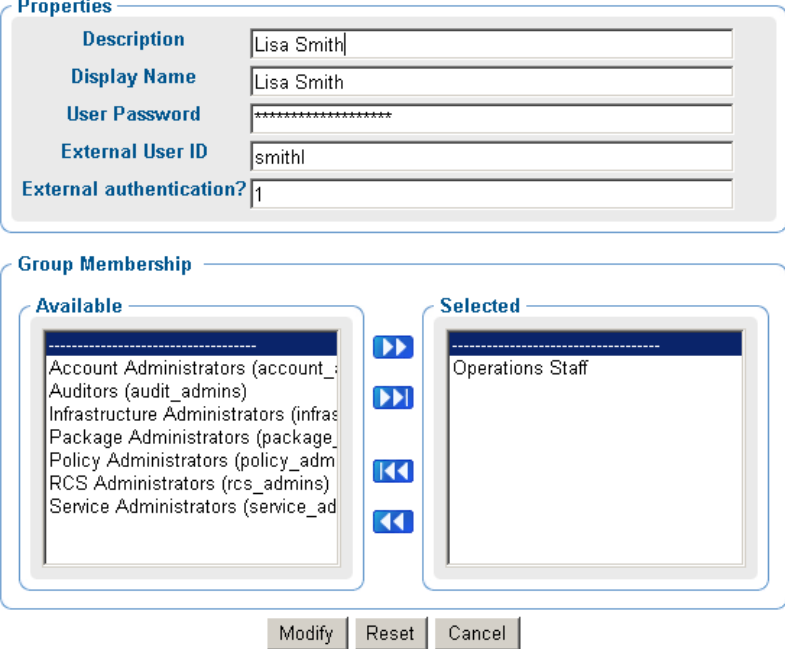
The Modify Person dialog box opens.

 -  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.
- 11 From the Available list, select one or more groups to add the user to.
- 12 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 279 for more information about how to use this dialog box.

Modify Person



Properties

Description	Lisa Smith
Display Name	Lisa Smith
User Password	*****
External User ID	smithl
External authentication?	1

Group Membership

Available

- Account Administrators (account_
- Auditors (audit_admins)
- Infrastructure Administrators (infras
- Package Administrators (package_
- Policy Administrators (policy_adm
- RCS Administrators (rcs_admins)
- Service Administrators (service_ad

Selected

- Operations Staff

Modify Reset Cancel

13 Click **Modify**.

The Person Properties dialog box opens.

 **Lisa Smith**
Person Properties

[Properties](#) | [Object Information](#)

Properties

Create Time Stamp	2004/09/27 18:47
External authentication?	1
External User ID	smithl
Group Membership	Operations Staff
Modify Time Stamp	2004/09/27 18:53
User ID	LSmith01

[Back to top](#)

Object Information

Display Name	Lisa Smith
Description	Lisa Smith
X500 Distinguished Name	uid=lsmith01, cn=user, cn=acmecorp, cn=radia
Object Class	top person

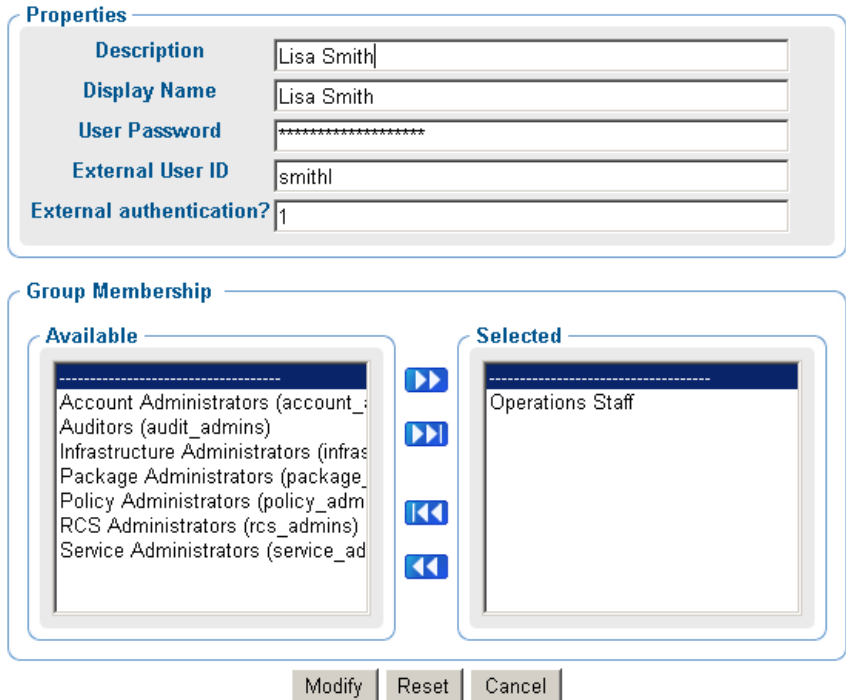
[Back to top](#)

Modifying Users

To modify a user

- 1 Use the Navigation aid and workspace 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.

Modify Person



Properties

Description	Lisa Smith
Display Name	Lisa Smith
User Password	*****
External User ID	smithl
External authentication?	1

Group Membership

Available

- Account Administrators (account_
- Auditors (audit_admins)
- Infrastructure Administrators (infras
- Package Administrators (package
- Policy Administrators (policy_adm
- RCS Administrators (rcs_admins)
- Service Administrators (service_ad

Selected

- Operations Staff

Modify Reset Cancel

- 5 Make any necessary changes. For detailed information about configuring users, see Adding Users on page 230.

➤ 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 authentication 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 and workspace 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.
- 5 Click  to confirm that you want to remove the user from the Management Portal Directory.

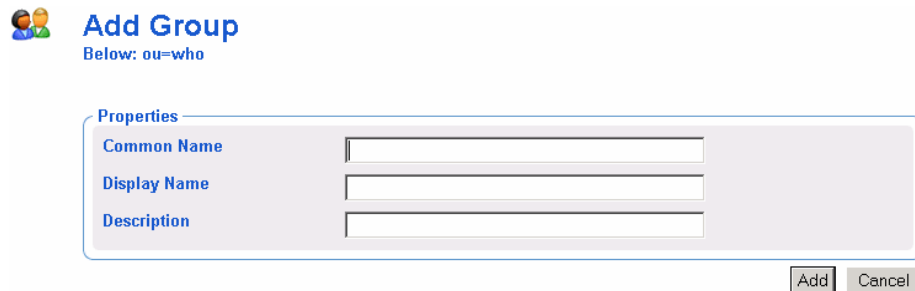
or


Click  to indicate that you do not want to remove the user.

Adding User Groups

To add a group

- 1 Use the Navigation aid and workspace to go to the **Directory** → **Zone** location.
- 2 In the workspace, click **Administrators & Operators**.
- 3 In the Model Administration task group, click **Add Group**.
The Add Group dialog box opens.



 **Add Group**
Below: ou=who

Properties

Common Name	<input type="text"/>
Display Name	<input type="text"/>
Description	<input type="text"/>

- 4 In the Common Name text box, type a name for the container object.



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 Management Portal.
- 6 In the Description text box, type a description that will appear in the Details view.
- 7 Click **Add**.

The Modify Group of Administrators and Operators dialog box opens. An example is shown in the following figure.

Modify Group of Administrators and Operators

The dialog box is titled "Modify Group of Administrators and Operators". It is divided into two main sections: "Properties" and "Members".

Properties:

- Display Name:** Network Admins
- Description:** Network Admins

Members:


Available:

- Guest
- Operator
- Portal Administrator
- RCS Administrator
- Test User


Selected:

Navigation buttons between lists: >>, >>|, |<<, <<<

Buttons at the bottom: Modify, Reset, Cancel

- 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 279 for more information about how to use this dialog box.

10 Click **Modify**.

The new group is added to the Administrators & Operators container.

11 To display the Properties, click the View Properties icon in the toolbar



The Group of Administrators and Operatoros Properties page opens and you can review your changes.

Network Admins Group of Administrators and Operators Properties

Properties | Object Information

Properties

Create Time Stamp	2006/01/11 00:24
Members	Operator
	RCS Administrator
Modify Time Stamp	2006/01/11 00:31

Back to top

Object Information

Display Name	Network Admins
Description	New User Group
Common Name	Network Admins
X500 Distinguished Name	cn=network_admins, cn=user, cn=acme corp, cn=radia
Object Class	top groupOfNames

Back to top

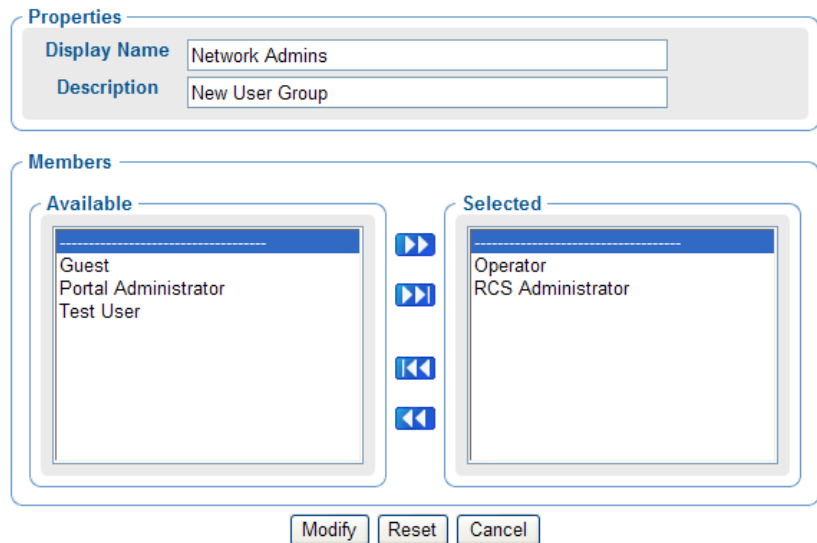
Modifying Groups

To modify a group

- 1 Use the Navigation aid and workspace 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 of Administrators and Operators dialog box opens.

Modify Group of Administrators and Operators



Properties

Display Name: Network Admins

Description: New User Group

Members

Available

- Guest
- Portal Administrator
- Test User

Selected

- Operator
- RCS Administrator

Modify Reset Cancel

5 Make any necessary changes. For detailed information about configuring users, see [Adding User Groups](#) on page 235.


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 and workspace 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 of Administrators and Operators confirmation page opens.
- 5 Click  to confirm that you want to remove the group from the Management Portal Directory.
or
Click  to indicate that you do not want to remove the group.

Managing the Portal Zone Directory

The 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 Management Portal Zone, as well as infrastructure and job status and history information. This section describes how to backup, restore, or query the Management Portal Directory, as well as how to import and export subsets of the Management Portal Directory.

Creating a Backup of the Portal Zone Directory

Use the Backup Directory task to create a backup copy of the entire 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 240.
- The procedure To backup the Management Portal Directory begins on page 241.
- If you would like to export a portion of the Management Portal Directory, see Exporting Data from the Portal Directory on page 247 for more information.



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 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 Management Portal automatically maintain the backups for you.

Each backup creates a new subdirectory in the `\etc\backup` directory of where the 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.

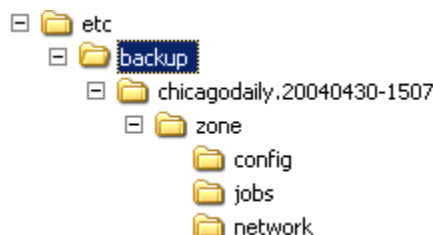
Thus, the full name of each backup directory includes the format:

```
<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.

The next figure 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.



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 17 below summarizes the location of additional *.mk files in a typical zone backup subdirectory.

Table 17 Sample Backup Subdirectory Contents

Location	Contents (*.mk files)
<<backup-subdirectory>>\zone	chassis, 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 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.



Create a 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 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 Management Portal Directory

- 1 Use the Navigation aid and workspace to go to the **Zone** level.
- 2 In the Directory Management task group, click **Backup Directory**.
The Submit Backup—Backup Opts dialog box opens.



Submit Backup

- 1 Backup-opts — 2 Schedule — 3 Summary

Backup file

Directory	C:\Novadigm\IntegrationServer\etc\backup
Filename	<input type="text" value="chicagodaily"/>

".YYYYMMDD-HHMM" will be appended to above input
Where YYYYMMDD-HHMM is time at backup creation

Next Cancel

- 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 240.

- 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 281.
- 6 Click **Next**.
- The Submit Backup—Summary dialog box opens.



Submit Backup

- 1 Backup-opts — 2 Schedule — 3 **Summary**

Backup Options

Directory: C:\Novadigm\IntegrationServer\etc\backup
 Filename: dailychicago

Scheduler Information

Starting On: 04/30/2004 22:45:00
 Duration: 0
 Periodic Interval: 86400
 Priority: 0
 Type: day

Submit Back Cancel

- 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 264 for more information.

- 8 Go to *SystemDrive:\Novadigm\IntegrationServer\etc\backup* to access the backup directories for the Management Portal.

The Management Portal maintains up to seven backup directories with the same assigned name, and 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 task to restore a backup of the entire Management Portal Directory.



The Restore task can only restore backups created from version 2.x or later of the Management Portal.

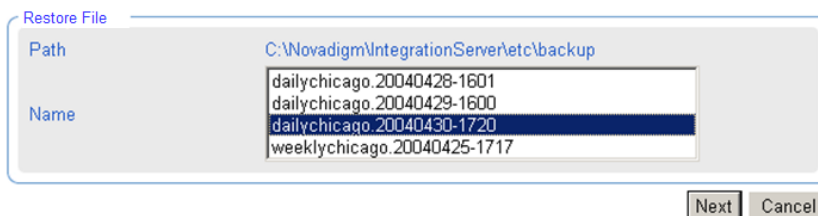
To restore the Management Portal Directory

- 1 Use the Navigation aid and workspace to go to the Zone level.



- In the Directory Management task group, click **Restore**.
The Submit Restore—File dialog box opens.

Submit Restore

1 File — 2 Confirm — 3 Finish



Path	Name
C:\Novadigm\IntegrationServer\etc\backup	dailychicago.20040428-1601
	dailychicago.20040429-1600
	dailychicago.20040430-1720
	weeklychicago.20040425-1717


- 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.
- Click **Next**.
A confirmation dialog box opens.
- Click  to confirm that you want to restore the Management Portal Directory.
or
Click  to indicate that you do not want to restore the Management Portal Directory.
- After the confirmation of a restore, the Finish dialog box opens when the restore is complete. Click **Finish** to continue.
The restore of the selected backup is complete.

Querying the Portal Directory

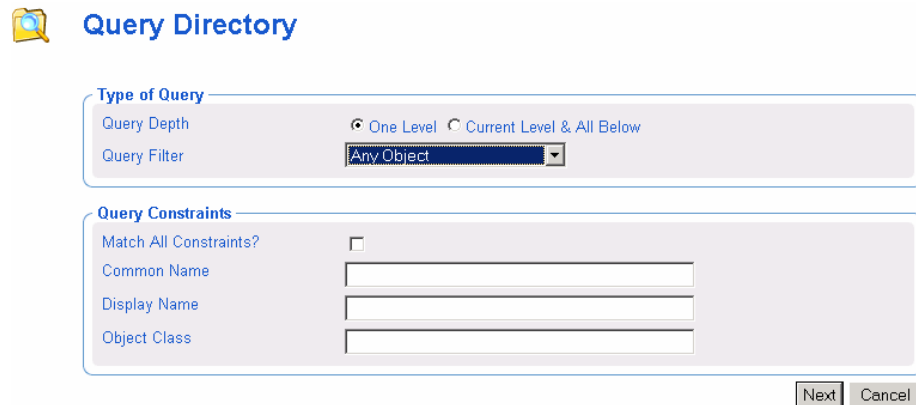
Use the Query task icon on the Toolbar to locate objects in the Management Portal Directory. You may use the results of the query to view information, or to select the authority for a job.

To perform a query

- 1 Use the Navigation aid and workspace to go to the place in your infrastructure where you want to perform a query.

- 2 Click the Query icon on the Toolbar .

The Query Directory dialog box opens.



- 3 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.
- 4 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.
- 5 If you want to constrain your query, type the appropriate information in the text boxes listed in the Query Constraints area.



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":

—Select **Current Level & All Below** in the Query Depth area.

—Select **Administrators & Operators** from the Query Filter drop-down list.

—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**:

—Select **Current Level & All Below** in the Query Depth area.

—Select **Administrators & Operators** from the Query Filter drop-down list.

—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.

- 6 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.
- 7 Click **Next** to initiate the query.

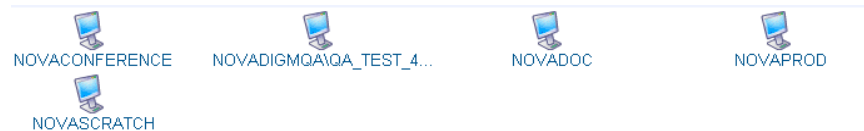
The results of the query appear in the workspace.



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 the following figure.






If you want to perform a task on an object in the query results, first click the object to set its Authority.

Exporting Data from the Portal Directory

Use the Export task to export a subset of your 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 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 277 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 279 for more information.
- 6 Click **Next**.
The Submit Export—Exp opts dialog box opens.

Submit Export

1 Query – 2 Select – 3 Exp-opts – 4 Schedule – 5 Summary

Output File

Directory	c:\Novadigm\IntegrationServer\etc\export
Filename	<input type="text" value="Admins"/>

.ldif will be automatically appended to the filename
4 items will be exported

Next Back Cancel

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 281.

10 Click **Next**.

The Submit Export—Summary dialog box opens.

Submit Export

1 Query – 2 Select – 3 Exp-opts – 4 Schedule – 5 Summary

Selected Audience

Administrators & Operators
Network Admins
Operations StaffPortal Administrator

Selected Options


Filename: Admins.ldif

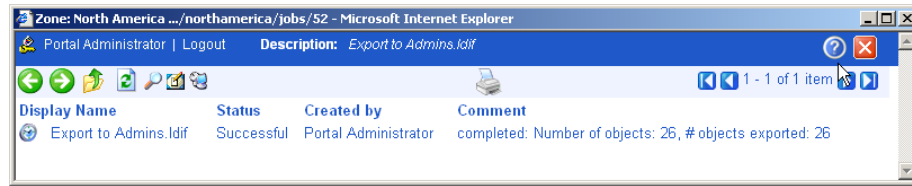
Scheduler Information

Starting On:	08/16/2002 14:30:00
Duration:	0
Periodic Interval:	0
Priority:	0
Type:	none

Submit Back Cancel

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  on the job window toolbar. See Viewing Properties on page 264 for more information.



- 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 Management Portal Directory. For example, if you prefer to modify the Management Portal Directory manually, in a text file, rather than through the Management Portal user interface, you can export the directory, make your modifications, and then import the file into the Management Portal Directory.

- ▶ Be sure to back up your Management Portal Directory before importing any data. See Creating a Backup of the Portal Zone Directory on page 239 for more information.

To import the Management Portal Directory

- 1 Use the Navigation aid to select the place in your infrastructure where you want to place the imported data.
- 2 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`).

Submit Import

- 1 Pick-file — 2 Pick-roots — 3 Import-select

Input File

Path: c:\Novadigm\IntegrationServer\etc\export

Filename:

- EntireNetwork.ldif
- Export1.ldif
- all.ldif
- backup.ldif
- backup1.ldif

Next Cancel

- 3 Click the file that you want to import.
- 4 Click **Next**.
- 5 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.

Submit Import

- 1 Pick-file — 2 Pick-roots — 3 Import-select

Roots

<input checked="" type="checkbox"/> Administrators & Operators	<input type="checkbox"/> Tasks	<input type="checkbox"/> Entire Network
<input type="checkbox"/> Jobs	<input type="checkbox"/> Entitlement	<input type="checkbox"/> Radia Subscriber Information

Next Back Reset Cancel

- 6 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.



Submit Import

- 1 Pick-file
- 2 Pick-roots
- 3 **Import-select**

Differences

Nodes to display :

- + Test User (who/test)
- ▶ Administrators & Operator (who)
- ▶ Operator (who/operator)
- ▶ Guest (who/guest)
- ▶ Portal Administrator (who/admin)

1 - 5 of 6 items ▶

Add

No nodes in list.

Delete

No nodes in list.

Modify

No nodes in list.

- 7 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.
- 8 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.

Submit Import


1 Pick-file — 2 Pick-roots — 3 **Import-select**

Differences

Nodes to display : All Select All

- Administrators & Operators (who)
- Operator (who/operator)
- Guest (who/guest)
- Portal Administrator (who/admin)

Add

 Test User (who/test)

Delete

No nodes in list.

Modify


No nodes in list.

Commit Back Cancel

9 Click **Commit**.

The items are added to the Portal directory.

The example below shows the Test User object was added to the Portal Directory.



The screenshot displays a grid of user objects in the Portal Directory. Each object is represented by a small icon of a person and a text label below it. The objects are arranged in three columns. The first column contains 'Guest', 'Operations Staff', and 'Test User'. The second column contains 'Lisa Smith' and 'Operator'. The third column contains 'Network Admins' and 'Portal Administrator'.

Updating Portal Tasks

Use Update Portal Tasks to update the tasks available to you when you receive a new build of the Management Portal.

To update Portal tasks

- 1 Stop the Management Portal. See Starting and Stopping the Management Portal on page 45 for more information.
- 2 Copy the new `rmp.tkd` into the `\modules` folder of your Radia Integration Server directory (by default `SystemDrive:\Novadigm\IntegrationServer\modules`).
- 3 Start the Management Portal. See Starting and Stopping the Management Portal on page 45 for more information.
- 4 Use the Navigation aid and workspace to go to the Zone Configuration Tasks container.
- 5 In the Directory Management task group, click **Update Portal Tasks**.



- 6 The Update tasks – select dialog box opens.



Submit Update

1 Update-tasks-select

Differences

Nodes to display :

- Radia Full Connect (what/notify/full)
- Radia Full Connect (what/notify-subscription/full)

Add

No nodes in list.

Delete

No nodes in list.

Modify

No nodes in list.

- 7 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 Management Portal.
 - Select **Delete** to review only those tasks that can be removed from the Management Portal.
 - Select **Modify** to review only those tasks that can be changed in the Management Portal.
- 8 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.



Submit Update

1 Update-
tasks-
select

Differences

Nodes to display : All

No nodes in list.

Add

No nodes in list.

Delete

No nodes in list.

Modify



Radia Full Connect (what/notify/full)



Radia Full Connect (what/notify-subscription/full)

Commit

Cancel

9 Click **Commit**.

The selected tasks (shown in the Add, Delete, and Modify areas) are updated in the Management Portal Tasks container.

Managing Jobs

The Jobs container in the Management Portal Zone Directory stores objects that represent all of the current jobs in the system, and jobs completed within the past four days.



Jobs can be viewed in the History Container as soon as they are executed. See Viewing Job History on page 263.

Filtering Job Groups or Jobs by Status

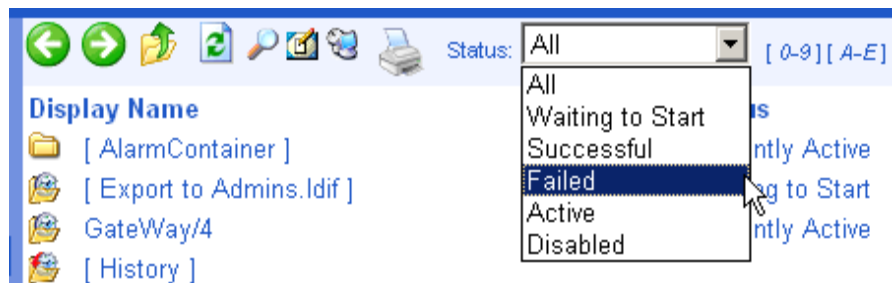
Use the Status list box on the Authority toolbar to quickly filter a Jobs container display by job status. For example, if you are viewing all Jobs (that is, a list of all Job Groups), select a Status of "Failed" to view only the Job

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.

- ▶ 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 258.

To filter Jobs by Status

- 1 Use the Navigation aid and workspace 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.



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 and workspace 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.



Modify Job Group

Scheduler Information

Name

Description

Tracing Enabled? on off

Time Window

Run:

Starting on: at

Job Throttling

Have a maximum of jobs running at any time

and start them in batches of jobs per every

seconds

- 5 Modify the job as necessary.

To modify Scheduler Information:

- 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.

To modify Time Window information:

- 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.

To modify Job Throttling information:

- In the Have a maximum of n 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 and start them in batches of n jobs per minute 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.

- 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 and workspace 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 dialog box opens.

Query Job

Time Window

Scheduled From Time: Aug 07, 2005 16:00
Scheduled To Time: Aug 11, 2005 16:00

Display Selection

Display: JobGroups

Job Characteristics

Match All Constraints?

Status:

Target Audience:

Created by:

Create CSV file

Directory: C:\Novadigm\081005\etc\export
CSV Filename:
filename will be appended with .csv extension

Next Cancel

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**.



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.

Use the Create CSV file area to save the results of your query to a file in CSV (comma delimited) format. The saved file is placed in the Directory location named in this area.

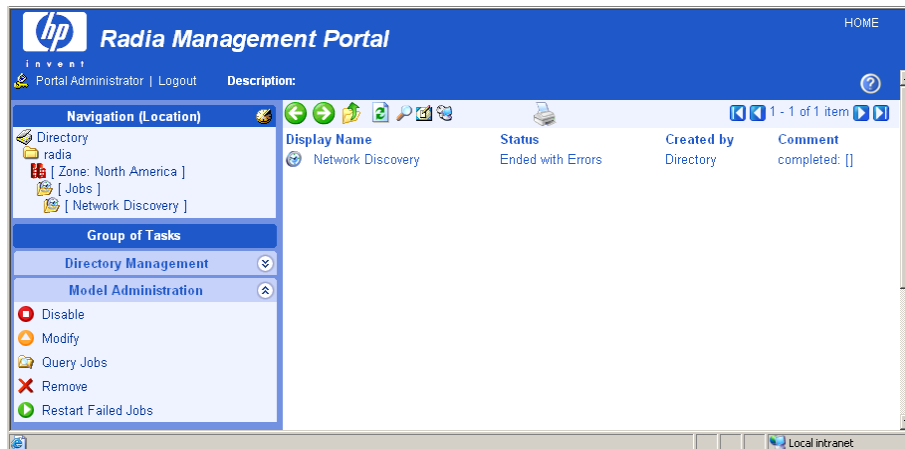
- 11 In the CSV Filename text box, optionally type a filename if you want to save the query results. The filename will be appended with the .csv extension.
- 12 Click **Next**.

A list of the jobs or job groups that match the selected 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

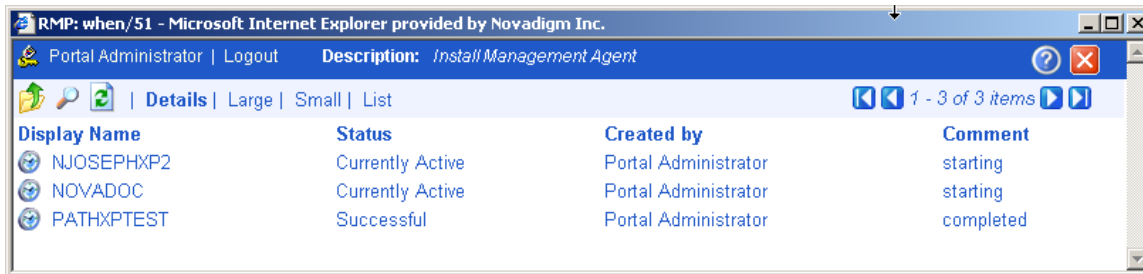
Restarting Failed Jobs in a Job Group

- 1 Go to the Jobs container, and display a job group containing one or more failed jobs.
 - ▶ 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.



- 13 In the Model Administration task group click **Restart Failed Jobs** to restart the failed jobs in this job group.

The jobs are restarted immediately, as shown in the active jobs page (see the next figure).



- 14 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.

- ▶ This task applies to job groups only and is not available for individual jobs.

To stop job groups



- 1 Use the Navigation aid and workspace to go to the **Directory** → **Zone** containers.

- 2 In the Workspace, click **Jobs**.
- 3 Click the job group that you want to stop.
- 4 In the Model Administration task group, click **Stop**.
A confirmation appears in the workspace.
- 5 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 and workspace to go to the **Directory** → **Zone** containers.
- 2 In the workspace, click **Jobs**.
- 3 Click the job or job group that you want to disable.
- 4 In the Model Administration task group, click **Disable**.
A confirmation appears in the workspace.
- 5 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

- 1 Use the Navigation aid and workspace to go to the **Directory** → **Zone** containers.
- 2 In the workspace, click **Jobs**.
- 3 Click the job or job group that you want to enable.
- 4 In the Model Administration task group, click **Enable**.
A confirmation appears in the workspace.
- 5 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

- 1 Use the Navigation aid and workspace to go to the **Directory** → **Zone** containers.
- 2 In the workspace, click **Jobs**.
- 3 Click the job or job group that you want to remove.
- 4 In the Model Administration task group, click **Remove**.
A confirmation appears in the workspace.
- 5 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

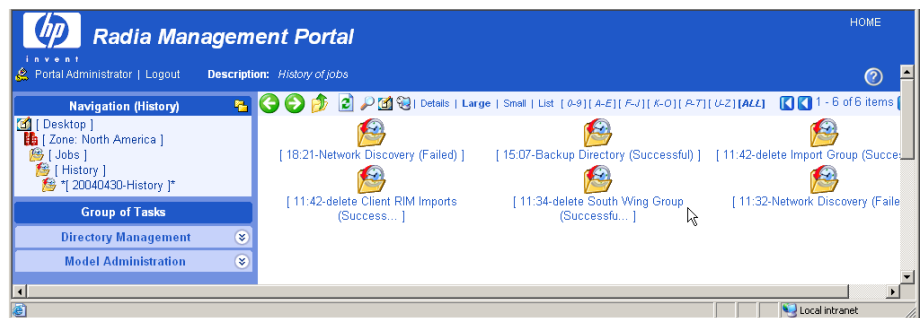
The History Container stores daily histories of all executed jobs, displayed in reverse date and time order. Jobs are written to the current day's history file as soon as execution stops (with or without errors).

To view job history

- 1 Use the Navigation aid and workspace to go to the **Directory** → **Zone** containers.
- 2 In the workspace, click **Jobs**.
- 3 In the workspace, click **History**.
- 4 Job histories are listed in reverse chronological order by date and time. History files include the date in the format: YYYYMMDD.
- 5 Click the history file for the date whose jobs you want to review.




Click **Details** to view a concise summary of the job groups for that day.



- 6 Click a specific job group from those displayed in the workspace.
The workspace lists the jobs that ran in that job group.
- 7 Click a job in the workspace.
The Job Properties dialog box displays the details of the job.

Viewing Properties

Click the View Properties icon  on the toolbar to display the properties for an object or a job. The properties that appear vary based on the selected object.

Service Techs Group Properties

Properties | Object Information

Properties

Create Time Stamp	2004/05/01 21:30
Members	DOCTESTB prod_device1 SUDH1864 A_Test800
Modify Time Stamp	2004/05/04 19:59

[Back to top](#)

Object Information

Common Name	Service Techs
X500 Distinguished Name	cn=service techs, cn=west coast group, cn=group, cn=northamerica, cn=radia
Object Class	top group

[Back to top](#)

Most Properties pages will display the group areas shown in the figure above. 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 underlined 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.
- Click the **Back** button on your web browser to return.

Summary

- Run Update Portal Tasks when you receive a new build of the 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 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 task to restore a backup of the entire Management Portal Zone Directory.
- Use the Export task to export a subset of your Management Portal Directory to an LDIF file.
- Use the Import task to import an LDIF file into your Management Portal Directory.
- Use the Move Device 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 Static or Dynamic port assignment.
- Be able to install the Proxy Server.
- Be able to synchronize the Proxy Server.
- Be able to install, update, and open a remote Management Portal Zone.
- Be able to add Task Templates for scheduling jobs.
- Be able to schedule jobs to run in multiple 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 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.




This chapter discusses the operational details of how to perform these tasks using the Management Portal and assumes that you have an understanding of how to use the HP OpenView Radia product suite.

If necessary, refer to the HP OpenView web site for more information.

The core tasks in the Management Portal are:

- **Manage Computer**
Click **Manage Computer** to explicitly bring one or more computers into your Management Portal Zone. Managed computers have an entry in the Management Portal's Zone → Devices container, and an automatic membership in the Default Group. For details, see *Managing Computers in Your Management Portal Zone* on page 272.
- **Add Task Template**
Click **Add Task Template** to preset the options for a Task Type, such as Notify or Install Proxy Server, 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 Radia Client**
Click **Install Radia Client** to install the Radia Client on remote computers. See *Installing the Radia Client* on page 302 for more information. Multiple Client Install Profiles are supported. For details, see *Supporting Remote Installs Using Multiple Profiles* on page 307.
- **Install Management Agent**
Click **Install Management Agent** to install the Radia Management Agent on remote computers. See *Installing the Radia Management Agent* on page 295 for more information.
- **Install Proxy Server**
Click **Install Proxy Server** to install the Radia Proxy Server on remote computers. See *Installing the Proxy Server* on page 315 for more information.
- **Synchronize Proxy Server**
Click **Synchronize Proxy Server** to force the Proxy Server to connect to the Configuration Server to preload the files to the static cache on the

Proxy Server. See Synchronizing the Proxy Server on page 320 for more information.

- **Purge Proxy Server Dynamic Cache**
Click **Purge Proxy Server Dynamic Cache** to purge the dynamic cache of the Proxy Server. See Purging the Dynamic Cache of the Proxy Server on page 322 for more information.
- **Notify Devices**
Use the Notify tasks to perform an action on the selected audience. See Using the Notify Tasks on page 283 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 286 for more information.
- **Sequence Job Task**
Use **SequenceJob** 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 Management Portal**
Click **Install Management Portal** to remotely install another Management Portal Zone in your infrastructure. See Installing Additional Management Portal Zones (Subordinate Zones) on page 327 for more information. Also refer to the tasks for Open Subordinate Zone and Schedule Zone Operation.
- **Update Management Portal**
Click **Update Management Portal** to remotely update the code delivered with a new build to the subordinate Management Portal Zones in your infrastructure. See Updating Subordinate Management Portal Zones on page 333 for more information.
- **Open Subordinate Zone**
Click **Open Subordinate Zone** to quickly access the Management Portal of another Zone in your enterprise from the Zone Access Points container. See Opening a Subordinate Zone on page 339 for more information.
- **Schedule Zone Operation (ZoneJob task)**
Click **ZoneJob** from the Zone Access Points container to run a Notify or Install Proxy Server 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 334 for more information.

Managing Computers in Your Management Portal Zone

Use the Manage Computer task to bring the computers in your network or external directories under the control of the Management Portal Zone explicitly.

▶ As of Management Portal v2.0.1, 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.

To learn other ways to add devices to your RMP Zone, see *Adding Devices to an RMP Zone* on page 159.

The Manage Computer task:

- Places the selected computers in the Zone's Devices container, which establishes it as a unique device in the Zone directory.
- Makes the devices members of the Zone's Groups container Default Group.

Once a device is under management of the 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

▶ As of RMP 2.0.1, you do not need to perform this task before running an install task; any install tasks will automatically bring a device in your network under management before proceeding with the install.

- 1 Use the Navigation aid and workspace to go to the Zone's Networks container.

- 2 In the Workspace, select the Network containing the computer to be managed. For example, Microsoft Windows Network.
- 3 In the Workspace, navigate through the Network hierarchy to the computer object. For example, select the Domain and then select the Computer.



Legend

- a** Navigate to computer.
 - b** Select Manage Computer.
- 4 Click **Manage Computer** in the Operations task group.

At this point, the 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.



The Operations task group displays many tasks that are available for this managed Device. To take the best advantage of the Management Portal, after adding a device you will want to:

- Move or copy it into all appropriate Groups of devices that are needed for operations on this device. For details, see *Moving Devices into a Group* on page 186.
- Install the Radia Management Agent on the Device to make use of Cross References groups. For more information on the advantages of adding the Radia Management Agent, see *Installing the Radia Management Agent* on page 295.

To manage a group of computers in your network



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 management 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 161.

- 1 Go to the **Zone** → **Network** container.
- 2 Navigate to a Network level containing the group of computers that you want to have managed by the Management Portal.
- 3 Click **Manage Computer** in the Operations task group.
- 4 Complete the selection of the computers to be brought under management.
- 5 Click **Modify**.

All selected computers are added to the Zone's Devices container and the Default Group of the Zone's Groups container.

To move or copy these devices into different groups, see *Moving Devices into a Group* on page 186.

To manage one or more computers located in Active Directory



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 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 135.

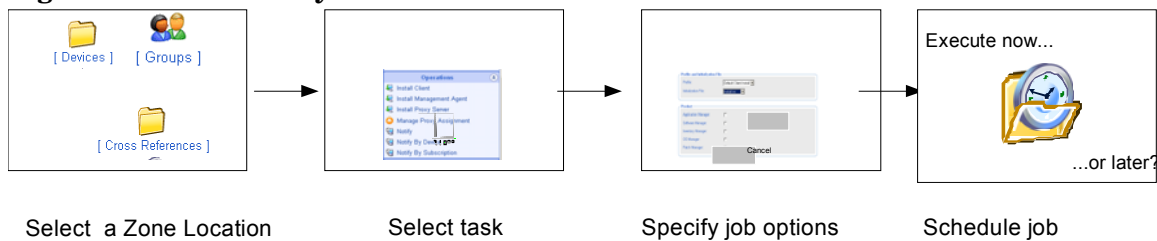
About the Task Lifecycle

Operational tasks are performed on devices and device groups under management by the 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 the next figure.

Figure 25 Task lifecycle



1 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 Management Portal Directory.



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.

2 Select the task.

The tasks available are filtered according to your selected starting location. For example, the Synchronize 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 Proxy Servers.

3 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.

4 Specify scheduling options.

Specify when you want the job to run.

5 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 Management Portal. When you finish entering the necessary information, a job is created.

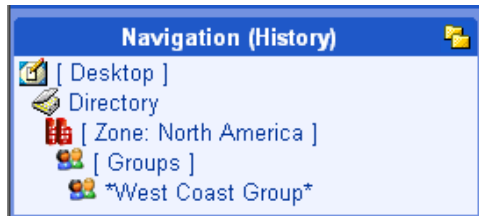
This section covers these basic procedures in detail.

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 88. 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 159.
- 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 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 65.



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".

- ▶ If you selected a single Authority, such as a particular computer, and then select a task, you will bypass the Query dialog box.

Figure 26 Query dialog box

Query Directory

Type of Query

Query Depth: One Level Current Level & All Below

Query Filter: Any Object

Query Constraints

Match All Constraints?

Common Name:

Display Name:

Object Class:

Next Cancel

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.



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":

—Select **Current Level & All Below** in the Query Depth area.

—Select **Administrators & Operators** from the Query Filter drop-down list.

—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**:

—Select **Current Level & All Below** in the Query Depth area.

—Select **Administrators & Operators** from the Query Filter drop-down list.

—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.

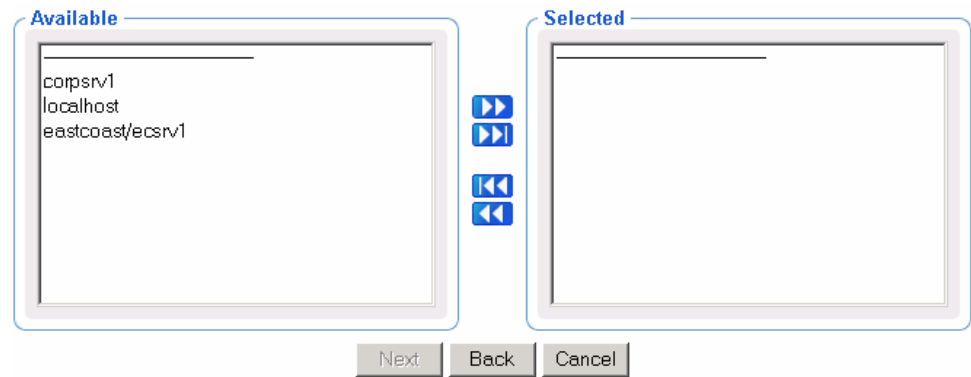
Selecting an Audience

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.




You will bypass the Select dialog box if your starting Zone location is a single object when you select the task, or, if the result of the Query is a single object.

Figure 27 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

- 1 From the Available list, select one or more devices.
- 2 Click  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  to add all of the devices to the Selected list.

- 3 If you want to remove devices from the audience list, select the appropriate devices from the Selected list and then click .

or

If you want to remove all of the devices from the list, simply click  to remove all of the devices from the Selected list.

- 4 Click **Next** to move to the next step in the task.



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 ten computers. Below this job group ten 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 28 Submit Notify—Schedule dialog box (Windows)

The screenshot shows the 'Submit Notify—Schedule dialog box (Windows)' with three main sections:

- Scheduler Information:** Contains fields for 'Job Name' (empty), 'Description' (Full Connect), and 'Priority' (Normal).
- Time Window:** Contains fields for 'Run' (Once), 'Starting on' (May 5, 2004 at 15:50), and 'Duration' (00 hours 00 minutes).
- Job Throttling:** Contains text: 'Have a maximum of 30 jobs running at any time, and start them in batches of 0 jobs per minute.'

At the bottom right, there are three buttons: 'Next', 'Back', and 'Cancel'.

To schedule a job

- 1 Complete the 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 the 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.
- 3 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.
- 4 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 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.



Use the Notify task from the Cross References container groups (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 container 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 286 for more information.

Refer to the *Installation and Configuration Guides for the HP-OpenView Application Manager Using Radia* or *HP-OpenView Software Manager Using Radia* 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.

- ▶ The 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 and Subnet of the targeted machine is available in the device properties.

To notify an audience

- 1 Use the Navigation aid to select the Authority.
- 2 From the Operations task group, click **Notify**.

- ▶ If you selected a single Authority, such as a particular computer or a group of devices, and then selected Notify, you will bypass the Query and Select dialogs. Go to step 6.


The Query dialog box opens.

- 3 Specify criteria to narrow the scope of the job. See *Performing Queries* on page 277 for more information.

- ▶ 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 279 for more information.
- 6 Click **Next**.

The Submit Notify—Notify Opts dialog box opens.



Submit Notify

1 Query — 2 Select — 3 **Notify-opts** — 4 Schedule — 5 Summary

Notify Type

Radia Refresh Catalog

Notify Information

Command: radskman req="Refresh Catalog",mname=|mgrname|,dname=SOFTWARE|
Port number: 3465
User: user1
User Password:

1 item selected

Next Back Cancel

- 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
```









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 288 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 Submit Notify — 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 281.
- 13 Click **Next**.
The Submit Notify — Summary dialog box opens.
- 14 Click **Submit**.
The Job Status window opens with list of the jobs. This dialog box 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.
- 15 When you are done viewing the job status, click  to close the Job Status dialog box, and return to the 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.

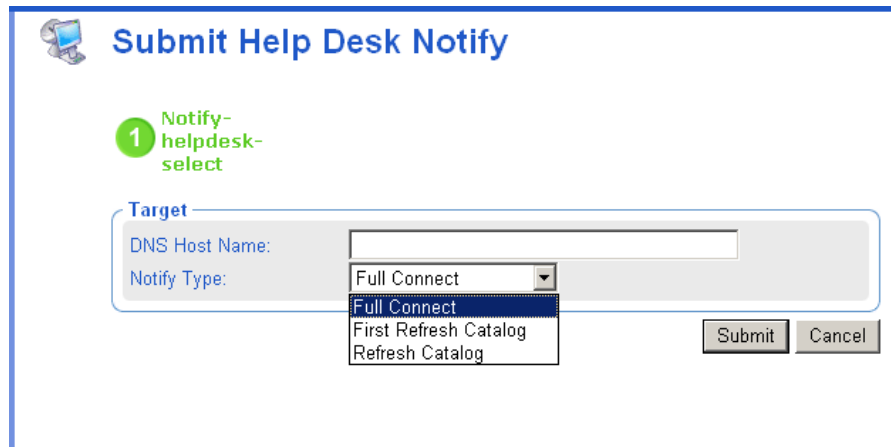
The options and command syntax for the Notify task submitted through the Help Desk Notify need to be previously set or customized. For details, refer to one of the following sections:

- Setting Default Options for Notify Commands on page 288.
- Creating Custom Notify Commands on page 292.

To notify a single computer from the Help Desk Tasks group

- 1 From anywhere in a Portal Zone, click the toolbar icon for Help Desk Notify 

The Submit Help Desk Notify window opens.



Submit Help Desk Notify

1 Notify-helpdesk-select

Target

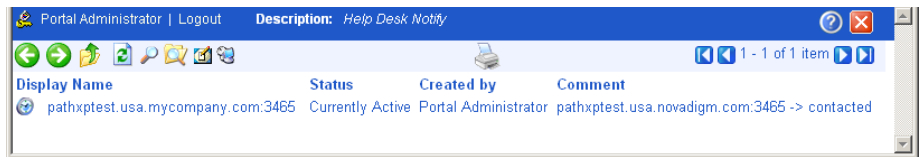
DNS Host Name:

Notify Type:

- Full Connect
- First Refresh Catalog
- Refresh Catalog

- 2 In the DNS Host Name field, type the DNS Host Name of the client computer to be notified.
- 3 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 288.
- 4 Click **Submit**.

The selected Notify is run immediately, and the Job Status window opens.



- 5 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:

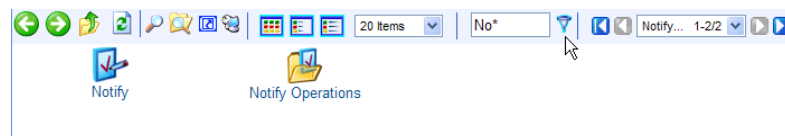
- Help Desk Notify (listed under H's)
- Notify

To set default options for Notify commands

- 1 Navigate to the **Directory** → **Zone** → **Configuration** container.
- 2 In the workspace, click **Tasks**.
- 3 In the workspace, locate the Notify task that you want to modify, such as **Notify**.

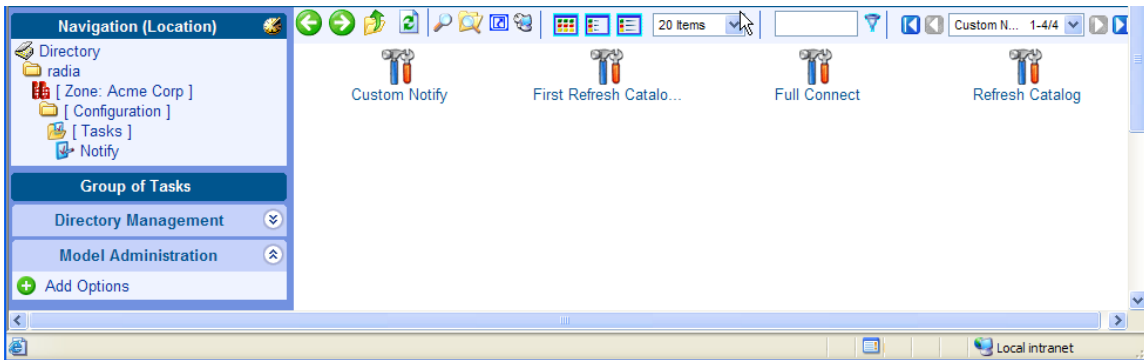


To quickly find the Tasks beginning with No, type **No*** in the filter area and press Enter. A sample result is shown in the following figure.



For more information, see [Paging and Filtering Icons](#) on page 84.

- 4 Click the **Notify** task to select it.
- 5 The workspace displays the Options applied to the various Notify operations.



- 6 In the workspace, click the type of Notify operation for which you want to set default options, such as **Refresh Catalog**.

The Options Properties dialog box opens.

Refresh Catalog
Options Properties

Properties | Object Information

Properties	
Command	radskman req="Refresh Catalog",mname= mgmname ,dname=SOFTWARE,ip= mgr_ip ,port= mgr_port ,cat=y
Complete When	radia/catalog
Create Time Stamp	2005/12/15 12:10
Modify Time Stamp	2005/12/15 12:10
Port Number	3465
User	user1

Back to top

Object Information	
Display Name	Refresh Catalog
Common Name	catalog
X500 Distinguished Name	cn=catalog_cn=notify_cn=task_cn=config_cn=acme_corp_cn=radia
Object Class	top nvdTaskOptions

Back to top

- 7 In the Model Administration task group, click **Modify**.
The Modify Options dialog box opens.



Modify Options

Properties

Display Name	Refresh Catalog
Command	radskman req="Refresh Catalog",mname=lmgr
Port Number	3465
User	user1
User Password	•••••
Complete When	Client Connects to RCS

Modify Reset Cancel

8 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:

Client Contacted

Client Connects to RCS

Client Sends Application Event

Complete When Job Property:

adhoc

radia/catalog

radia/service

9 Click **Modify**.

The Options Properties dialog box opens and you can review your changes.



The command line in the following figure is used for illustrative purposes only.

Refresh Catalog Options Properties

Properties | Object Information

Properties

Command	radskman req="Refresh Catalog",mname=Radia,dname=SOFTWARE,ip=10.10.10.1,port=3464,cat=y
Complete When	adhoc
Create Time Stamp	2004/04/27 18:06
Modify Time Stamp	2004/05/05 17:48
Port Number	3465
User	user1

[Back to top](#)

Object Information

Display Name	Refresh Catalog
Common Name	catalog
X500 Distinguished Name	cn=catalog, cn=notify, cn=task, cn=config, cn=northamerica, cn=radia
Object Class	top mvdTaskOptions

[Back to top](#)

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 the figure above match the default settings for the fields in the next figure.



Submit Notify

1 Query — 2 Select — 3 **Notify-opts** — 4 Schedule — 5 Summary

Notify Type

Full Connect

Notify Information

Command	radskman mname=Radia,dname=SOFTWARE,ip=10.10.10.1,port=
Port Number	3465
User	user1
User Password	•••••

1 item selected

[Next](#) [Back](#) [Cancel](#)

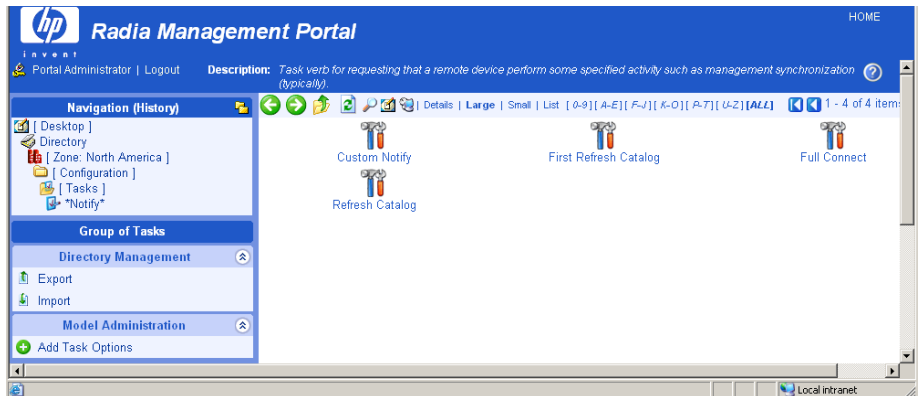
See Notifying an Audience on page 284 for more information about the Options dialog box.

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**.



- 4 In the Model Administration task group, click **Add Task Options**.

Add options

Properties

Common Name	<input type="text"/>
Display Name	<input type="text"/>
Command	<input type="text"/>
Port Number	<input type="text"/>
User	<input type="text"/>
User Password	<input type="text"/>
Complete When	Client Contacted <input type="button" value="v"/>

- 5 In the Common Name text box, type a name for the custom Notify task.



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 18 Notify Job Completion Options

"Complete When" Selections	Equivalent Entry on Task Property 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.

Open Notepad Options Properties

Properties | Object Information

Properties	
Command	c:\notepad.exe
Complete When	adhoc
Create Time Stamp	2004/05/05 17:58
Modify Time Stamp	2004/05/05 17:58
Port Number	3465
User	user1

[Back to top](#)

Object Information	
Display Name	Open Notepad
Common Name	Open Notepad
X500 Distinguished Name	cn=open_notepad, cn=notify, cn=task, cn=config, cn=northamerica, cn=radia
Object Class	top nvdTaskOptions

[Back to top](#)

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 284.
- For more information about the Submit Help Desk Notify dialog box, see [Using Help Desk Notify](#) on page 286.

Deploying Radia Management Infrastructure Products and Applications

Use the 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 SP3, XP SP2, or Server 2003 SP1.



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 11.0 or above, PA Rise 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 Management Portal installation program will copy these files automatically. See Installation Procedures on page 32 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.

```
└─ extended_infrastructure
   └─ common_components
      └─ management_portal
         └─ proxy_server
```

- 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 Management Portal creates the packing list when you launch the remote installation.
- The Management Agents must be able to communicate back to the Management Portal successfully. If they appear to be having communication problems with the Portal, consider specifying a valid network address using the `LISTENING_ADDRESS` parameter in the `RMP.CFG` file. For more information, see Table 3 on page 133.

Specific instructions about how to use the Management Portal to perform each remote install follows.

Installing the Radia Management Agent

You can use the Management Portal to perform operational and administrative tasks on the Radia infrastructure; however, the 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 Management Portal. It cannot perform any tasks on its own.

When you use the 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 Management Portal, the Radia Management Agent performs the task initiated by the 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 Management Portal at regular intervals in order to make its presence known. The Radia Management Agent will notify the 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 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`). Typical registration changes include a different RMA port number for RMAs using dynamic port assignments, or a different IP address in DHCP environments.

If the Radia Management Agent has no changes to report from the previous day, it does not contact the Management Portal.



Consider using RMAs with a static port assignment if you want to eliminate the RMA-registration updates that are generated by RMAs using dynamic port assignments.

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 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, MAC address and IP subnet.

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 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 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, and to reduce daily registrations from a Radia Management Agent due to a new port number (which occurs with dynamic port assignments).

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.

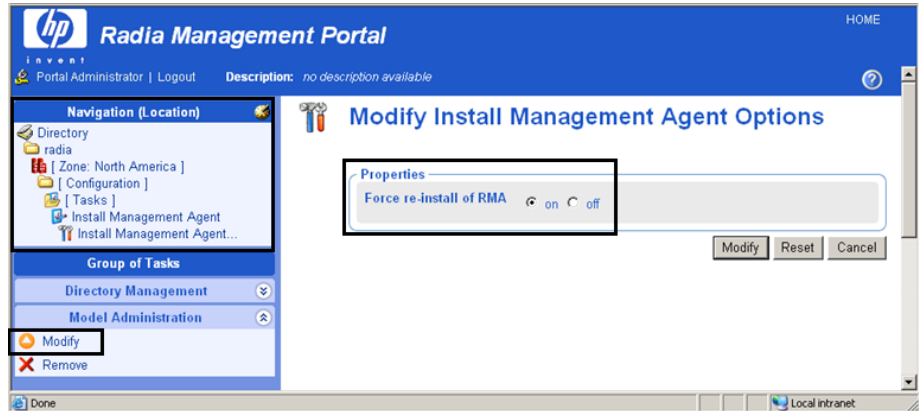
To set the Install Radia Management Agent task options

- 1 Go to the **Directory** → **Zone** → **Configuration** → **Tasks** container.

From the Workspace, page forward  or use the filter area  to locate and then select the **Install Management Agent** task.

- 2 In the Workspace, select **Install Management Agent Options**.
- 3 Click **Modify** in the Model Administration task group.

The Modify Install Management Agent Options dialog box opens.



- 4 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.

To install the Radia Management Agent


- Be sure to read Requirements for Remote Installations on page 294 before performing this procedure.
- 1 Use the Navigation aid to select the place in your infrastructure where you want to install the Radia Management Agent.
 - 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 Management Portal is not currently managing the targeted Network or LDAP devices, the Management Portal will bring them under management as part of the install task.
 - 2 From the Operations task group, click **Install Management Agent**.

▶ If you selected a single Authority, such as a particular computer or a group of devices, and then selected Install Management Agent, you will bypass the Query and Select dialogs. Go to step 6.

3 If the Query dialog opens, specify criteria to narrow the scope of the job.

4 Click **Next**.

The Select dialog box opens.

5 Select the audience from the Available list, and then click  to add them to the Selected list.

6 Click **Next**.

The Install Management Agent — Install Opts dialog box opens.

Install Management Agent

1 Query — 2 Select — 3 **Install-opts** — 4 Schedule — 5 Summary

Attributes

Select Client Port Dynamic Static

User

User Password

1 item selected

Next Back Cancel

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.

▶ If you are installing the Radia Management Agent on the same computer as the Management Portal, delete Administrator from the User text box.

7 Use the Select Client Port radio buttons to specify whether the 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. However, dynamic port assignments also require daily registrations of new port numbers by the Management Agents.

- Using a static port assignment is available to communicate to an Agent that is behind a firewall. This option also eliminates daily registrations of new port numbers by the Management Agents.
- 8 If you selected a Client Port type of Static, type the port number in the Port Number text box.
 - 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 Click **Next**.

The Schedule dialog box opens.

12 In the Schedule dialog box, specify when you want this job to run.

13 Click **Next**.

The Install Management Agent—Summary dialog box opens.



Install Management Agent

1 Query — 2 Select — 3 Install-opts — 4 Schedule — 5 Summary







Selected Audience	
DOCTESTB	

Attributes	
Client Port Number	Dynamic
User	Administrator

Scheduler Information	
Starting On:	05/05/2004 19:25:00
Duration:	0
Periodic Interval:	0
Priority:	0
Type:	none

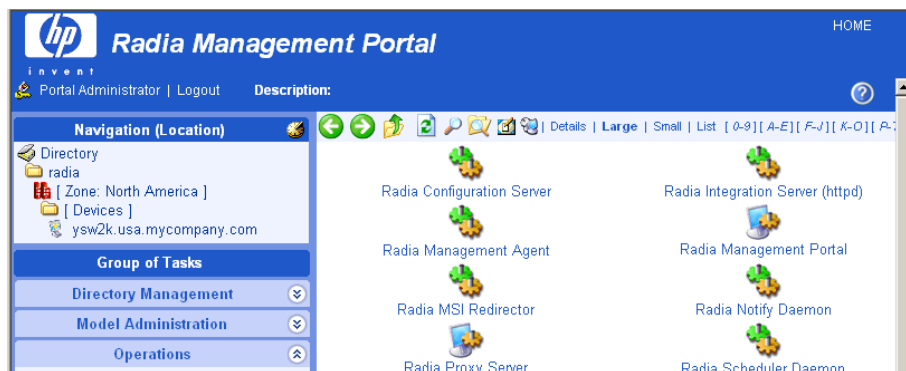
14 Click **Submit**.

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.
- 15 When you are done viewing the job status, click  to close the Job Status page, and return to the 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 Management Portal uses the information discovered by the Radia Management Agent to add the device to the appropriate groups in the Cross-References container of the Zone.



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 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 Management Portal's registry.


To refresh a Radia Management Agent's sub-service discovery

- 1 In the Navigation area, navigate to the appropriate device object whose Management Agent service discovery needs to be refreshed.



You do not need to navigate to the Management Agent, just to the device object.

- 2 From the Operations task group, click **Refresh Management Agent**.

Click  to refresh the Workspace area of the Management Portal. You'll see the current, newly registered Radia services and sub-services for the object.

Installing the Radia Client

Use the Install Radia 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 six feature sets, one for each client—Application Manager, Software Manager, Inventory Manager, OS Manager, Patch Manager, and Server Management.

- ▶ Use the Assign Proxy Assignment task prior to the Install Radia Client task if you want to deploy a set of Radia Clients from pre-assigned Proxy Servers, instead of directly from the 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 Management Portal to do all the work. For details, see Assigning Proxy Servers on page 311.
The Management Portal supports multiple client profiles. For details, see Supporting Remote Installs Using Multiple Profiles on page 307.

To install the Radia 4.x Clients with the Management Portal

- ▶ Be sure to read Requirements for Remote Installations on page 294 before performing this procedure.
For detailed information, such as system requirements and customization options, refer to the *Application Manager Guide* or the *Software Manager Guide*. These guides are available from the HP OpenView web site.

- 1 Use the Navigation aid to select the device or group of devices on which you want to install the Radia Clients.

- ▶ As of RMP 2.0.1, you can select a location in a Zone → Networks container or a currently connected LDAP directory location that contains computers on which you want to install the Radia Clients. If the Management Portal is not currently managing the targeted Network or LDAP devices, the Management Portal will bring them under management as part of the Install Radia Client task.

- 2 From the Operations task group, click **Install Radia Client**.


- ▶ If you selected a single Authority, such as a particular computer or a group of devices, and then selected Notify, you will bypass the Query and Select dialogs. Go to step 6.

The Query Dialog opens.

- 3 Specify criteria to narrow the scope of the job. See Performing Queries on page 277 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 279 for more information.
- 6 Click **Next**.
The Install Client—Client Opts dialog box opens.



Install Client

1 Query — 2 Select — 3 **Client Opts** — 4 Schedule — 5 Summary

a

Profile and Initialization File

Profile:

Initialization File:

b

Product

Application Manager:

Software Manager:

Inventory Manager:

OS Manager:

Patch Manager:

Server Management:

c

Install Options

RCS Host Name:

RCS Port Number:

Perform Silent Install?:

Perform Connect After Install?:

d

Remote Client Credentials

Select Client Port: Dynamic Static


User:

User Password:

Legend

- a** Select the Client Install Profile.
- b** Select the Radia Clients to install.
- c** Specify the Radia Configuration Server parameters.

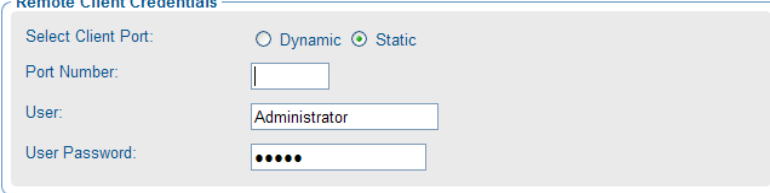
- d Specify the logon credentials for the target device.
- 7 From the Profile drop-down list, select a client profile to use for the installation. For details on creating Client Profiles, see Adding, Modifying, and Deleting Install Profiles on page 308.
- 8 In the Initialization File area, select the 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 Configuration Server.

The Management Portal will honor settings placed in a customized *.INI file when it installs the client.
- 9 In the Product area, select the clients that you want to install on the target devices.
 -  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 Configuration Server.
- 10 In the RCS Host Name text box, type the IP address or host name that the Radia Client will use to access the Configuration Server.
- 11 In the RCS Port number text box, type the port number that the Radia Client will use to access the Configuration Server.
- 12 Select the **Perform Silent Install?** check box if you want to install a client without any user interface.
- 13 Select the **Perform Connect After Install?** check box if you want the client computer to connect to the Configuration Server after the installation. This allows the client computer to register with the Configuration Server. Refer to the *Application Manager Guide* for more information.

When the client computer connects to the Configuration Server, the Management Portal also captures information about your subscribers and stores it in the Management Portal Directory. See Discovering Radia Subscriber Information on page 314 for more information.
- 14 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. However, dynamic port assignments also require daily registrations of new port numbers by the Management Agents.

- Using a static port assignment is available to communicate to an Agent that is behind a firewall. This option also eliminates daily registrations of new port numbers by the Management Agents.

If you select a Client Port type of Static, a Port Number text box appears.



Remote Client Credentials

Select Client Port: Dynamic Static

Port Number:

User:

User Password:

- 15 Type the static port number in the Port Number text box.
- 16 In the User text box, type the administrator ID to obtain administrative authority on the target device's domain.
- 17 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.

- 18 Click **Next**.

The Schedule dialog box opens.

- 19 In the Schedule dialog box, specify when you want this job to run. For more information, see *Scheduling Jobs* on page 281.

- 20 Click **Next**.

The Install Client—Summary dialog box opens.



Install Client Install

1 Query – 2 Select – 3 Client Opts – 4 Schedule – 5 **Summary**

Selected Audience	
Pubs_Test_Machine	
Profile and Initialization File	
Profile:	Default Client Install
Initialization File:	Install.ini
Product	
Application Manager	
Software Manager	
Inventory Manager	
OS Manager	
Patch Manager	
Server Management	
Install Options	
RCS Host Name:	radia
RCS Port Number:	3464
Client Port Number:	Dynamic
User:	Administrator
Scheduler Information	
Starting On:	2005/06/16 12:45:00
Duration:	0
Periodic Interval:	0
Priority:	0
Type:	none

21 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 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 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.

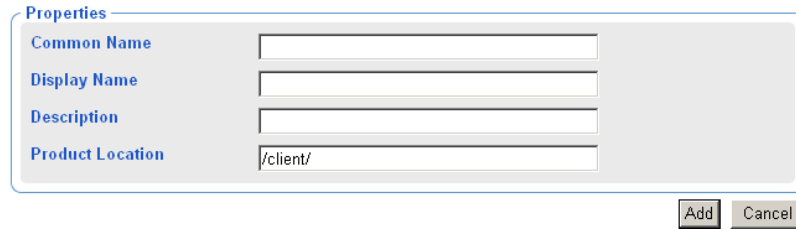
To add a Client Install Profile

- 1 Navigate to the following location in the Management Portal.



- 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

Add Cancel

3 Complete the Properties for the Add Client Install Profile, as follows:

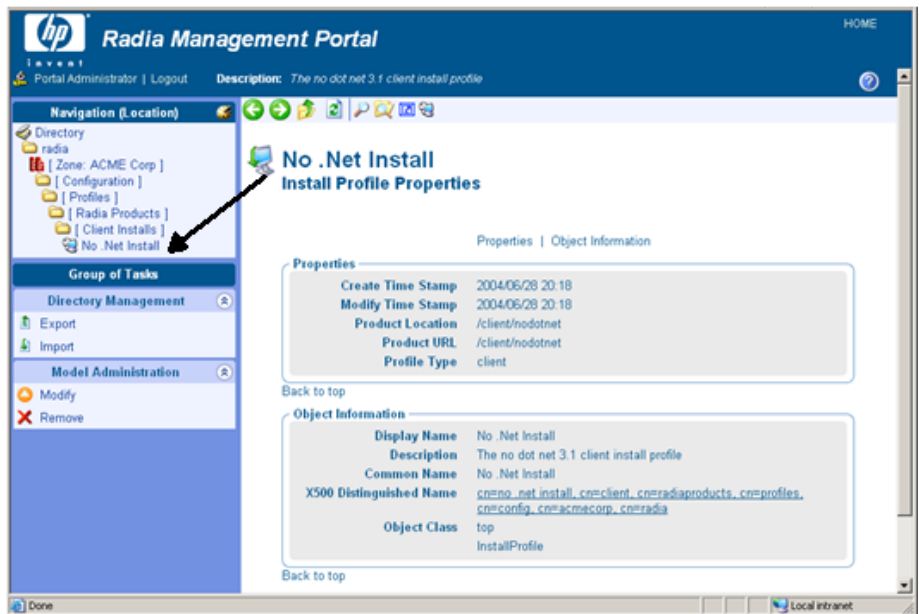
Common Name	A unique name for the Client Install Profile object in the RMP.
Display Name	The display name for this Client Install Profile in the RMP.
Description	A full description of the source code installed by this profile.
Product Location	The directory in the base-RMP <code>/media/client</code> 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 Management Portal users will now be able to select this profile from the Options page when using the Install Radia Client task.

To modify a Client Install Profile

- 1 Navigate to the where the profiles for Client Installs are located, shown in the following figure.



- 2 Click on the install profile object to be modified. You cannot modify the Default Client Install object.
- 3 Click **Modify** in the Model Administration task group. The Modify Install Profile page opens.
- 4 Modify any of the fields, and click **Modify**.



Modify Install Profile

Properties

Display Name	<input type="text" value="No .Net Install"/>
Description	<input type="text" value="The no dot net 3.1 client install profile"/>
Product Location	<input type="text" value="/client/nodotnet"/>

- 5 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 Radia Client task. It does not delete the source code from the Product Location.

- 1 Navigate to the [Client Installs] container and click on the profile to be deleted.

The Properties page for the Install Profile opens.

- 2 Click **Delete** in the Model Administration task group.

A prompt asks you to confirm the delete.

- 3 Click the green check mark to confirm the delete.

The profile object is removed from the [Client Installs] container.

Assigning Proxy Servers

Use the Assign Proxy Server task to designate Proxy Servers in your infrastructure to handle the deployment of client installation scripts for designated devices.

To assign a set of devices to a Proxy Server, first create a group in the Groups container for all devices to be assigned to a given Proxy Server. Create separate groups for devices being managed by different Proxy Servers. See Adding Devices to a New Group on page 308 for more information on how to create groups of devices. Then use the Assign Proxy Server task to assign a Proxy Server to all members of the group. Repeat the Assign Proxy Server task for each Proxy Server receiving node assignments.

After making all Proxy Server assignments, use the Install Radia Client task to schedule the installation of the clients. If a device that is scheduled for a

client installation has been assigned to a Proxy Server, the Management Portal will first synchronize with the Proxy Server, and then the Proxy Server will install the client on the device.

To change or remove proxy assignments, first change the group members, and then repeat the same Assign Proxy Server steps used to assign nodes to the Proxy Server.

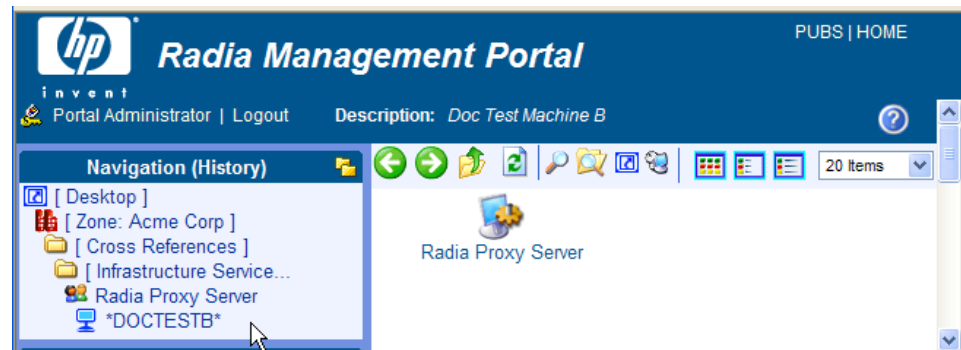
Requirements for Managing Proxy Assignments

- One or more previously installed Proxy Servers.
- For each Proxy Server, an installed Radia Management Agent that has also successfully discovered the Proxy Server service.

If these requirements have been met, when you navigate to a device containing the RMA-discovered Proxy Server, the Proxy Server icon will display in the Workspace of the Management Portal.

For example, the next figure shows the 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 Proxy Server, all would be listed in the Zone Cross References container. Go to the Infrastructure Services group and click on Proxy Server. All devices that have Radia Management agents and Proxy Servers on them are automatically added to this Cross References group.

Figure 29 Proxy Server discovered by the Management Agent

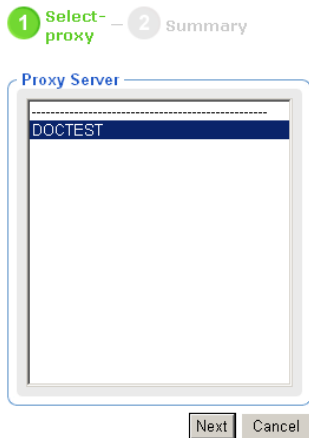


To assign devices to a Proxy Server

- 1 Create a group of Devices in the Groups container. Move all devices that are to be assigned to a single Proxy Server in the new Group. For details, refer to Adding Devices to a New Group on page 308.

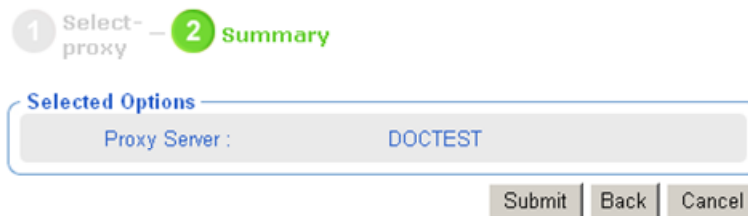
- 2 Use the Navigation aid to select the new Group for making proxy assignments.
- 3 In the Operations task group, click **Assign Proxy Server**.
The Manage Proxy Assignment – Select-proxy dialog box opens.

Manage Proxy Assignment



- 4 Select a Proxy Server from the list to handle the client deployment for the set of devices that are members of the selected Group.
- 5 Click **Next**.
The Manage Proxy Assignment — Summary dialog box opens.

Manage Proxy Assignment



- 6 Click **Submit** to save the proxy assignment of nodes to the selected server.
- 7 After completing all proxy assignments, run the Install Radia Client task from the Operations task group of the Management Portal, as discussed in Installing the Radia Client on page 302. If a proxy-assigned node is

selected for the client install, the Proxy Server performs the client script deployment, as opposed to the Management Portal.

Discovering Radia Subscriber Information using Managed Services

The Management Portal can be enabled to capture information about your subscribers and stores it in the 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.

Radia Services will appear in the cross references container as long as:

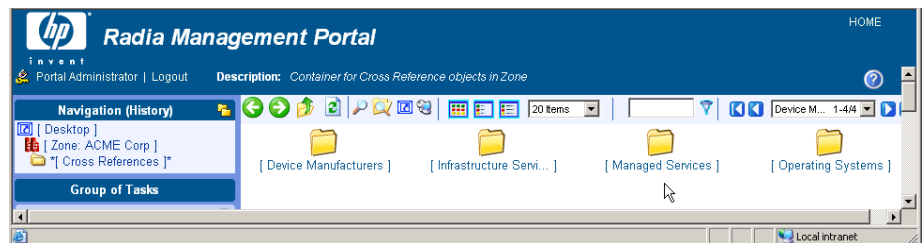
- Client reported objects have been enabled for posting to the Management Portal. For more information, see *Posting Client Objects to the Management Portal* on page 45.
- Application Event reporting is turned on for the services being installed.
- A client has installed at least one service.

When the Radia client computers connect to the Configuration Server, information is captured from the client reporting objects, and then the Messaging Server routes the appropriate client objects, such as APPEVENT, to the Management Portal. Refer to the *Messaging Server Installation and Configuration Guide* on the HP OpenView web site for more information on how to install and configure the Radia Messaging Service to route messages to the 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 Configuration Server has reported Radia managed applications.



- 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 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.

Installing the 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 configuration (*.CFG) file, if multiple ones exist.

Refer to the *Installation and Configuration Guide for the HP OpenView Proxy Server using Radia* for more information.

See Preparing and Locating Configuration Files for Proxy Server Installs on page 319 for details on preparing and locating customized CFG files for this task.

- ▶ In order to take advantage of the Install Proxy Server task, consider creating a standard administrator ID across the domains in your network.

To install the Proxy Server

- ▶ Be sure to read Requirements for Remote Installations on page 294 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 Proxy Server.

- ▶ As of RMP 2.0.1, you can begin to install the Proxy Server by selecting one or more devices from a location in your Zone, a Networks container, or an LDAP directory. If the Management Portal is not currently managing the targeted Network or LDAP devices, the Management Portal will bring them under management as part of the install task.

- 2 From the Operations task group, click **Install Proxy Server**.


- ▶ If you selected a single Authority, such as a particular computer or a group of devices, and then selected Notify, you will bypass the Query and Select dialogs. Go to step 6.

The Query dialog box opens.

- 3 Specify criteria to narrow the scope of the job. See *Performing Queries* on page 277 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 279 for more information.

- 6 Click **Next**.

The Install Proxy Server—RPS Options dialog box opens.



Install Proxy Server

1 Query — 2 Select — 3 **Rps-opts** — 4 Schedule — 5 Summary

Install Options

RCS Host Name:

RCS Port Number:

User:

RPS Config File:

Remote Client Credentials

Select Client Port: Dynamic Static

User:

User Password:

- 7 In the RCS Host Name text box, type the name or IP address for the Configuration Server.
- 8 In the RCS Port number text box, type the port number for the Configuration Server.
- 9 In the RCS User text box for Install Options, type the user ID to use to connect to the 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 Management Portal.



To make customized Proxy Server configuration files available for selection during this task, see *Preparing and Locating Configuration Files for Proxy Server Installs* on page 319.

- 11 In the User text box for Remote Client Credentials, type the administrator ID to obtain administrative authority on the target device's domain.

- 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 281.

- 15 Click **Next**.

The Install Proxy Server—Summary dialog box opens.



Install Proxy Server

1 Query – 2 Select – 3 Rps-opts – 4 Schedule – 5 **Summary**

Selected Audience

ys1683.usa.novadigm.com

Install Options

RCS Host Name:	physw2k.usa.novadigm.com
RCS Port Number:	3464
User:	RPS
RPS Config File:	Default Copy
Client Port Number:	Dynamic
User:	administrator

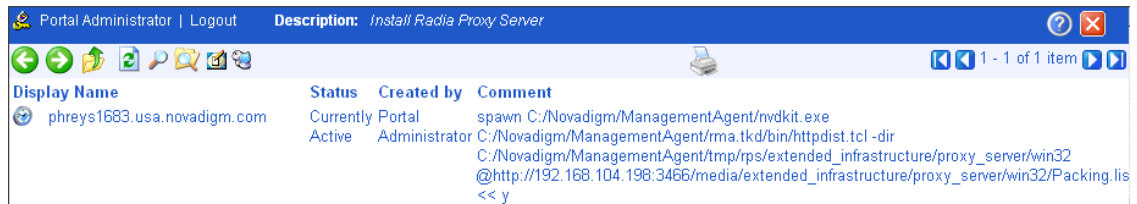
Scheduler Information




Starting On:	05/06/2004 17:50:00
Duration:	0
Periodic Interval:	0
Priority:	0
Type:	none




Submit Back Cancel

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.



- 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.
- 16 When you are done viewing the job status, click  to close the Job Status page, and return to the 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 Management Portal to use them. When you run the Install Proxy Server task from the 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 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

- 1 Prepare a fully configured `rps.cfg` file.

Perform a local installation of the Proxy Server on a test machine that is the same platform as the intended Proxy Server platform. Edit the resulting `rps.cfg` file using the directions given in the *Proxy Server Guide* in the section *Configuring the Proxy Server*.

- 2 Place the configured `rps.cfg` file in a specific 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 Proxy Server: win32, hpux, or solaris. For example, the location for a Windows 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 Management Portal is installed.

The default is either

```
SystemDrive:\Novadigm\IntegrationServer
```

or

```
SystemDrive:\Novadigm\Radia Integration Server
```

depending on when it was installed.

- b Go to the following folder location in the 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 Proxy Server on.

- d Add an `\etc` folder to the `\media` directory.
 - e Copy the `rps.cfg` file to this platform-specific `\media\etc` folder. For example, if the Management Portal is installed on `C:\Novadigm\IntegrationServer`, and the 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`
- 3 Run the Install Proxy Server task from the Management Portal, as usual. The installation task will also transfer the fully configured `rps.cfg` file.

Synchronizing the Proxy Server

Use the Synchronize Proxy Server task to force the Proxy Server to connect to the Configuration Server to preload the files to the static cache on the Proxy Server. The task is available for devices whose properties include a 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 Proxy Server to enable the task. For details, refer to Adding Services on page 195.

See the Proxy Server Guide for more information on the Proxy Server.

To synchronize one or more Proxy Servers

- 1 Use the Navigation aid to select the Proxy Server(s) that you want to synchronize.
 - To synchronize an individual Proxy Server, navigate to the Device's properties from a Group or Device container, and select the service for the Proxy Server.
 - To synchronize all Proxy Servers identified by the Radia Management Agents in a Zone at once, navigate to the 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 281.

- 4 Click **Next**.

The Submit Synchronize—Summary dialog box opens.



- 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 Proxy Server.
- Start of session between Proxy Server and Configuration Server (for preloading the files to the static cache on the Proxy Server).
- Job successful.

See [Viewing Properties](#) on page 264 for more information.

Purging the Dynamic Cache of the Proxy Server

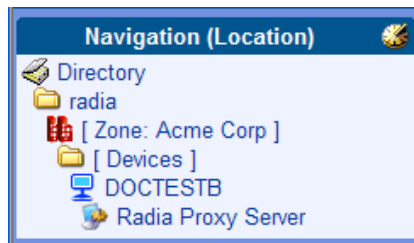
Use the Purge Proxy Server Dynamic Cache task to purge the dynamic cache of the Proxy Server. The task is available for Devices whose properties include a Proxy Server (cn=rps) service.

- For devices that have a Radia Management Agent installed, a Proxy Server service is automatically discovered. Once discovered, it will be listed in the Zone's Cross References Container within the Infrastructure Services group for Proxy Servers.
- For devices that do not have a Radia Management Agent installed, you can manually add a service for the Proxy Server to enable the task. For details, refer to Adding Services on page 195.

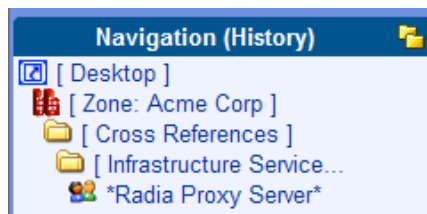
See the Proxy Server Guide for more information.

To purge the dynamic cache of the Proxy Server

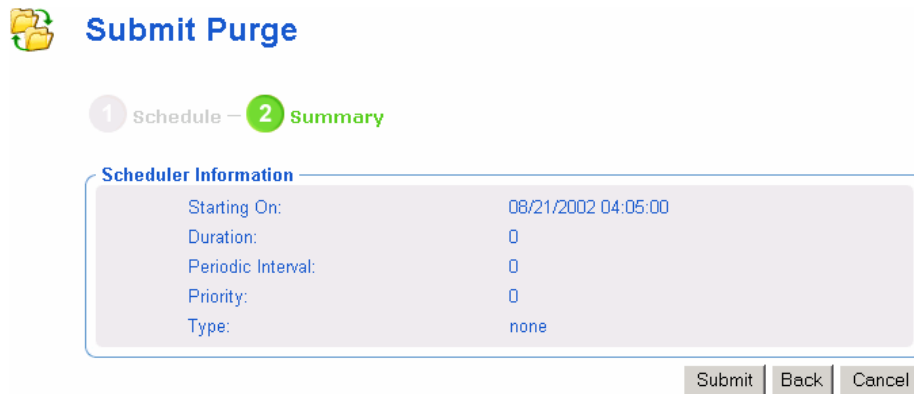
- 1 Use the Navigation aid to select the Proxy Server service on the Device or group of devices whose cache you want to purge.
 - To purge the dynamic cache of an individual Proxy Server, navigate to the Device's properties from a Group or Device container, and select the service for the Proxy Server. The following figure shows a sample location of a Proxy Server on a single device:




- To purge the dynamic cache of all Proxy Servers identified by the Radia Management Agents in a Zone at once, navigate to the Radia Proxy Server group. This group is located in the **Zone** → **Cross References** → **Infrastructure Services** container, as shown in the following figure.



- 2 In the Operations task group, click **Purge Proxy Server 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 281.
- 4 Click **Next**.
The Submit Purge—Summary dialog box opens.



- 5 Click **Submit**.

A list of the jobs 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 264 for more information.

Managing Services

Use the 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 any of the following Zone locations: the Devices container, the Groups container, or the 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.



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 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

- 1 Use the Navigation aid and workspace to go to **Zone** → **Configuration** → **Task Templates**.

The existing Task Templates (if any are available) are displayed in the Workspace.



- In the Operations task group, click **Add Task Template**.

The Add Task Template options page opens.

Add Task Template

1 Task-template-opts — 2 Summary

Task

Task Type

Task Name

- Use the Task Type drop-down menu to select the type of task for which you are adding a template.

➤ 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.

➤ 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 283.
- To complete Install Proxy tasks, see Installing the Proxy Server on page 315.

- Click **Next**.

The Add Task Template Summary page opens.

Add Task Template

1 Task-template-opts — 2 **Summary**

Task

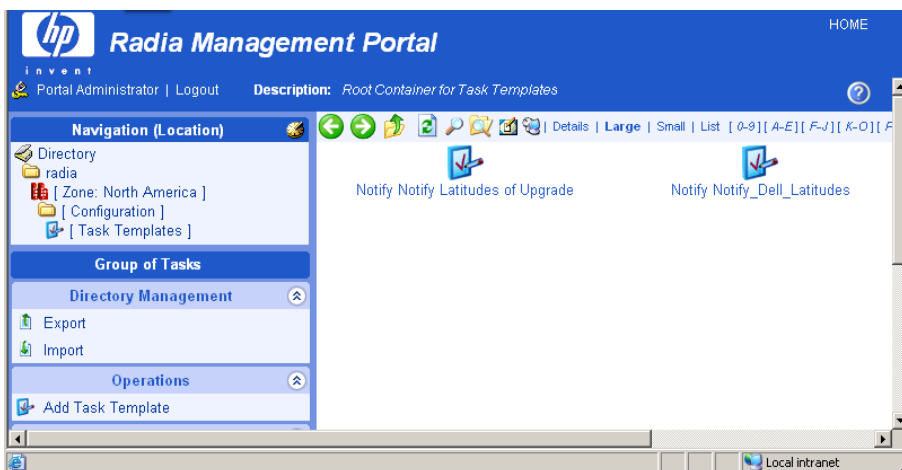
Task Type :	Notify
Task Name :	Notify Latitudes of Upgrade

Selected Options

Display Name :	Full Connect
Command :	radskman req="Refresh Catalog",mname=EastCoast,dname=SOFTWARE,ip=10.10.10.2,port=3464,cat=y
Port Number :	3465
User :	user1

- 7 Review the Selected Options. To change them, click **Back** and revise the options. To save them, click **Submit**.
- 8 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.



Removing Task Templates

To remove task templates

- 1 Navigate from the Directory to the Zones, Configuration, Task Templates container.
- 2 Click on the task template to be deleted.
The Workspace displays the object for the selected Task Template.
- 3 In the Model Administration Task group, click **Remove**.
A message asks you to confirm the removal of the template.
- 4 Click the green checkmark ✓ to confirm the removal.



Remove Task Template

"Notify Notify_Dell_Latitudes" has children

Are you sure you want to remove this object and all its children? ✓ ✕

Selective Delete of Child Objects

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.

- 5 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.

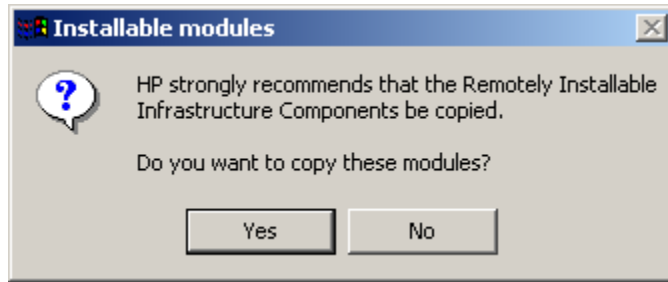
Installing Additional Management Portal Zones (Subordinate Zones)

Once your initial Management Portal zone is installed, you can use the Management Portal to remotely install additional Management Portal zones in your enterprise. These zones are called subordinate zones.

Prerequisite for Install Management Portal task

- The media that is needed to run the Install Management Portal task must be stored in the Radia Integration Server \media directory, in a structure that mirrors the original Management Portal installation media.

- The Management Portal installation program, `setup.exe`, automatically copies the needed files to the appropriate locations when you select **Yes** to the following prompt:



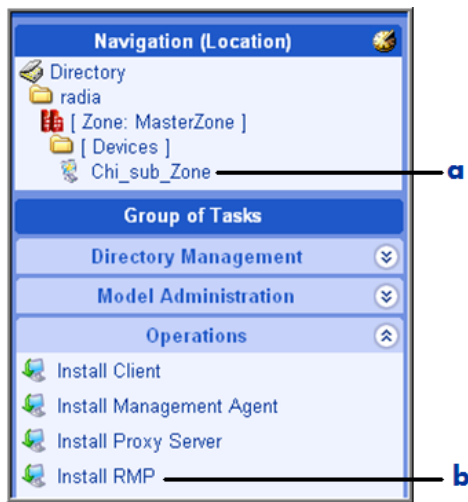
- To verify that your Management Portal includes the needed install media, you can check that the following directory structure exists:


```
<<RMP_install_directory>>\media\extended_infrastructure\management_portal\\
```
- 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 32 for more information.

To install a Management Portal Zone from the Master Zone

- 1 Login to the Master Zone Management Portal as **Admin**.
- 2 The device on which you are installing the Management Portal 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 175.) After adding the device, navigate to and display the Device Properties.



Legend

- a** Locate device.
- b** Select Install Management Portal.

- 3 Click **Install Management Portal** in 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 19 Zone Options for the Install Management Portal task

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.
Zone Display Name	Chicago Sub Zone	Zone display name is the label for the Zone object in the Management Portal.
RIS Port	3466	The port number of the Management Portal Radia Integration Server (RIS) service. Default is 3466.
RIS Install Directory	C:/Novadigm/ IntegrationServer	The base directory for the Management Portal on the remote device. Important: Use <i>forward</i> slashes for both Windows and UNIX path syntax.

Field	Example	Description
RIS Service Name Suffix	ChicagoRMP	<p>Optional entry. If used, this suffix is appended to the Radia Integration Service (RIS) name, httpd, to allow for a distinct entry from other RIS entries that may be running on the same server.</p> <p>If a suffix is entered, the Management Portal install checks to see if there is an existing service with this suffix to allow for a refresh of that service. If there is no existing RIS service with this suffix, the Management Portal install only continues if the above RIS directory is empty.</p> <p>Note: If you enter a suffix, then append this suffix to the <httpd> entry when you start or stop the Portal from a command line. For example:</p> <pre>nvdkit start httpdChicagoRMP.tkd nvdkit stop httpdChicagoRMP.tkd</pre>

Table 20 Remote Client Credentials for the Install Management Portal task

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	A Management Portal 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.

4 After completing all entries, click **Next**.



Install RMP

1 Query – 2 Select – 3 Rmp-opts – 4 Schedule – 5 Summary

Zone Options

Zone Name	<input type="text" value="Chicago"/>
Zone Display Name	<input type="text" value="Chicago"/>
RIS Port	<input type="text" value="3466"/>
RIS Install Directory	<input type="text" value="C:/Novadigm/IntegrationSe"/>
RIS Service Name Suffix	<input type="text" value="ChicagoRMP"/>

1 item selected

Remote Client Credentials

Select Client Port: Dynamic Static

User:

User Password:

Confirm Password:

Next Back Cancel

The Schedule panel (Step 4 of 5) of the Install RMP page opens. The default schedule is to run the Install RMP task immediately.

- 5 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.



Install RMP



- 1 Query – 2 Select – 3 Rmp-opts – 4 Schedule – 5 **Summary**

Selected Audience	
PHU1683	

Selected Options	
Zone Name :	Chicago
Zone Display Name :	Chicago
RIS Port :	3466
RIS Install Directory :	C:/Novadigm/IntegrationServer
RIS Service Name Suffix :	ChicagoRMP

Install Options	
Client Port Number:	Dynamic
User:	Administrator

Scheduler Information	
Starting On:	04/24/2004 15:40:00
Duration:	0
Periodic Interval:	0
Priority:	0
Type:	none

- 6 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 .
 - To refresh the status, click .
- 7 When the install job finishes, the 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 Start 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 Management Portal Zones

After you install an update to the Master Portal for a service pack or release, use the Update Management Portal task in the Operations task group to propagate the code updates to the Subordinate Management Portal Zones in your enterprise. This task allows you to synchronize the build numbers of the Management Portal modules throughout the Zones in your enterprise.

- ▶ 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 to be applied by the Update Management Portal task in the necessary media location.

To apply code updates to Subordinate Zones from the Master Zone

- 1 From the Master Portal, navigate to the Zone Access Points container.



- 2 To update all Management Portal Zones at once, click **Update Management Portal** from the Operations task group.

or

To update a single Zone, select the individual Zone object and click **Update Management Portal** 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 295 for more information.

Scheduling Zone Operations

Scheduling Zone Operations using the ZoneJob task requires you to have the following objects in your Zone directory:


- Zones in the Zones Access Points container. When you use the Install Management Portal task 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 88.
- Task Templates for the job being scheduled. For details, see *Managing Task Templates* on page 324.
- 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*.

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 **Zone** → **Zone Access Points** container to schedule zone operations for one or more zones.



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  on the toolbar above the Workspace.

- 2 In the Operations task group, select the **ZoneJob** task.

The Schedule Zone Operations - Query window opens for you to Query and Select the zones to be included in this schedule.



Submit Schedule Zone Operation

1 Query – 2 Select – 3 Zonejob-opts – 4 Schedule – 5 Summary

Type of Query

Query Depth:

Current Object

One Level

Current Level & All Below

Query Filter:

Query Constraints

Match All Constraints?:

Common Name:

DNS Host Name:

Port Number:

- 5 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.

- 6 Move the zones for the job to be scheduled to the Selected column using the Arrow icons, or, by double-clicking on an entry.



Submit Schedule Zone Operation

1 Query – 2 **Select** – 3 Zonejob-opts – 4 Schedule – 5 Summary

The screenshot shows a window titled "Submit Schedule Zone Operation" in the "Select" step. It has two columns: "Available" and "Selected". The "Available" column contains the text "Zone: Gregg" and "Zone: vlad". The "Selected" column is empty. Between the columns are four navigation buttons: a right arrow, a right arrow with a plus sign, a left arrow with a minus sign, and a left arrow. At the bottom of the window are three buttons: "Next", "Back", and "Cancel".

- 7 Click **Next** to schedule the job against the zones listed in the Selected column.

The Submit Schedule Zone Operation – ZoneJob opts window opens.



Submit Schedule Zone Operation

1 Query – 2 Select – 3 **Zonejob-opts** – 4 Schedule – 5 Summary

The screenshot shows a window titled "Submit Schedule Zone Operation" in the "Zonejob-opts" step. It has a section titled "Zone Job Name" with two dropdown menus: "Task Template" and "Group". The "Group" dropdown is open, showing a list of device groups: "Radia MSI Redirector", "Radia Messaging Service", "Windows XP", "Dell", "Dell Computer Corporation", "Dell Computer Corp.", "Sales Information", "Amortize", "Service Pack 1", "Latitude", and "Latitude D600". At the bottom right of the window are three buttons: "Next", "Back", and "Cancel".

- 8 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 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 the next figure 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.

Submit Schedule Zone Operation

1 Query – 2 Select – 3 **Zonejob-opts** – 4 Schedule – 5 Summary

Zone Job Name

Task Template: Notify_Dell_Latitudes

Group: Latitude

Next Back Cancel

- 9 Click **Next** to add a schedule to the zone operation.

The Submit Schedule Zone Operations – Schedule window opens.



Submit Schedule Zone Operation

1 Query – 2 Select – 3 Zonejob-opts – 4 **Schedule** – 5 Summary

Scheduler Information

Job Name:

Description:

Priority:

Time Window

Run:

Starting on: at

Duration: hours minutes


Job Throttling

Have a maximum of jobs running at any time,
and start them in batches of jobs per minute.

- 10 In the Scheduler Information area, enter a Job Name, such as **Notify Latitudes of Upgrades**. If desired, modify the Description and Priority.
- 11 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.
 - ▶ You can select **Do Not Schedule** to save the Job and select the Job for use in the Sequence Tasks operation.
- 12 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.
- 13 Click **Next** to review the summary and submit the job.

The Submit Schedule Zone Operation – Summary window opens.
- 14 Click **Submit** to submit the job for the selected zones.
- 15 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.

Display Name	Status	Created by
{Zone: Chicago Sub Zone}	Currently Active	Portal Administrator
{Zone: North America}	Currently Active	Portal Administrator
{Zone: Paris}	Currently Active	Portal Administrator

- 16 To View Job Properties for any of these zone jobs, click on the job listing, then click on the View Properties toolbar icon .

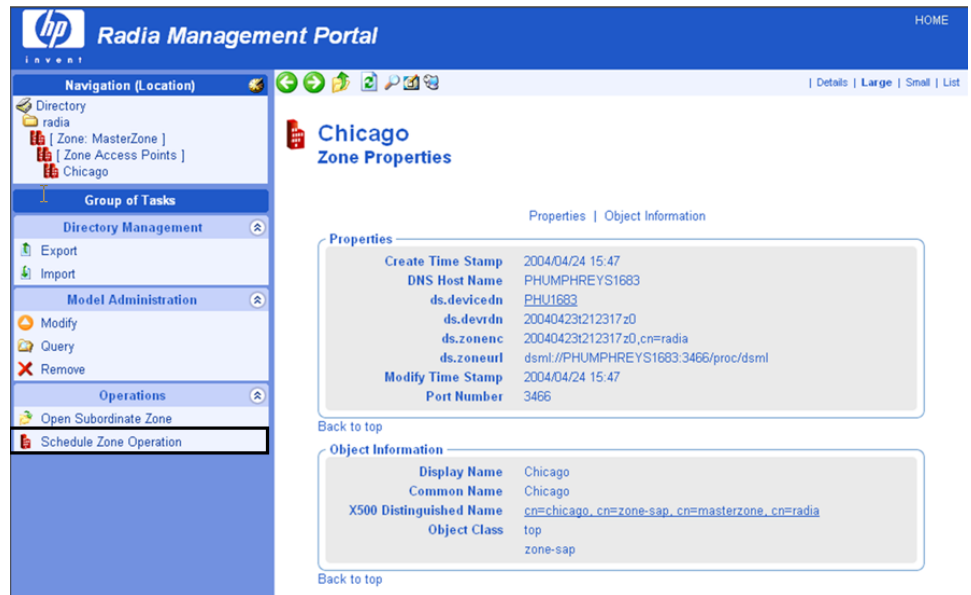
What happens with jobs scheduled from Remote Zone Operations?

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 a managed zone object in the Zone Access Points container, and then click **Open Subordinate Zone** in the Operations task group. The following figure shows a sample navigation location for opening a subordinate zone.



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 is Notify Dell Latitudes. The zone audience included the Zone of Chicago.



Select the [**Notify Dell Latitudes Job Group**] to see the Job details.

Display Name	Status	Created by
notify:Notify_Dell_Latitudes	Successful	

To exit a Zone, click **Logout** in the banner area above the Navigation aid, and close the Browser window.

Sequencing Jobs (In Progress)

Use Sequence Job 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 **SequenceJob** in the Operations task group.

Submit Job Sequence

1 Sequencejob Opts - 2 Schedule - 3 Summary

Task Sequence

Task Sequence

Next Back Cancel

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 VNC Distribution through the Management Portal. TightVNC: Enhanced VNC Distribution is a freely redistributable 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>.



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

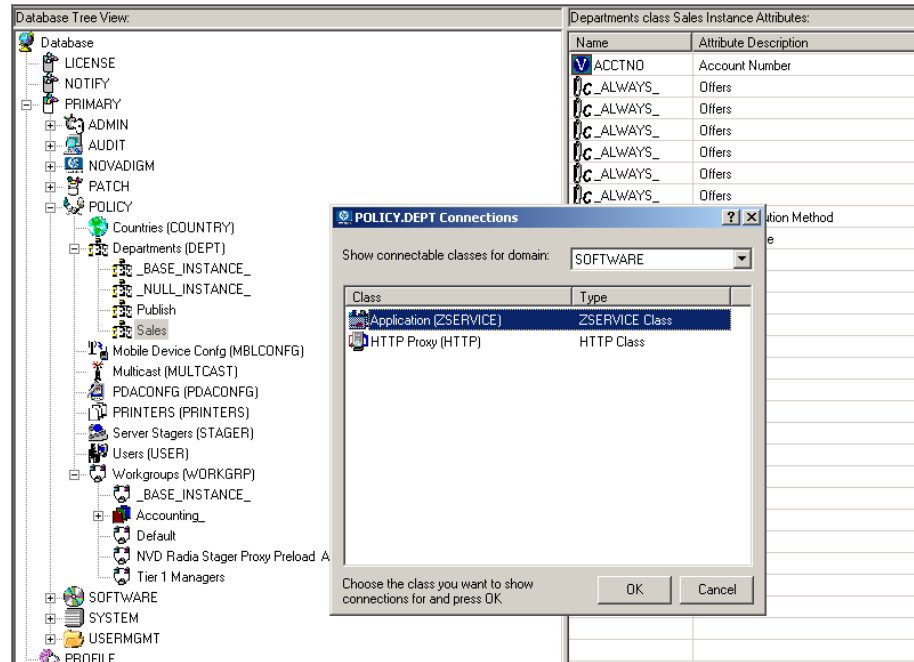
- Ability to use the Radia System Explorer.
- Ability to distribute applications (with the Radia Client or using a Notify operation).
- In the ZSERVICE class of the Radia Database, the service installation methods (such as ZCREATE and ZDELETE) must be set to a length of at least 57 characters to prevent 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 Management Portal.

Connecting the Remote Control Service to Users

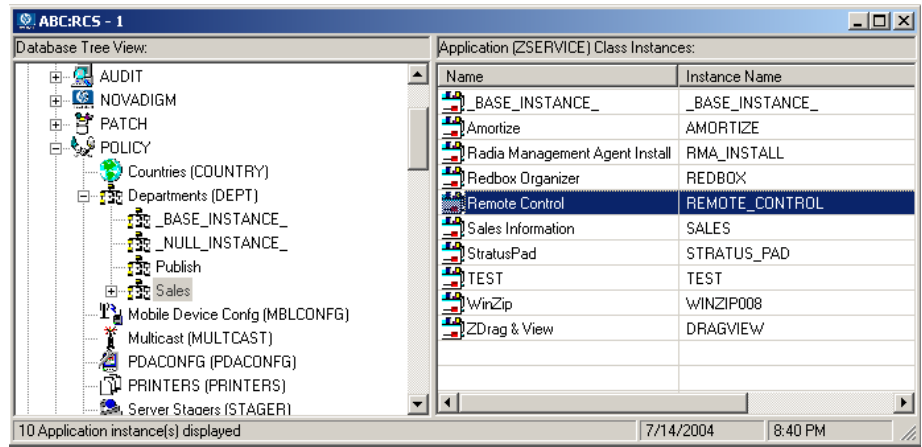
Use the Radia System Explorer on the Radia Administrator's Workstation to connect the Remote Control Service to the appropriate users, servers, or groups, representing the devices to be managed by Radia. Make a service connection between the Application (ZSERVICE).Remote Control service and the appropriate class instance in the PRIMARY.POLICY domain, such as a USER, DEPT, or WorkGRP class instance.

To connect the remote control service to users

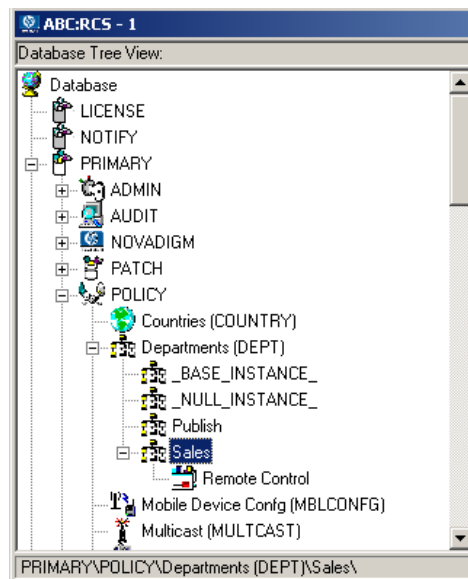
- 1 Use the Radia System Explorer and go to the PRIMARY.POLICY domain.
- 2 Navigate to the appropriate DEPT, USER, or WorkKGRP class instance you want connected to the Remote Control Service. The next figure uses the Sales Department instance as an example.
- 3 Right-click the selected instance (in the 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.



- 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.



- 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.



Now you can distribute the Remote Control service to the devices to be managed using the Radia Client or the Notify task.

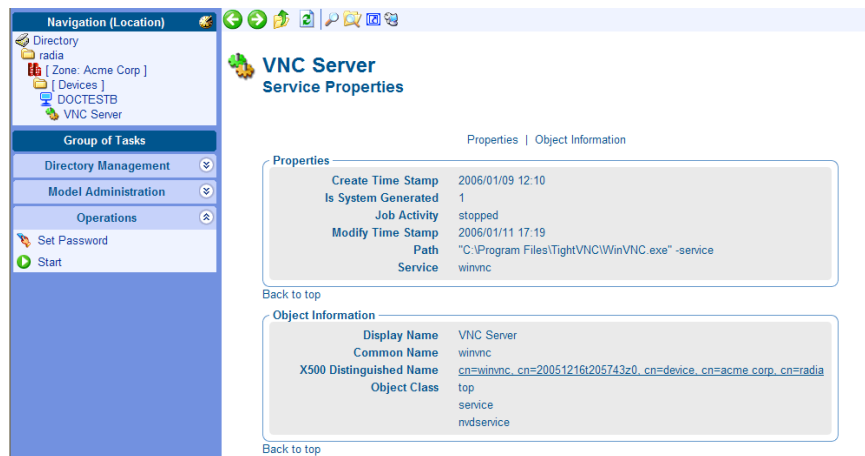
Using Remote Control (*Windows Clients Only*)

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.

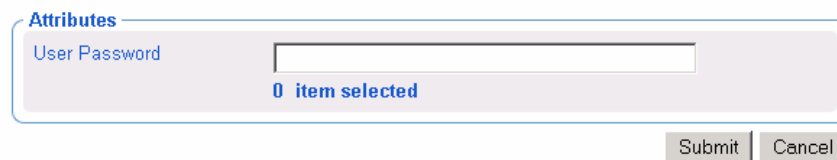


The screenshot shows a management console interface. On the left is a navigation pane with a tree view containing 'Directory', 'radia', '[Zone: Acme Corp]', '[Devices]', 'DOCTESTB', and 'VNC Server'. Below the tree is a 'Group of Tasks' section with 'Directory Management', 'Model Administration', and 'Operations'. The 'Operations' group is expanded, showing 'Set Password' and 'Start'. The main content area is titled 'VNC Server Service Properties' and has two tabs: 'Properties' and 'Object Information'. The 'Properties' tab is active, showing a table of service details: Create Time Stamp (2006/01/09 12:10), Is System Generated (1), Job Activity (stopped), Modify Time Stamp (2006/01/11 17:19), Path ('C:\Program Files\TightVNC\WinVNC.exe' -service), and Service (winvnc). Below this is an 'Object Information' section with a table: Display Name (VNC Server), Common Name (winvnc), X500 Distinguished Name (cn=winvnc, cn=20051216a205743z0, cn=device, cn=acme_corp, cn=radia), and Object Class (top, service, nvdservice).

- 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.

Set Password



The dialog box has a title bar 'Attributes'. Below the title bar is a text input field labeled 'User Password'. Below the input field, it says '0 item selected'. At the bottom right of the dialog box are two buttons: 'Submit' and 'Cancel'.



- 4 In the User Password text box, type the password for the VNC session.

- 5 Click **Submit**.


The VNC Properties Service dialog box opens.

- 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  if you want to refresh the page to display the latest status.
- Click  to view detailed information, such as the status of the installation.

When you are done viewing the job status, click  to close the Job Status page, and return to the Management Portal.

- 7 In the workspace, click  to refresh the view and see that the service started.

VNC Server Service Properties

Properties | Object Information

Properties

Create Time Stamp	2006/01/09 12:10
Is System Generated	1
Job Activity	started
Modify Time Stamp	2006/01/11 17:19
Path	"C:\Program Files\TightVNC\WinVNC.exe" -service
Service	winvnc

Back to top

Object Information

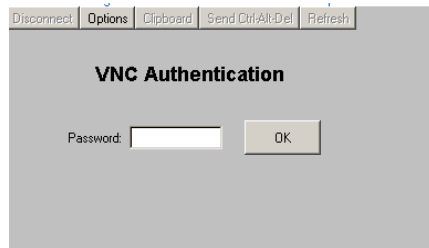
Display Name	VNC Server
Common Name	winvnc
X500 Distinguished Name	cn=winvnc, cn=20051216t205743z0, cn=device, cn=acme corp, cn=radia
Object Class	top service nvdservice

Back to top

Legend

- a** The service has started.
- 8 In the Operations task list, click **Start Viewer** to start the VNC session. A prompt for VNC authentication opens.

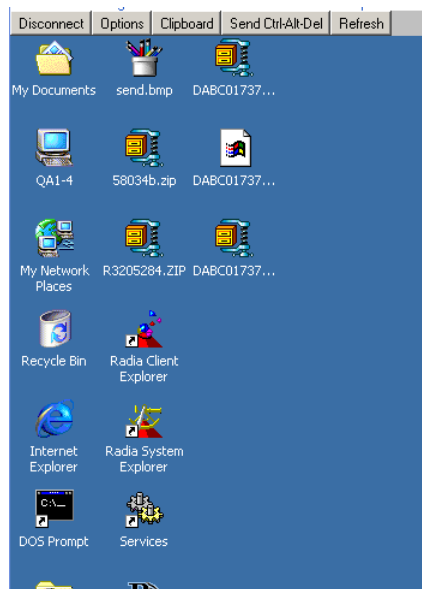
- ▶ If your Web browser does not support Java applets, you may see this message "Refresh this Page for Remote Authentication Prompt". Be sure to install the Java component.



- 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.

- ▶ 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 Management Portal. For details, see the topic Customizing the Start Viewer Task Properties on page 348.



- ▶ The initial request temporarily uses Port 5800. The connection uses Port 5900.

To disconnect the VNC session

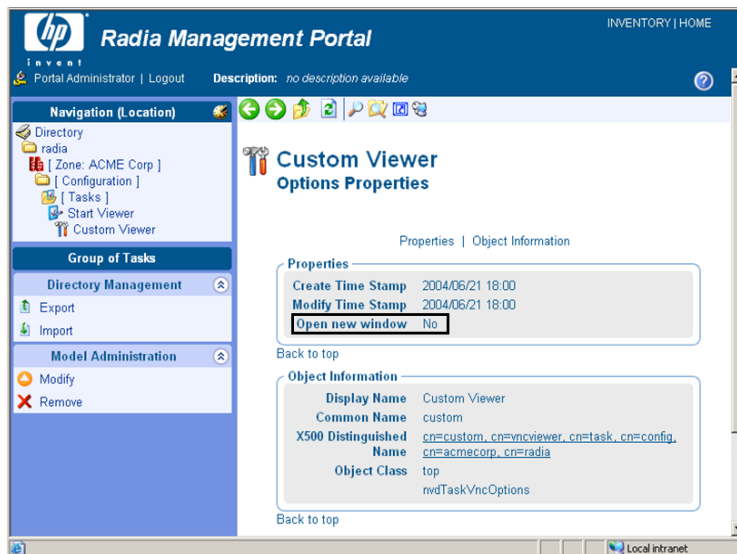
- 1 At the top of the workspace, click **Disconnect** to disconnect the session. If you browse to another page in the Management Portal, the session will automatically be disconnected.
- 2 Click **Stop** in the Operations task group to stop the VNC server. You may need to click  to refresh the view and see that the service started.

Customizing the Start Viewer Task Properties

You can customize the Start Viewer task of the Management Portal to display the remote session in a new window, as opposed to displaying the remote session within the Management Portal workspace area (the default). To do this you will modify the Start Viewer task from the Management Portal before you begin the VNC session.

To customize the Start Viewer Task from the Management Portal

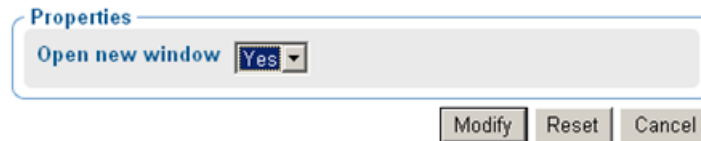
- 1 Navigate to the Zone → Configuration container.
- 2 In the workspace, click **Tasks**.
- 3 Browse to and select the **Start Viewer** task.
- 4 Select **Custom Viewer**.
- 5 The Options Properties dialog box opens.



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 Management Portal.
 - **Yes** means the remote session is displayed in a new, separate window.
- 6 To modify the Open new window property, click **Modify** in the Model Administration task group.
 - 7 The Modify Options dialog box opens. Use this dialog box to change the value for the Open new window property.

Modify Options



The screenshot shows a dialog box titled "Properties". Inside the dialog, there is a label "Open new window" followed by a dropdown menu currently set to "Yes". Below the main content area, there are three buttons: "Modify", "Reset", and "Cancel".

- 8 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 Management Portal.
 - **Yes** means the remote session is displayed in a new, separate window.
- 9 Click **Modify** to save your selection.

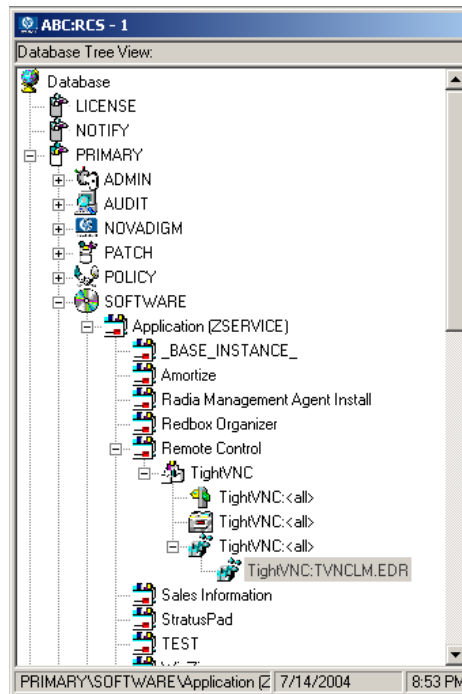
Configuring Remote Control

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

- 1 Go to **Start** → **Programs** → **Radia Administrator Workstation** → **Radia System Explorer**.
- 2 In the Radia System Explorer Security Information dialog box, type your User ID and Password, and then click **OK**.

- 3 Go to **PRIMARY** → **SOFTWARE** → **Application (ZSERVICE)** → **Remote Control**.
- 4 Double-click **TightVNC** and then double-click the registry resource for TightVNC (the last one).



- 5 Right-click **TightVNC:TVNCLM.EDR** and select **Edit Registry Resource**.
- 6 Navigate to WinVNC3 to view the local machine-specific settings.

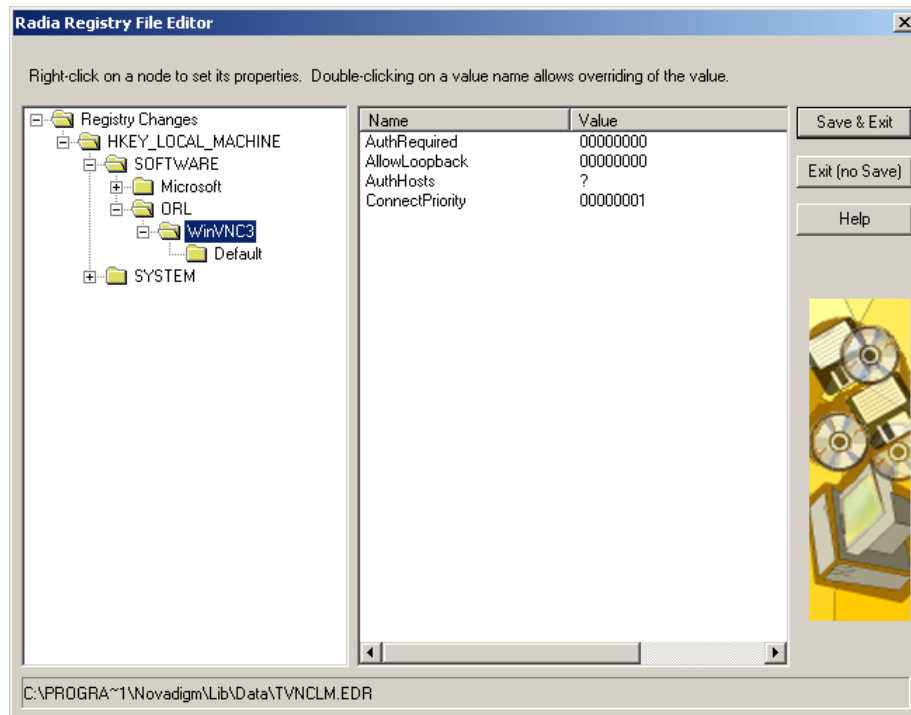


Table 21 Local Machine-Specific Settings for TightVNC Service

Field	Description
AuthRequired	<p>Set AuthRequired = 1 (default) to ensure that a password is set when you start the service.</p> <p>Set AuthRequired = 0 to disable null password checking by WinVNC.</p> <p>Use DWorD format.</p>
AllowLoopback	<p>Set AllowLoopback = 0 to disable the ability to remote control the local machine.</p> <p>Set AllowLoopback = 1 to allow the ability to remote control the local machine.</p> <p>Use DWorD format.</p>

Field	Description
AuthHosts	<p>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:</p> <ul style="list-style-type: none"> - 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 authorized to connect <p>Example: +192.10,-192.10.12</p> <p>This parameter is used in conjunction with the QuerySettings parameter.</p> <p>Use STRING format.</p>
ConnectPriority	<p>By default, the TightVNC server disconnects existing connections when a non-shared connection authenticates.</p> <p>You can change this behavior by setting this value to:</p> <ul style="list-style-type: none"> 0 - to disconnect all existing connections 1 - to continue all existing connections. 2 - to refuse any new connections. <p>Use DWorD format.</p>

7 Click **Default** to see the local default user properties that you can set.

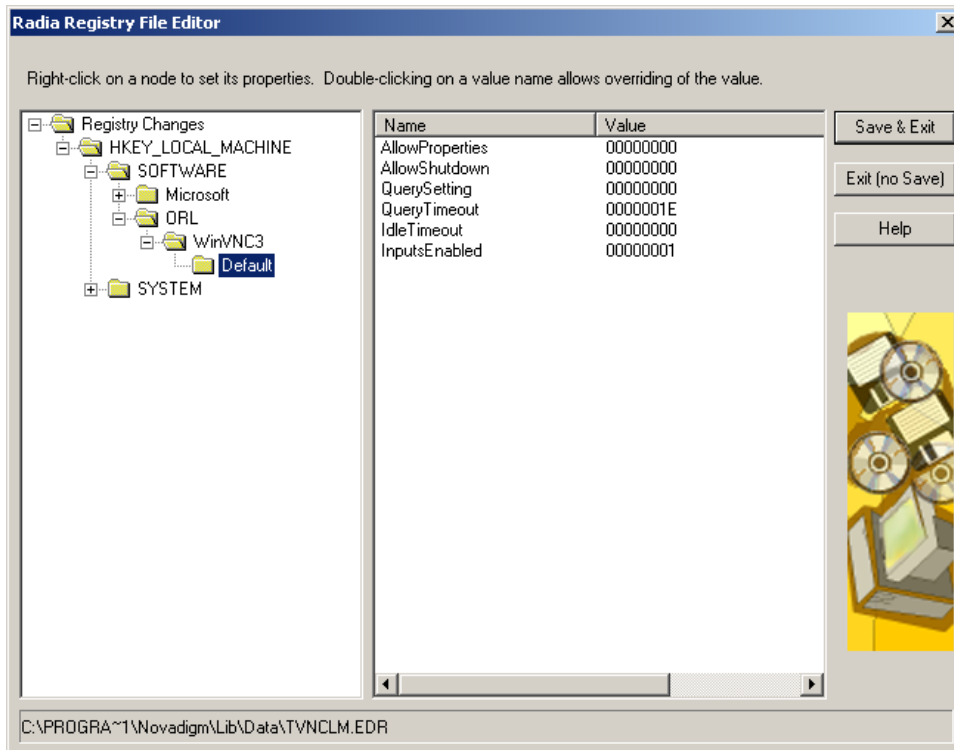


Table 22 Local Default User Properties for TightVNC Service

Field	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.

Field	Description
QuerySetting	<p>Sets whether you want to prompt the user about an incoming connection. This setting must be used in conjunction with AuthHosts.</p> <p>Set this value to:</p> <p>0 or 1 – Does not prompt on incoming connection. 2 – Prompts on incoming connection (default).</p> <p>Use DWorD format.</p>
QueryTimeout	<p>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.</p> <p>Use DWorD format.</p>
IdleTimeout	<p>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.</p> <p>Use DWorD format.</p>
InputsEnabled	<p>Allows incoming connections to send input.</p> <p>If InputsEnabled = 1 you can interact with the remote computer.</p> <p>If InputsEnabled = 0 you can view the remote computer, but cannot interact with it.</p> <p>Use DWorD format.</p>

Summary

- Bring computers in your network under control of the Management Portal using the Manage Computer task. This is required before performing any other operation from the Portal.
- Each task in the 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 Management Portal's media directory.
- Use the Install Management Agent task to deploy the Radia Management Agent on remote devices.
- Use the Install Radia Client task to deploy the Radia Clients to remote devices.
- Use the Install Proxy Server task to deploy the Proxy Server to remote devices.
- Use the Synchronize Proxy Server task to preload files from the Configuration Server to the static cache on the Proxy Server.
- Use the Purge Proxy Server Dynamic Cache task to purge the dynamic cache of the Proxy Server.
- You can use the Start, Stop, Pause, Restart, and Resume tasks to manage remote infrastructure products.
- Use the Install Management Portal 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 Management Portal task to apply the code delivered in a new build of the Management Portal to the remote Management Portal 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 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 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 Management Portal for Windows.

The log files are:

- `httpd-port.log`
This is the main log for the Management Portal. It contains information about the actions that you perform in the Management Portal, operational statistics, as well as the version and build number of the 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 360 for more information.

To change the trace level for the logs

- 1 Open the file
SystemDrive:\Novadigm\IntegrationServer\etc\httpd.rc
for Windows, which is located on the computer that is running the 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

```

- 2 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 23 Trace Levels

Trace Level	Description
0	No logging.

Trace Level	Description
1	Logs errors only.
2	Logs warnings and errors.
3	Logs informational messages, warnings, and errors. <i>Recommended trace level setting for customers.</i>
4	Logs all debug information. <i>Recommended for experienced customers only.</i>
5 - 9	Full trace <i>Not recommended for customer use.</i>

- 3 Save the file changes and restart the Radia Integration Server service.

Common Message Types

The following message types are used in the main Management Portal log (`httpd-port.log`).

Table 24 Common Message Types

Message Type	Description/Example
Info	<p>Provides general information. For example:</p> <pre>20010913 12:37:55 Info: LdifImport/4: BEGIN</pre> <p>Indicates that a job to import an LDIF has begun.</p> <pre>20010913 12:37:55 Info: RMP: Starting Scheduler...</pre> <p>Indicates that the RMP Scheduler service is started.</p> <pre>20010913 12:37:55 Info: RMP: Management Portal ready</pre> <p>Indicates that the Management Portal is up and running.</p>

Message Type	Description/Example
Audit/success	<p>Indicates a successful change to an object in your Management Portal Directory.</p> <p>For example:</p> <pre>20010913 12:46:43 Audit/success: RMP: (who/admin) add: uid=jbanks, cn=opsys,ou=who</pre> <p>Indicates that a new user was added.</p>
Audit/failure	<p>Indicates an unsuccessful change to an object in your Management Portal Directory.</p> <p>For example:</p> <pre>20010913 16:26:31 Audit/failure: RMP: (who/admin) add: uid=Guest, ou=who, object "uid=guest,ou=who" already exists</pre> <p>Indicates that you were not able to add a user with the ID Guest to the organizational unit "who" because it already exists.</p>
Error	Indicates a critical problem.
Warning	<p>Indicates a non-critical problem.</p> <pre>20010913 16:20:42 Warning: to: output to 1 job-create-reply 2 resume: no gate</pre>

Collecting Information for HP Technical Support

If you need to contact HP Technical Support for assistance, be sure to collect the following information:

- 1 The log directory, stored by default in the following locations:

For Windows, `SystemDrive:\Novadigm\IntegrationServer\logs`

- 2 Version information for `nvdkit.exe`. See [Viewing and Logging Version Information](#), below.

- 3 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 239 for information about these files.


- 4 The `etc` directory files and complete `etc/zone` subdirectory contents), stored by default in the following location:

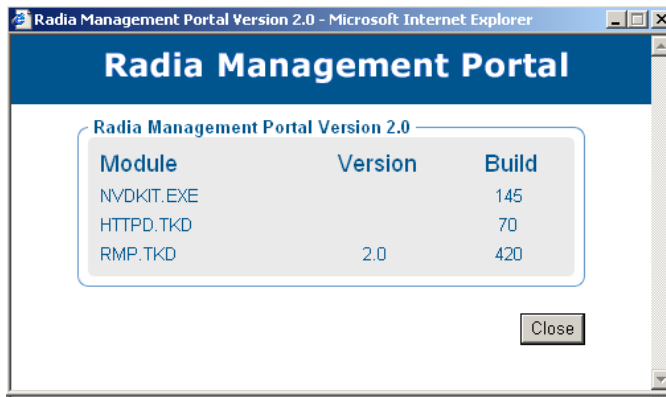
`/opt/Novadigm/IntegrationServer/etc`

The `etc/zone` subdirectory holds the `*.mk`, `*.ldif`, and `*.chkp` files for loading all objects in a 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 and Logging Version Information

After logging into the Management Portal, click the Information button  on the banner area to open the Version Information Window. A sample window is shown in the following figure.



This window displays the installed Module, Version, and Build levels for the Management Portal, including component modules `NVDKIT.EXE`, `HTTPD.TKD`, and `RMP.TKD`. Whenever this window is displayed, the version and build levels for each module are also written to the Management Portal log (`httpd-port.log`).

Gathering Version Information for NVDKIT.EXE

Use this command-line method of obtaining version information for `NVDKIT.EXE` as an alternative to viewing and logging it from the Version Information window of an active 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.

```
C:\WINNT\System32\cmd.exe
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.

C:\>d:
D:\>cd nov*
D:\Novadigm>cd radia int*
D:\Novadigm\Radia Integration Server>nvdkit version
Kit Version: 2.1
Tcl Version: 8.2.2+

D:\Novadigm\Radia Integration Server\nvdkit.exe:
module nvdkit, build 116 20020227 14:01:56 UST
module tclkitsh, build 42 20020226 21:37:12 UST
module lib/nvd.sql, build 16 20011108 17:44:46 UST
module lib/nvd.tcl, build 48 20020226 21:45:10 UST
module lib/vfs, build 12 20011217 21:36:48 UST

D:\Novadigm\Radia Integration Server>
```

➤ The `httpd-port.log` also contains version and build information.

Gathering Version Information for RADISH.EXE

Radish.exe runs on the 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 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.


```
C:\Novadigm\ConfigurationServer\bin>radish version
Adapter Version: 2.1
Kit Version: 2.1
Tcl Version: 8.2.2+

C:/Novadigm/ConfigurationServer/bin/radish.exe:
module nvdkit, build 120 20020412 19:05:06 UST
module nvdmtcl, build 44 20020426 15:58:28 UST
module tclkitsh, build 43 20020318 21:31:04 UST
module lib/nvd.sql, build 17 20020412 19:04:16 UST
module lib/nvdtcl, build 50 20020411 21:56:50 UST
module lib/vfs, build 13 20020412 19:01:26 UST

C:\Novadigm\ConfigurationServer\bin>_
```

- 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, the figure above illustrates a Configuration Server running Build 44 of `radish` (which is shown as module `nvdmtcl`, build 44 in the output).



`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 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 Management Portal Zones \(Subordinate Zones\)](#) on page 327.

Summary

- The `httpd-port.log` is the main log for the 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 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..

Index

A

- accessing, Radia Management Portal, 46
- Active Directory computer, managing, 274
- AD authentication. *See* LDAP Authentication
- Add Component to Instance task, 96
 - description, 81, 94
- Add Connections task. *See* Add Component to Instance task
- Add Connections window, 96
- Add Device task, 73
- Add Directory Service task, 73, 135
- Add Group (of devices) task, 73
- Add Install Profile, 309
- Add Install Profile task, 73, 309
- Add Job Sequence task. *See* Sequence Job task
- Add object-type task, 73
- Add Policy Object task, 79, 103, 104
- Add Shortcut to Desktop task, 62, 82
- Add Task Template task, 76, 270, 326
- adding
 - client install profile, 309
 - components to instances, 96
 - delegated administration role, 220
 - instances, 95
 - Notify command, 292
 - policy objects, 104
 - services, 195
 - task template, 326
 - user groups, 235
 - users, 230
- Administrators and Operators Container, 89
- AllowLoopback, 353
- AllowProperties, 355
- AllowShutdown, 355
- Notify task, 283
- Application Manager client, installing, 303
- architecture, 20
- Assign Proxy Server task, 76, 303, 312
- assigning

- devices to Radia Proxy Server, 313
- users to groups, 236

Attribute Editor, 166

audience

- notifying, 284
- selecting, 279, 280

authentication, 230

AuthHosts, 354

AuthRequired, 353

B

- backing up Radia Management Portal Directory, 239, 241
- Backup Directory task, 71, 239
- backup directory, maintenance, 241
- banner, 56
- job throttling, 258
- Browse and Modify window, 162
- Cross-References, 91

C

- cacert.pem file, 137
- changing passwords, 48
- Chassis Container, 89
- client install profile, 309
 - adding, 309
 - deleting, 312
 - modifying, 311
- Common Name syntax options, 246, 279
- components to instances
 - adding, 96
- computer groups, managing, 274
- computers, managing, 272
- Configuration Container, 89
- configuring
 - delegated administration, 219
 - groups, 230
 - users, 230
- Confirm Password field, 332

- Connect to Directory Service task. *See* Start Directory Service task
- connection
 - removing, 100
- ConnectPriority, 354
- containers
 - description, 87
 - modifying, 198
 - removing, 199
- Copy Instance task, 81, 98
 - description, 94
- copying
 - instances, 98
- core functions
 - auditing, 20
 - authentication, 19
 - cross referenced device groups, 19
 - entitlement, 19
 - logging, 20
 - network discovery, 19
 - notify, 19
 - querying, 20
 - remote administration, 19
 - remote installations, 19
 - remote Radia Configuration Server and Policy Administration, 19
 - scheduling, 20
- Create Instance task, 81
 - description, 94
- Cross Reference Container object, 127
- Cross References container, 315
- Cross-References, 90
 - by Device Architecture, 90
 - by Device Manufacturers, 90
 - by Enclosure Manufacturers, 90
 - by Infrastructure Services, 90
 - by Operating Systems, 91
 - by Subnets, 91
- custom commands for notify operations, 292

D

- Daily jobs. *See* History container
- delegated administration
 - configuring, 219
 - querying, 228
- delegated administration role
 - adding, 220
 - modifying, 227
 - removing, 228
- Delete Instance task, 81, 99

- description, 94
- deleting client install profile, 312
- deleting instances, 99
- dependency, modifying, 117
- deploying Radia infrastructure, 295
- desktop
 - adding shortcuts, 62
 - returning to, 62
- details view, 92
- Device Architecture groups, 90
- Device Manufacturer groups, 90
- devices
 - moving into a group, 186
 - removing from a group, 189
- Devices Container, 91
- Directory Management task group, 249
- Directory object, 60
- Directory Service
 - definition, 25
 - removing, 149
 - starting, 150
 - stopping, 152
- Directory Services Container, 90
- Directory Services object, 126
- directory, navigating, 57
- Disable Job task, 262
- Disable task, description, 73
- disabling job groups, 262
- Disconnect from Directory Service task. *See* Stop Directory Service task
- disconnecting VNC session, 350
- Discovery Interval, 36
- Discovery Start Delay text box, 37
- dual-NIC cards and LISTENING_ADDRESS, 133
- Dynamic Cache. *See* Purge Proxy Server Dynamic Cache task
- dynamic IP address and LISTENING_ADDRESS, 133

E

- Enable Job task, 262
- Enable task, description, 74
- enabling Job Groups, 263
- Enclosure Manufacturers groups, 90
- entitlement, modifying, 219

Export task, 71, 247
exporting Radia Management Portal Directory, 247

F

failed jobs, restarting, 260
filtering jobs, 256
flags, modifying, 118
Force re-install of RMA, 299

G

global default policy, 219
group membership, 236
groups
 adding user groups, 235
 configuring, 230
 modifying, 237
 removing, 238
Groups Container, 92
Groups object, 126
groups of objects, 87

H

Help Desk Notify task, 76, 82, 271, 283, 287
History container, viewing, 263
history.mk, locating, 364
HOME link, 56, 62
httpd-3466.error.txt, 360
httpd-port.log, 360, 362, 366
httpd-port.YY.MM.DD.log, 360

I

icons
 Back, 83
 Forward, 83
 view properties, 83
IdleTimeout, 356
Import Device task, 74
Import task, 71, 249
importing Radia Management Portal Directory, 249
infrastructure
 configuring, 126
 managing, 126
 navigating, 86
Infrastructure Service groups, 90

Initialization File, 306
InputsEnabled, 356
Install Management Agent task, 296, 298
Install Management Portal task, 76, 331
 prerequisite, 329
install profiles, 309
Install Proxy Server task, 316
Install Radia Client task, 270, 303
 description, 77
Install Radia Management Agent, description, 76, 270
Install Radia Management Portal task, 271
Install Radia Proxy Server task, description, 76, 270
Install Zone task, 126
installing
 Management Portal
 CD-ROMS used, 30
 Management Portal
 preparation, 30
 Management Portal Zone, 330
 Radia Client, 303
 Radia Management Agent, 296, 299
 Radia Management Portal, 32
 Radia Proxy Server, 316
instance
 adding, 95
 copying, 98
 deleting, 99
 modifying, 99
interface
 banner, 56
 Toolbar, 82
 workspace, 86
interface Navigation aid, 57
Inventory Manager client, installing, 303
IP address, RMA-discovered, 297

J

Job Groups, 281
 disabling, 262
 enabling, 263
 modifying, 256
 querying, 258
 removing, 263
 stopping, 261
job history
 viewing, 264
job throttling, 282, 340

- batch size per minute, 282
- job limit, 282
- modifying, 257
- jobs
 - definition, 270
 - disabling, 262
 - enabling, 262
 - filtering by status, 256
 - managing, 255
 - priority, 281
 - querying, 258
 - removing, 263
 - scheduling, 281, 282
 - sorting, 281
- Jobs
 - sequencing, 343
- Jobs Container, 92
- Jobs running at any time (maximum), 257

L

- LDAP authentication
 - configuration parameters, 153
 - enabling, 153
 - modifying the default for users, 156
- LDAP data, transferring, 247
- LDAP objects
 - paging, 5, 84
- LDAP Policy Extension, custom value, 156
- LDAP_AUTH parameter, 155
- LDAP_AUTH_DN parameter, 155
- LDAP_AUTH_HOST parameter, 155
- LDIF, definition, 247
- lifecycle of a task, 275
- LINKS, 133
- LISTENING_ADDRESS, 133
- logging off, 44
- logging off Management Portal, 48
- logging on, 47
- logs
 - httpd-3466.error.txt, 360
 - httpd-port.log, 360, 366
 - httpd-port.YY.MM.DD.log, 360
 - message types, 362

M

- MAC address, RMA-discovered, 297
- maintenance backup directory, 241

- Manage Computer task, 270, 272
- Manage Proxy Assignment task. *See* Assign Proxy Server task, *See* Assign Proxy Server task
- managed device, definition, 25
- Managed Service groups, 91
- managed services cache, refreshing, 115
- Managed Sites, 26
- Management Portal
 - logging off, 48
- Management Portal Zone
 - installing, 330
 - updating code from a Service Pack, 335
- Management Portal Zone friendly name, 39
- Management Portal Zone Name, 38
- Management Portal Zones, updating, 44
- managing
 - Active Directory computers, 274
 - computer groups, 274
 - computers, 272
 - services, 325
 - mass delete, 199
- Master Portal, 25
- master zone, definition, 22, 25
- maximize, 70
- members. *See* users
- message types, 362
- metakit files, 239
- Microsoft Internet Explorer, security setting, 31
- minimize, 70
- Model Administration task group, description, 72
- Modify Instance task, 99
 - description, 81, 94
- Modify Policies task, 103, 105
- Modify Policy Defaults task, 80, 116, 119
- Modify Policy Dependencies task, 80, 116
- Modify Policy Flags task, 80, 116, 118
- Modify Policy Object task, 79
- Modify Policy Overrides task, 80
- Modify Policy Overrides task, 116, 121
- Modify Policy Targets task, 79, 103, 107
- Modify task, 198, 256, 257
 - description, 74
- modifying
 - client install profile, 311
 - delegated administration roles, 227

- groups, 237
- instances, 99
- Job Groups, 256
- Notify task, 288
- objects, 198
- passwords, 48, 233
- policies, 106
- policy defaults, 120
- policy dependencies, 117
- policy flags, 118
- policy overrides, 121
- policy targets, 107
- Radia Management Portal Directory, 249
- users, 233

mount point, definition, 25, 136

Move Device task, 74

multiple profiles, 308

N

navigating, 57

Navigation

- history, 58
- location, 59

Navigation aid, 65

- description, 57

NETSCAN parameter, 129

NETSCAN_INCLUDE_LIST parameter, 130

NETSCAN_POLL parameter, 36, 130

NETSCAN_START_DELAY parameter, 37, 130

Network Container, 92

Network Discovery, 127

- configuring, 128, 157
- delay start, 37
- job interval, 36

Network Discovery and Mount Points object, 126

network objects, viewing, 60

new containers, 89

Notify command, adding, 292

Notify task, 283, 284

- description, 77, 271
- Help Desk Tasks group, 82
- modifying, 288

Notify, Help Desk Notify task, 287

notifying

- audience, 284
- by device characteristics, 283
- by subscription, 283
- custom commands, 292

- default options, 288
- nvdkit.exe, version information, 365

O

objects

- modifying, 198
- removing, 199

Open Subordinate Zone task, 77, 271, 335, 341

Operating System groups, 91

operations policy, 219

Operations task group, description, 75

OS Manager client, installing, 303

overrides, modifying, 121

P

LDAP directory, 85

Paging and filtering icons, LDAP directory, 85

Paging LDAP objects, 5, 84

password

- changing, 48
- modifying, 233

Patch Manager client, installing, 303

Pause task, 325

Perform Connect After Install, 306

Perform Silent Install, 306

person. *See* users

policies, modifying, 106

Policy (advanced) task group, 80, 116

policy defaults, modifying, 120

policy dependency, modifying, 117

policy flags, modifying, 118

policy object

- adding, 104
- removing, 105

policy overrides, modifying, 121

policy targets, modifying, 107

Policy task group, 78, 103

policy tasks, configuring a custom LDAP prefix, 156

policy, resolving, 109

Port Number field, 332

Portal Directory

- accessing, 60
- navigating, 65

Portal Run-time, 20

- Portal tasks
 - updating, 253
- Portal Zone Directory, description, 20
- PREFIX parameter, 158
- PREFIX, adding to rmp.cfg, 156
- RPS.CFG file, 320
- Install Proxy Server task, 320
- prerequisites, remote control, 344
- priority jobs, 281
- properties, viewing, 364
- proxy assignments, 313
- Purge Dynamic Cache task
 - description, 271
- Purge Proxy Server Dynamic Cache task, 323
 - description, 77
 - periodic scheduling, 324
- purging dynamic cache, 324

Q

- query
 - Common Name syntax options, 246, 279
 - syntax options, 246, 279
- Query Constraints, 278
- Query Filter, 278
- Query Jobs task, 258
- Query Jobs, description, 74
- Query task, description, 74
- Query toolbar icon, 245
- Query User's Delegated Administration, description, 74
- querying, 278
 - delegated administration, 228
 - Radia Management Portal Directory, 245, 277
- QuerySetting, 356
- QueryTimeout, 356

R

- Radia Client, installing, 303
- Radia Information Base, 146
- Radia Managed Services, viewing, 315
- Radia Management Agent
 - description, 21
 - installing, 296, 299
 - log. *See* rma.log
 - port assignment, 298

- Radia Integration sub-service discovery, 302, 303
- refreshing, 303
- registration throttling feature, 296
- re-install options, 298
- task options, 298
- tasks, 297
- Radia Management Portal
 - accessing, 46
 - infrastructure, 86
 - installing, 32
 - LISTENING_ADDRESS, specifying, 133
 - log files, 360
 - logging off, 44
 - logging on, 47
 - prerequisites, 30
 - starting, 45
 - stopping, 46
 - version and build. *See* httpd-port.log
 - zone friendly name, 39
 - zone name, 38
- Radia Management Portal Directory
 - authentication, 230
 - backing up, 241, 247
 - backup, 239
 - exporting, 247
 - importing, 249
 - modifying, 249
 - querying, 245, 277
 - restoring, 243
 - troubleshooting, 31, 367
- Radia Management Portal Zone Directory, 239
- Radia Proxy Server
 - assigning devices, 313
 - installing, 316
 - Purge Dynamic Cache task, 77, 323
 - Purge Proxy Server Dynamic Cache task, 271
 - synchronizing, 321
- Radia services, remote stop and start, 325
- Radia subscriber information, discovering, 315
- radish.exe
 - build number, 367
 - version information, 366
- RCS - Primary Container, 90
- RCS Administration task group, 80
 - prerequisites, 94
- README file, 30
- Refresh Managed Services Cache task, 79, 103, 115
- Refresh Management Agent task, 303
- refreshing
 - managed services cache, 115
 - Radia Management Agent, 303

- remote administration capabilities, 347
- remote control, 343
 - configuring parameters, 351
 - configuring server behavior, 351
 - connecting service to users, 344
 - disconnect task, 350
 - distribute service to device, 347
 - prerequisites, 344
 - procedures, 347
 - Start Viewer task, 348
 - system requirements, 344
- remote control service, connecting to users, 345
- remote installations, requirements, 295
- remote installs, 308
- remote zone operations, 341
- Remove Component from Instance task, 81, 100
 - description, 94
- Remove Connections task. See Remove Component from Instance task
- Remove Connections window, 100
- Remove job task, 263
- Remove Policy Object task, 79, 103, 105
- Remove Shortcuts from Desktop task, 64, 75
- Remove task, 75, 149, 191, 199
- removing
 - connections, 100
 - delegated administration roles, 228
 - groups, 238
 - Job Groups, 263
 - jobs, 263
 - objects, 199
 - policy objects, 105
 - task group, 218
 - task templates, 329
 - users, 235
- removing devices, 189
- Resolve Policy task, 79, 103, 109
- resolving policy entitlements, 110
- Restart Failed Jobs task, 75, 259
- Restart task, 77, 325
- restarting failed jobs, 260
- Restore task, 71, 243
- restoring Radia Management Portal Directory, 243
- Resume task, 77, 325
- RIB, connecting to, 146
- RIS. See Radia Integration Server
- RIS Install Directory field, 331

- RIS Port field, 331
- RIS Service Name Suffix field, 332
- RMA. See Radia Management Agent
- RMA registration throttling, 296
- rma.log, 302
- rmp.cfg, 128, 154, 157
 - LDAP authentication parameters, 153
 - PREFIX parameter, 156
- rmp.tkd, 253
- role, definition, 219
- RPS.CFG file
 - preconfigured, 320

S

- Schedule Zone Operation task, 26, 77, 78, 271, 328, 336
- Scheduler Information area, 340
- scheduling
 - jobs, 281, 282
 - zone operations, 336
- search patterns, 246, 279
- Select Client Port, 300, 306
- Select Client Port field, 332
- RPS.CFG File, 318
- selecting an audience, 279
- Sequence Job task, 77, 271, 343
- Server Management client, installing, 303
- servers
 - description, 87
 - modifying, 198
 - removing, 199
- services
 - adding, 195, 196
 - description, 88
 - managing, 325
 - modifying, 198
 - removing, 199
- Set Password dialog box, 347
- Set Password task, 78
- shortcuts
 - adding, 62
 - removing, 64
- Software Manager client, installing, 303
- Start a service task, 325
- start delay, 130
- Start Directory Service task, 72, 150

- job throttling, 258
- Start task, 78
- Start Viewer task, 78, 348
 - customizing, 350
- Start VNC server task, 348
- starting Radia Management Portal, 45
- Stop a service task, 325
- Stop Directory Service task, 72
- Stop Directory Service task, 152
- Stop job task, 261
- Stop task, 75, 78
- stopping
 - Job Groups, 261
 - Radia Management Portal, 46
- Submit Help Desk Notify window, 287
- Submit Job Sequence, 343
- Subnet groups, 91
- subordinate zone
 - definition, 22, 26, 329
 - opening, 341
- Subordinate Zones object, 126
- support, 7
- suspend a remote service, 325
- Synchronize Proxy Server task, 321
 - description, 78, 270
 - periodic scheduling, 322
- system requirements, 31
 - remote control, 344
- system-wide access, 219

T

- task group
 - adding, 213
 - description, 70, 213
 - maximize, 70
 - minimize, 70
 - modifying, 217
 - removing, 218
- task template
 - adding, 326
 - removing, 329
- Task Templates object, 127
- tasks
 - definition, 70, 213, 219, 270
 - Disable Jobs, 262
 - Enable Jobs, 262
 - lifecycle for operations, 275

- modifying, 198
 - performing, 54
 - query, 245
 - query jobs, 258
 - Remove jobs, 263
 - removing, 199
 - removing groups of devices, 191
 - Stop active job, 261
 - Synchronize Proxy Server, 321
 - updating, 43, 253
- tasks Radia Management Agent, 297
- technical support, 7
 - collecting information, 364
- test global policy, 219
- text file, 249
- throttling, 282
- TightVNC clients, remote control, 343
- Time Window area, 340
- toolbar
 - description, 82
 - new icons, 56
- trace levels, setting, 360
- Tracing enabled for jobs, 257

U

- Update Management Portal task, 271
 - description, 78
- Update Portal Tasks, 253
 - description, 71
 - procedure, 43
- Use for Policy field, 148
- USE_FQDNHOST_NAME, 134
- User field, 332
- user groups, adding, 235
- user interface, 55
- user names, acceptable, 47
- User Password field, 332
- users
 - adding, 230
 - assigning to groups, 236
 - configuring, 230
 - modifying, 233
 - removing, 235

V

- View Job History, 263
- View Properties task, description, 75, 82

- viewing
 - job history, 264
 - Managed Services groups, 315
 - properties, 264
 - subscriber information, 315
- VNC server, 347
- VNC session, disconnecting, 350

W

- Wake-on-LAN
 - multicast support, 134
 - support, 284
- WinVNC3, 352
- WOL_MCAST_ADDR, 134
- workspace, description, 86

Z

- Zone Access Points container, 92, 341

- definition, 26
- Zone Configuration Tasks container, 253
- Zone Containers, 88
 - navigating, 65
- zone directory structure, 22
- Zone Display Name field, 331
- Zone Information window
 - zone friendly name, 39
 - zone name, 38
- Zone Job Name group fields, 338
- Zone Name field, 331
- Zone Operations, scheduling, 336
- zone, definition, 22, 26
- zone.mk file, 20, 31, 239, 240, 367
- zone.mk, locating, 364
- ZoneJob, definition, 27

