HP Client Automation Enterprise

Portal

for the Windows® operating system

Software Version: 7.20

Installation and Configuration Guide

Manufacturing Part Number: none

Document Release Date: June 2009

Software Release Date: July 2008

Legal Notices

Warranty

The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

The information contained herein is subject to change without notice.

Restricted Rights Legend

Confidential computer software. Valid license from HP required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Copyright Notices

Trademark Notices

DHTML Calendar

Documentation Updates

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

- Software Version number, which indicates the software version.
  - The number before the period identifies the major release number.
  - The first number after the period identifies the minor release number.
  - The second number after the period represents the minor-minor release number.
- Document Release Date, which changes each time the document is updated.
- Software Release Date, which indicates the release date of this version of the software.

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

http://h20230.www2.hp.com/selfsolve/manuals

This site requires that you register for an HP Passport and sign-in. To register for an HP Passport ID, go to:

http://h20229.www2.hp.com/passport-registration.html

Or click the **New users - please register** link on the HP Passport login page.

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 Document Changes

Chapter	Version	Change
All	7.20	HP Configuration Management was renamed to HP Client Automation for this release. Note that not all components and products were re-branded. See Table 2 on page 6 for Task Name Changes as of Version 7.20.
Chapter 1	7.20	Page 19, Using this Guide with Core and Satellite Servers, new topic.
Chapter 1	5.10	Page 29, System Requirements have changed for this release. Page 30, Directory Size of a Single Zone, the maximum recommended size of a single Zone has increased to 50,000 devices.
Chapter 3	7.20	Page 73, About the Zone Containers, the *Cross-References Container* (cn=xref) has been renamed the *Device Categories* Container (cn=xref) as of Version 7.20.

Chapter	Version	Change
Chapter 4	5.10	Page 108, Setting Additional Configuration Parameters, added the following rows to Table 4: RCS_AUTO_CONNECT – used to automatically connect to the Primary ds-rcs whenever the startup property is Auto or Manual; REFRESHMSC – used to adjust how often the Managed Services Catalog is refreshed with the available managed-services in the Primary Configuration Server database.
Chapter 4	5.10	Pages 116 and 121 , Table 6 and Table 7 have revised defnitions for the Startup properties value of Manual.
Chapter 4	7.20 Aug 2008	Page 118, Table 6, added a note to the row explaining how to enter the URL when specifying an LDAPS directory service connection: ➤ Do not enter an IP address to specify the URL for ldaps; SSL does not verify IP addresses.
Chapter 4	5.10	Page 126, Directory Service Connection Status upon Portal Restart, added topic and Tables 11, 12, and 13 to summarize the conditions under which a Directory Service is reconnected to the Portal upon restart.
Chapter 4	All Jun 2009	Page 130, Modify LDAP Directory Service Options (for Web Services External Authentication and Filtering). Revised topic to clarify the LDAP Directory Service Options "Used for Authentication" and "Use Service Account" do not apply to users logging into the Portal directly; they only apply to users logging into the Enterprise Manager or Reporting Server which use the Portal Web Services to access the LDAP directory service.
Chapter 4	7.20 Aug 2008	Page 168, To import devices from a text file or list, added a requirement to use only ASCII characters when specifying the device names using a text file or list.
Chapter 5	5.10	Page 257, Upgrading the Portal Agent. To upgrade existing Portal Agents with a new build of `rma.tkd`, use the **Install Portal Agent** task or enable the Portal Agent Self-maintenance feature. Portal Agent Self-maintenance is documented in the *Portal Migration Guide*.

Chapter	Version	Change
Chapter 5	5.10	Page 254, To install the Portal Agent: When using the Domain Admin account to install the Portal Agent onto a device running Vista, ensure that File and Print Sharing is enabled on the Vista device.
Chapter 5	7.20	Page 251, Prerequisites for Installing Portal Agents onto Linux Devices, as of Version 7.20, HPCA no longer supports installing the Portal Agent or Client Automation Agent onto UNIX devices running **`AIX`**, **`HP-UX`** or **`Solaris`**.
Chapter 5	7.20	Page 258, Enabling Self-maintenance for Portal Agents, added: • Self-maintenance support for Portal Agents on Linux devices • Optional use of `criticalKitBuildNum` to upgrade the nvdkit build on the Agent.
Chapter 5	7.20 Aug 2008	Page 284, Table 24, added note to the row defining the Zone Display Name: **Note:** Use only ASCII characters in this field.
Chapter 6	5.10	Page 316, Portal Directory Troubleshooting, added topic for troubleshooting the Slapd service, adjusting the OVCMLDAP_HEARTBEAT_INTERVAL, and starting and stopping logging for the Slapd and related services.
Chapter 6	5.10	Page 318, Managing Portal Agent Signal Processing, new topic defines the rmp.cfg parameters that specify the the number of dedicated threads available to handle incoming RMA requests, RMA processing requests, and RMA registration requests.

Table 2 Task Name Changes as of Version 7.20

Task Group	Old Task Name	New Task (or Group) Name
Operations		
	Install CM Agent	Install Client Automation Agent
	Update CM Portal Tasks	Update Portal Tasks
CM-CS Administration		HPCA-CS Administration

Support

You can visit the HP Software support web site at:

www.hp.com/go/hpsoftwaresupport

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

HP Software 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 valued support customer, you can benefit by using the support site to:

Search for knowledge documents of interest

Submit and track support cases and enhancement requests

Download software patches

Manage support contracts

Look up HP support contacts

Review information about available services

Enter into 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 sign in. Many also require an active support contract. To find more information about support access levels, go to the following URL:

http://h20230.www2.hp.com/new_access_levels.jsp

To register for an HP Passport ID, go to the following URL:

http://h20229.www2.hp.com/passport-registration.html

Contents

1 Introduction

At the end of this chapter, you will:

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

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

Introduction

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

The Portal provides the following benefits:

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

Using this Guide with Core and Satellite Servers

⚠ If your environment uses Core and Satellite servers, first read the *Core and Satellite Servers Getting Started Guide* as the installation, configuration, and troubleshooting information in that guide may override the information in this guide.

About the Portal Capabilities

After installing the Portal, you can perform administrative and operational tasks on any piece of your Client Automation infrastructure. The capabilities of the Portal include:

- **Network Discovery**
  The Portal automatically discovers the objects in your networks.
- **Authentication**
  Use the Portal Directory to authenticate administrators.
- **Delegated Administration**
  Create roles in the Portal so that your administrators have access only to the tasks that are relevant to them and their roles.
- **Remote Installations of Client Automation infrastructure Components and Subordinate Portal Zones**
  Use the Portal to install Client Automation infrastructure products to remote devices running Windows. This includes the remote installation of additional 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 Portal.
- **Remote Infrastructure Administration**
  Use the Portal to manage Client Automation 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 Portal to access the Configuration Server DB on any Configuration Server in your enterprise, perform instance-level tasks, and assign and manage policy through Active Directory.

- **Device Categories**
  The Portal captures detailed information about device hardware, operating system, Client Automation infrastructure and managed services and stores it in the Portal Directory in self-managed device categories. This simplifies notification of all devices for a given classification in a single step.
- **Notify**
  Use Notify 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 query to extract information from the Portal directory.
- **Scheduling**
  Use scheduling to execute and track the progress of any task.
- **Auditing/Logging**
  Use auditing and logging to view information about administrators and the activities they performed within the Portal. All audit events will be stored in the log generated by the Portal.

About the Product Architecture

Although you will work with the Portal in your web browser, you may want to be familiar with its base architecture.

The Portal contains the following:

- The **Portal Run-time** contains the HPCA Portal service (httpd-managementportal) and the `RMP.TKD` module (located in the `\modules` directory).
- The **Portal Zone Directory**, is an OpenLDAP directory service in the Portal's `\etc\openldap` directory. When the Portal starts, it loads the database objects that represent a given instance of the Portal, or Zone. The database objects include all information needed to manage a given set of infrastructure at a given location:
  - Managed devices
  - Device group memberships
  - Chassis container for blade enclosures and racks

- Device Categories
- Job Status and Job History
- Users
- Configurations for Entitlements, Tasks, and Services
- Networks

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

- The **Portal Agent**, installed on the remote devices, performs tasks on behalf of the Portal. See Installing the Portal Agent on page 252 for more information.

Portal Zones Overview

Very large enterprises often find it necessary to use multiple 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 Portal by defining a zone and a specific zone directory structure for each 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 Portal.

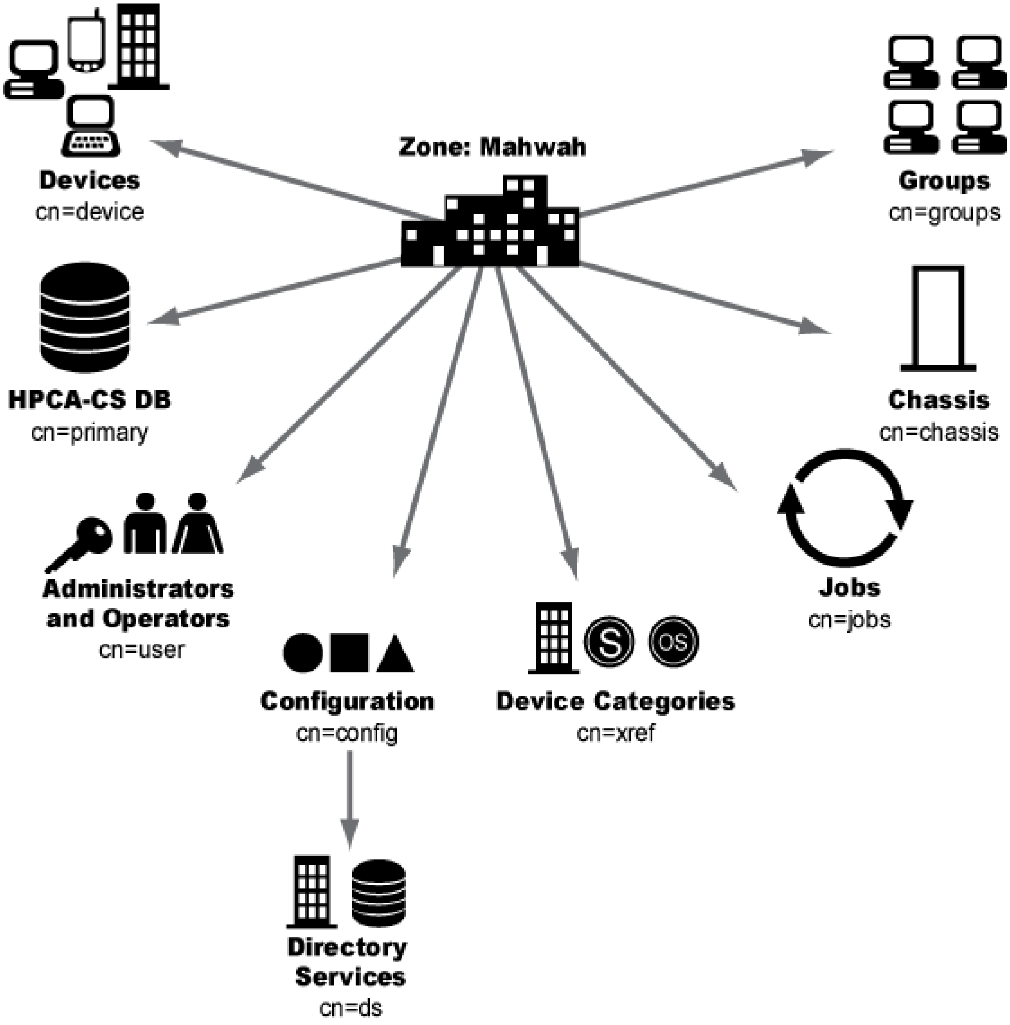
A zone is created whenever the Portal is installed, and all objects in the zone include the high-level qualifier of the zone name. The first installed zone is called the master zone and others are called subordinate zones. The properties for the zone object, itself, include the URL information needed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

The Zone Directory Structure

Every 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 73 for a description of each container and how they are used.

Figure 1 Portal directory of a zone

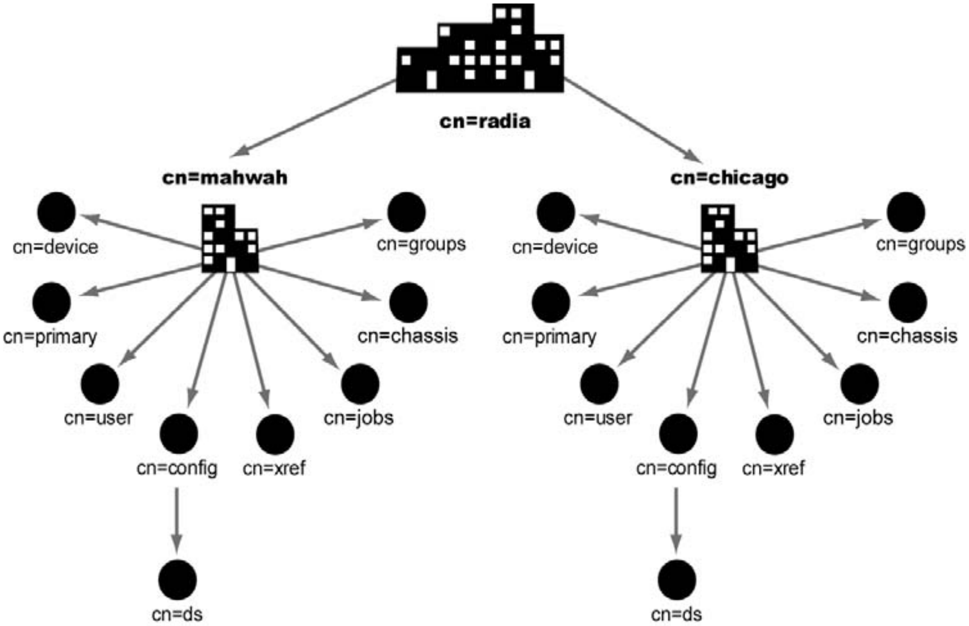


About Object Names in a Zone

The 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 Configuration Server is `cn=Primary,cn=Mahwah`.

Figure 2 Multiple zones of the 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 pop-up window as you hover your mouse pointer over the object's icon or label in the Portal.

The directory structure and naming context permit name distinction among all objects in all zones in your enterprise. This allows the HPCA administrators to schedule operations across devices in the entire enterprise from a single, central site.

New Terminology

The following terms are used frequently throughout this guide. You should become familiar with them before using this guide. Also 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 Portal. These include any Lightweight Directory Access Protocol (LDAP) directory, the Configuration Server, DSML (allowing access to another Portal zone), and metakit (`*.MK`) files.

A 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 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 Portal zone installed at an enterprise. Additional Portals are installed as subordinate zones to the 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 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 microprocessors, 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 Portal zones installed at an enterprise, usually from the initial 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 Portal.

A zone is created whenever the 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 container

The zones access points container defines all Portal zones in your enterprise. Go to the zone access points container to open another zone's Portal, as well as schedule zone operations on devices that exist in any zone in your enterprise. See ZoneJob below.

ZoneJob

A job group scheduled for devices in a named group across one or more 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 Portal is a web-based interface you use to manage your Client Automation infrastructure across your entire enterprise.
- You can perform administrative and operational tasks on objects in your infrastructure, administer instances in the Configuration Server DB, and assign policy using Active Directory.
- The Portal consists of the Portal Run-time, the Portal Zone Directory, and the Portal Agent. 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 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 Client Automation services.

2 Installing the Portal

At the end of this chapter, you will:

- Be able to install the Portal.
- Be able to log on to the Portal.
- Be able to change your password.

Preparing for Installation

⚠ If your environment uses Core and Satellite servers, first read the *Core and Satellite Servers Getting Started Guide* as the installation, configuration, and troubleshooting information in that guide may override the information in this guide.

1. Before you install the Portal, locate your HP license file.

   If you need assistance, contact HP Technical Support.

2. A complete Portal installation requires access to these folders of the HP Client Automation media:

   — **Infrastructure** media folder (used to install additional Portal Zones or Proxy Servers from the Portal)

   — **Agents** media folder (used to install Client Automation agents from the Portal)

3. Review the Release Notes delivered with the Client Automation product for the latest information.

Installing the Portal

Use the Portal to view and manage your existing Windows infrastructure, add new Client Automation infrastructure products and applications, as well as perform service and policy administration on your Configuration Server DB, using Active Directory, if needed.

This release supports environments with multiple Portal sites using the new zone architecture and features. Each Portal site being managed from the master portal site needs to have version 5.00 installed.

Prerequisites

The Portal has been optimized to work with the REXX method ZTASKEND and the Messaging Server.

HP recommends using the Portal with the latest ZTASKEND and the latest Messaging Server to improve the information process flow between the Configuration Server and the Portal.

- Using the latest version of ZTASKEND that is available with the latest Configuration Server enhances Portal performance.
- The minimum ZTASKEND required is Version 1.8. This is installed with the Configuration Server 4.5.4 SP3.

For details on migrating your Configuration Server, refer to the PDF located in the following folder on the Client Automation media: `Configuration Server\management_infrastructure\configuration_server \migrate_db`.

For details on installing the Messaging Server, refer to the *HP Cllent Automation Messaging Server Installation and Configuration Guide (Messaging Server Guide)*. For details on upgrading to the latest version of the Messaging Server, refer to the latest Migration Guide for that product.

System Requirements

- **Server**
  - Windows Servers* with Service Packs listed below:

    Windows 2000 Server, SP 4
    Windows Server 2003, SP2 and R2 SP2

    *For the latest information on Server requirements, also refer to Infrastructure Platform Support Table in the accompanying *Release Notes* for this version.
  - Installation of the 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**

Platform Support

For the latest information about the platforms that are supported in this release, see the accompanying *HPCAE 7.20 Release Notes*.

Directory Size of a Single Zone

The **Portal Directory** includes all configuration and entitlement information for the Portal as well as devices, groups, managed infrastructure, job status, network and mounted services information.

For performance reasons, HP recommends limiting the number of devices managed by a single zone to the following:

- Recommended maximum: 50,000 devices

Multiple Portal zones can be installed to meet the needs of enterprises of any size. To create additional zones in your enterprise, see Installing Additional Portal Zones (Subordinate Zones) on page 282.

Installation Procedures

⚠ You will not be permitted to install this version of the Portal to the same directory as an existing, pre-Version 5.00 Portal. It must be installed to a different directory.

For more information, refer to the Portal Migration Guide, located in the `\extended_infrastructure\management_portal\migrate` folder on the Client Automation media.

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

To install additional Portal zones in your enterprise, use the Install Subordinate Portal task in the Operations task group. For details, see Installing Additional Portal Zones (Subordinate Zones) on page 282.

Default Installation Path, Ports, and Service Name

The Portal no longer installs into a shared path, port or service of an Integration Server. The Portal installation defaults for v 5.x are summarized below:

- The default Portal install location is:

  `C:\Program Files\Hewlett-Packard\CM\ManagementPortal`

- Default Ports include:
  - Portal: **3471**
  - Listening Port for OpenLDAP: **3474**
  - Listening Port for OpenLDAP Backup: **3475**
- The Portal Service name is **httpd-managementportal.**
- The display service name is: **PortalHPCA Portal.**

To install the Portal

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

1 From the \Infrastructure directory on the Client Automation Enterprise media, go to the folder for \extended_infrastructure\management _portal\win32 and double-click **setup.exe**.

The Welcome window for the Portal setup program opens.

2 Click **Next**.

The End-User License Agreement window opens. You must accept the terms before you can install the Portal.

3 Click **Accept** to agree to the terms of the software license.

The Portal Location window opens.

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

> HP recommends accepting the new default path of:
>
> C:\Program Files\Hewlett-Packard\CM \ManagementPortal
>
> The Portal no longer installs into a shared Integration Server path, service, and port.

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 Portal \modules directory.

The Enable Network Discovery window opens.

7 Click **Yes** to enable Network Discovery (*recommended*). This option enables the 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 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 104.

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 minutes) after the Portal starts before starting the network discovery. The delay applies each time the Portal is started. Valid entries are 0 to 1440 miniutes (or 24 hours). By default, Network Discovery starts 15 minutes after you start the 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 104.

12 Click **Next**.

The first zone information window opens.

13 In the Portal Zone Name text box, type a zone name to represent this instance of the Portal. Each instance of the 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 21 for more information about Zones.

14 Click **Next**.

The second Zone information window opens.

15 In the Portal Zone Friendly Name text box, optionally type a friendly name for this 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 Portal user interface.

16 Click **Next**.

The Secure Listening Port window opens.

In the Secure Listening Port for Portal text box:

— Leave the default value of -1 to run the Portal on an unsecured port (the default is 3471).

— To specify an SSL-secured listening port for the Portal, enter the secured port number here.

Following installation, refer to the *HP Client Automation SSL Implementation Guide* for complete information on how to configure the Portal for secured communications.

17 Click **Next**.

In the Listening Port for OpenLDAP text box, select a port for the Portal Zone to communicate with its OpenLDAP Database. The default port is 3474.

18 Click **Next**.

In the Listening Port for OpenLDAP Backup text box, select a port for the Portal Zone to communicate with a Backup OpenLDAP Database. The default port is 3475.

19 Click **Next**.

The Enable Backup window opens.

20 Click **Yes** to enable the Backup Directory task (*recommended*). This option enables the Portal Backup Directory task and the resources it needs to create a Backup of the OpenLDAP Database. The Backup Directory task uses the Listening Port for OpenLDAP Backup.

or

Click **No** to disable the Portal Backup Directory task. This option is not recommended unless alternate database replication or backup processes are being used in your environment.

21 Click Next.

A summary window of the installation information opens.

22 Click **Install** to begin the installation.

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

23 Click **Yes**.

The Remotely Installable Components Location window opens.

If necessary, click **Browse** to navigate to the location of the **Infrastructure** folder on the Client Automation media.

24 Click **Next**. The modules are copied to the Portal `\media` directory.

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

25 Click **Yes**.

The Remotely Installable Client Components Location window opens.

If necessary, navigate to the **\Agents** directory.

26 Click **Browse** to navigate to the location of the **\Agents** directory, which contains the media for all agents.

27 Click **Next**.

The HPCA Agent modules are copied to the Portal's `\media` directory.

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

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

See Starting and Stopping the Portal on page 37 and Accessing the Portal on page 38 for information on performing these tasks manually.

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

Updating Portal Tasks

The Update Portal Task is not required the first time you install Portal.

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

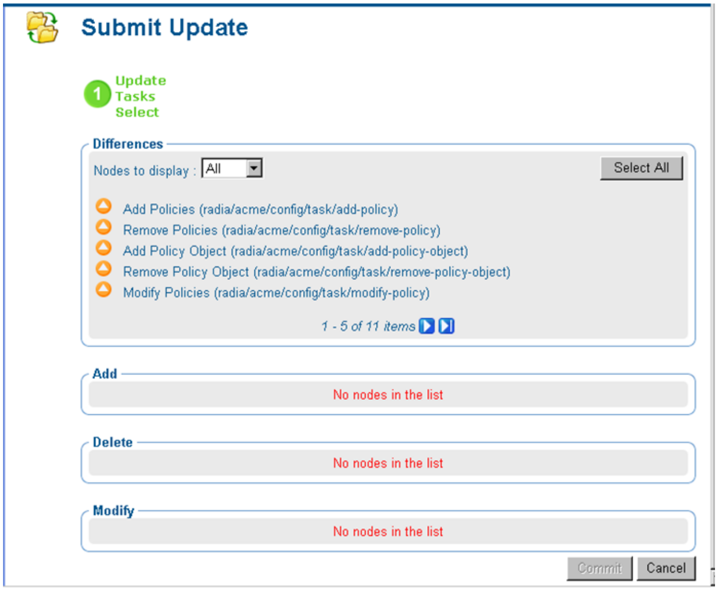
1 If necessary, restart the Portal, (the Windows service name is **HPCA Portal**).

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

3 Use the navigation aid to select **Directory** → **Zone** → **Configuration** → **Tasks**.

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

5 The Submit Updates dialog box opens.



Nodes to display : All

Add Policies (radia/acme/config/task/add-policy)
Remove Policies (radia/acme/config/task/remove-policy)
Add Policy Object (radia/acme/config/task/add-policy-object)
Remove Policy Object (radia/acme/config/task/remove-policy-object)
Modify Policies (radia/acme/config/task/modify-policy)

1 - 5 of 11 items

No nodes in the list

No nodes in the list

No nodes in the list

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

- To select all task changes, click **Select All**.
- To select individual task changes, double-click the item.

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.

Items selected from the Differences list are moved to the appropriate Add, Delete, or Modify list.

7 Click **Commit**.

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

To log off the Portal

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

Updating Subordinate Portal Zones with a New Build

Refer to the release notes that accompany a new build of the Portal for details on how to apply the updates. Generally, the same procedure used to install the initial 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 Portal includes an **Update Subordinate Portal** task. For details, see Updating Subordinate Portal Zones on page 286.

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

Specifying the IP Address for a Remote Portal

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

Posting Agent Objects to the Portal

All agent 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 Portal zone or discard them.

For details on how to configure the Messaging Server to post agent objects to a Portal Zone, refer to the *Messaging Server Guide.*

➤ Notifying agents using Wake-On-Lan (WOL) from the Portal no longer requires you to route agent objects to the Portal. The Portal Agent now collects the MAC address and subnet information needed for WOL directly from any device which has a Client Automation agent installed.

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

Starting and Stopping the Portal

To start the Portal

1. Access Windows Services if it is necessary to start the Portal.
   For example, to access Windows Services for a Windows 2000 machine, right-click the **My Computer** icon on the server desktop and click **Manage.** Expand the **Services and Applications** branch and click **Services**.
2. From Windows Services, right-click **HPCA Portal** and select **Start**.

To stop the Portal

1. Access Windows Services to stop the Portal. For example, to access Windows Services from Windows 2000 Server, right-click the **My Computer** icon on the server desktop and click **Manage**. Expand the **Services and Applications** branch and click **Services**.
2. Right-click **HPCA Portal** and select **Stop**.

Accessing the Portal

⚠ If your environment uses Core and Satellite servers, use the information in the *Core and Satellite Servers Getting Started Guide* to access the Portal.

To access the Portal

1 Open your web browser.

➤ See the Web-Client topic of System Requirements on page 29 to review the Web browser requirements for the Portal.

2 In the Address bar, type the following:

`http://<`*`IP Address or host name`***`>:3471`**

— *`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 Portal prompts you to login.

Logging On

To log on to the Portal

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

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

The password is **`secret`**.

⚠ Be sure to change your password before moving the Portal into your production environment. See Changing Passwords on page 39 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 Zone Directory appears in the workspace. See Performing Any Task in the Portal on page 44 for more information.

To log off the 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 Portal user interface, see page 45.

- For information about performing tasks, see Performing Any Task in the Portal on page 44.

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**.

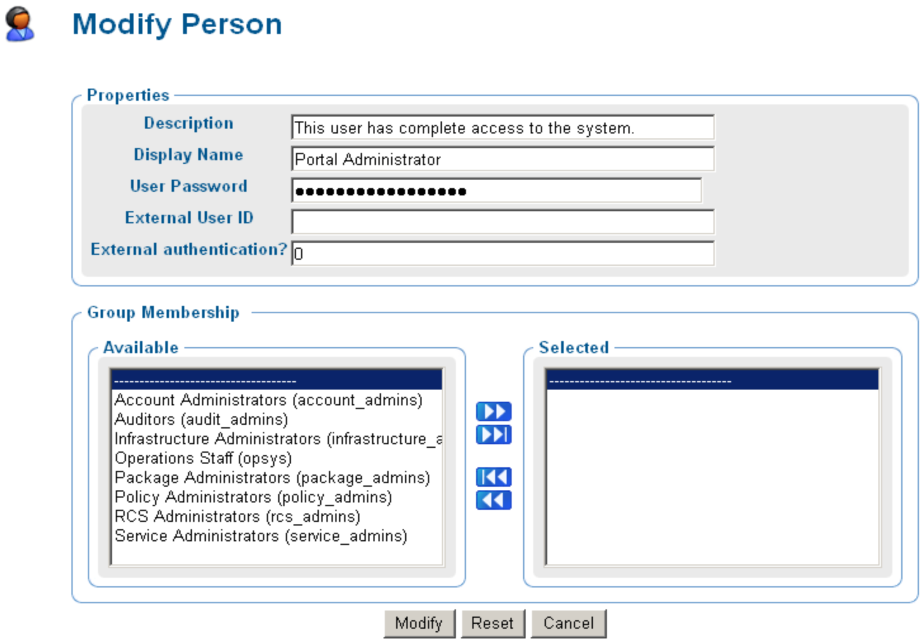
3 In the workspace, select the person whose password you want to change, such as the Portal Administrator.

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?: 0

Group Membership

Available:

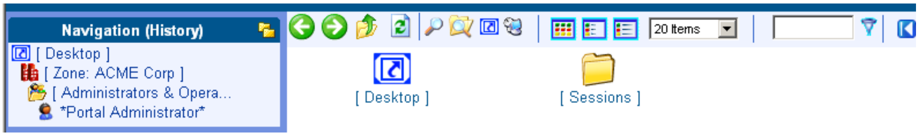
Account Administrators (account_admins)
Auditors (audit_admins)
Infrastructure Administrators (infrastructure_a
Operations Staff (opsys)
Package Administrators (package_admins)
Policy Administrators (policy_admins)
RCS Administrators (rcs_admins)
Service Administrators (service_admins)

Selected:
----

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 box 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 Portal, giving it a zone name. This installation becomes your enterprise's Master Zone.
- To install additional Portal zones, use the Install Subordinate 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 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 Portal to update the tasks available to you.
- Run **Update Subordinate Portal** to update subordinate zones in your enterprise with a new build, such as a Portal Service Pack.
- Optionally, the Messaging Server can be configured to route agent-objects from the Configuration Server to the Portal.

3 Using the Portal

At the end of this chapter, you will:

- Be familiar with the Portal user interface, 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 of the 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 Portal Zone.
- Know how to navigate to locations that has been configured for access from the Portal, including networks, the Configuration Server DB on a Configuration Server and an Active Directory or other LDAP directory in your enterprise.
- Be able to use the HPCA-CS Administration tasks to manipulate *instances* in the Configuration Server DB.
- Be able to use the Policy and Policy (Advanced) tasks to assign and manage policy through an external LDAP directory, including Active Directory.

Performing Any Task in the Portal

One of the benefits to using the 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.

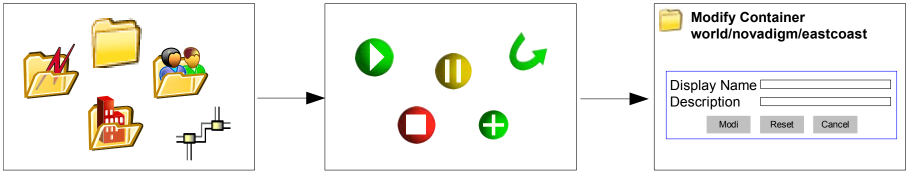
To perform any task in the Portal

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 this guide refer you to the appropriate starting locations. See the Taskbar and Task Summary on page 56 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 233 for detailed information on completing tasks.



Select Authority   Select a task   Enter necessary information

For detailed information about the user interface, see About the Portal Interface on page 45.

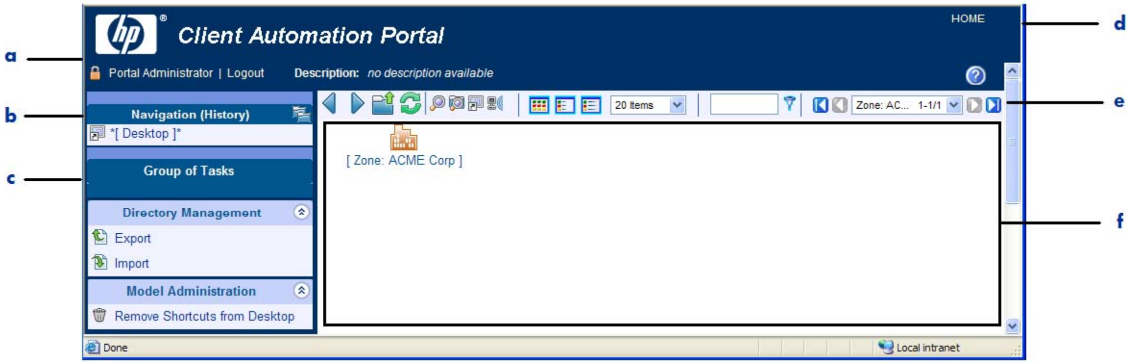
For detailed information about specific tasks, see the Administrative Functions and Operations Functions chapters.

For detailed information about using the Configuration Server and Policy tasks, see the topics beginning with Using the HPCA-CS Administration Tasks on page 79.

About the Portal Interface

The Portal user interface contains several distinct areas.

Figure 3 Portal user interface



Legend

a Banner

b Navigation Aid

c Taskbar

d HOME Link

e Toolbar

f workspace

- **Banner area.** See Banner on page 46.
- **Navigation aid (History or Location mode)**. The Navigation aid has two modes: History (the default) and Location. Use the icon on the right-side of the Navigation title bar to switch from one mode to the other. For details, see Navigation Modes: History and Location on page 47.
- **New Desktop location**. When you log on to the Portal, you start at the level of your desktop, in Navigation (History) mode. This starting location gives you quick access to the Portal directory and the containers and objects in the current 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 50 for more information.

- **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.
- **Groups of Tasks**. See Taskbar and Task Summary on page 56 for a complete list of task groups and a summary of all tasks available from the Portal.
- **Toolbar icon buttons.** See Toolbar on page 67 for more information.
- **Container objects** in your HPCA zone. See Portal OpenLDAP Directory and Zone on page 71.

Banner

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

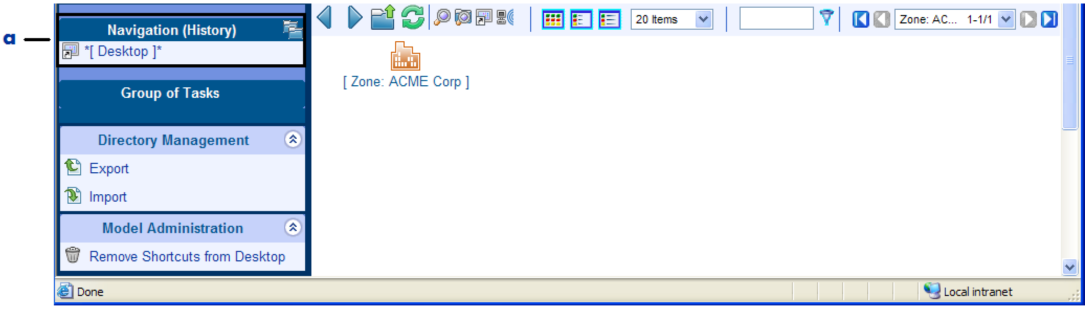
- Click **Logout** to log off the Portal.
- Click **HOME** to return to the Portal home page. This is the directory location in Navigation (Location) mode.
- Rest the mouse pointer on the ? button to display the Portal version number.
- After logging in, click the ? button to view detailed version and build level information for the Portal component modules. Whenever this Version information window is displayed, the version and build information is also written to the Portal log file: `httpd-managementportal-`*`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 313.

Using the Navigation Aid

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

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

Figure 4 Initial Desktop location in Navigation (History) mode



Legend

a History mode

This starting desktop location gives you quick access to the Portal directory and the containers and objects in the current 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 51 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 Portal. To toggle to the Navigation (Location) mode, click .

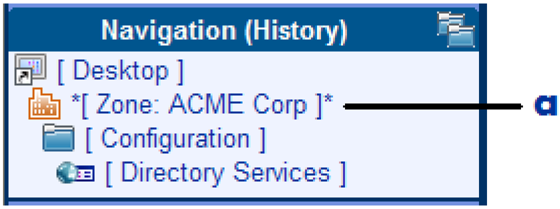
The Navigation (History) aid provides a record of your navigation path. To quickly return to a previously visited location, just click any entry in the Navigation (History) record.

- *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 Directory Services within the Zone Configuration 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 5 Navigation (History) records visited locations



[Desktop]
[Zone: ACME Corp]
[Configuration]
[Directory Services]

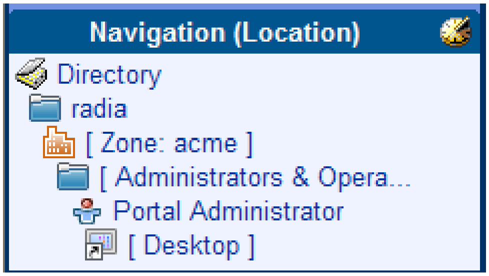
Legend

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 shown as an example only. Your screen may not look like this.

Figure 6 Desktop location in Navigation (Location) mode



Directory
radia
[Zone: acme]
[Administrators & Opera...
Portal Administrator
[Desktop]

Sample Navigation Session: Viewing Network Objects

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

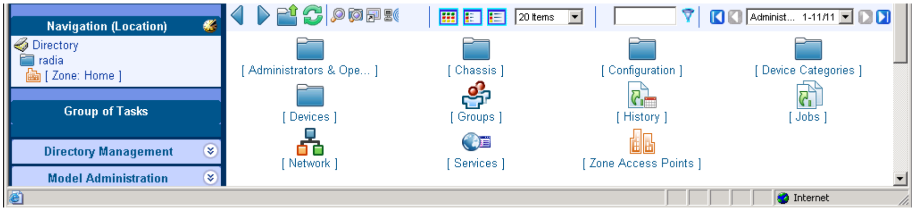
To access the Portal Directory and the Microsoft Windows Network

1 When you first log on, your Desktop displays in the Navigation aid. If you are not at this location, click **HOME** in the banner area and then click the **Desktop** entry in the Navigation area.

The Portal Directory object appears in the workspace.

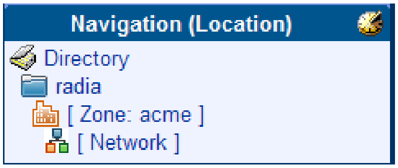
2 In the workspace, click the **Zone** object.

The highest-level objects in the zone appear in the workspace. See About the Zone Containers on page 73 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.



If Network Discovery has been enabled during the installation, there will be entries for various networks, such as the Microsoft Windows Network of discovered objects, 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 111.

If Network Discovery has not been enabled, the Network World Properties page is displayed. You can read through the steps that follow to learn how to filter the objects displayed within the workspace of the Portal interface.

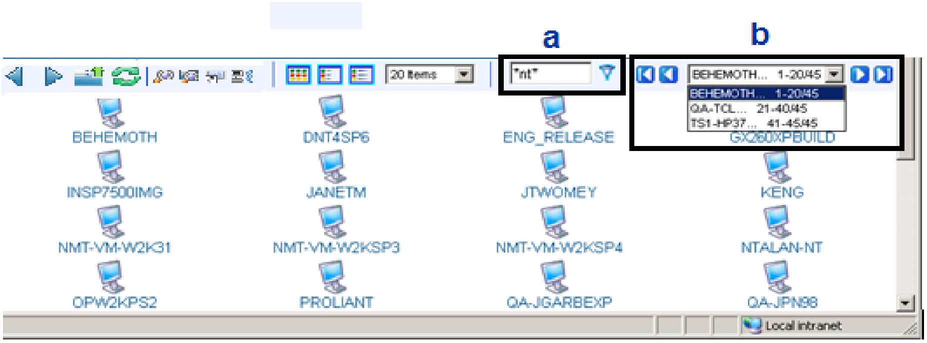
4 In the workspace, click **Microsoft Windows Network.**

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 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

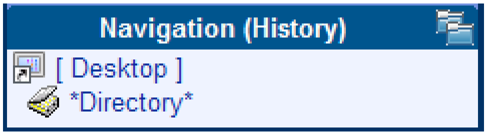
6 To return to the Desktop, click **[Desktop]** in the Navigation aid.

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.



Navigation (History)

[Desktop]

Directory

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

Adding Shortcuts to Your Desktop

This version of the Portal contains 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.

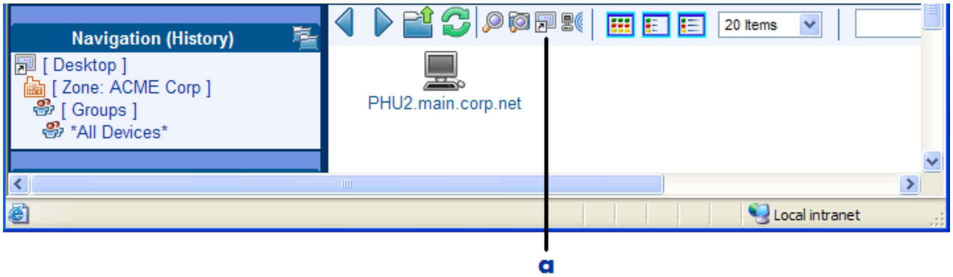
2 Navigate to the device or location for which you want to create a shortcut on the desktop. For example, to create a shortcut to the *All Devices* Groups in a Zone, navigate to it by clicking the following entries in the workspace area:

— Zone

— Groups

— All Devices

3 After navigating to the location for which you want to create a shortcut, click the **Add Desktop Shortcut** icon on the toolbar.



Navigation (History)

[Desktop]

[Zone: ACME Corp]

[Groups]

All Devices

Legend

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

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

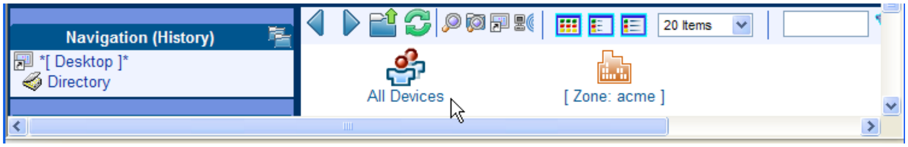
4 Click ✓ to confirm that you want to add the shortcut.

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 50.
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.
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.
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

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. Understand that every task you select in the Portal is performed within a selected level of authority.

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

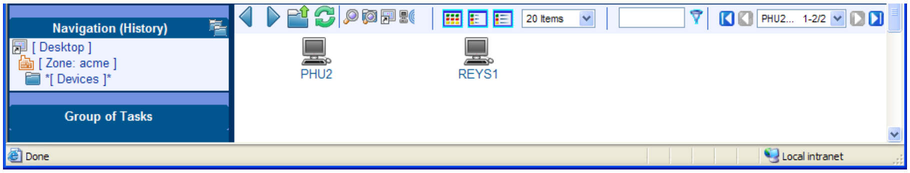
3 In the workspace, click the zone icon.

The workspace displays the highest-level objects in the zone directory.

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 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, 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 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 140.

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

See About the Zone Containers on page 73 for detailed information on the Devices container and the other Zone containers.

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

— Click this toolbar icon to go up one level in the navigation path.

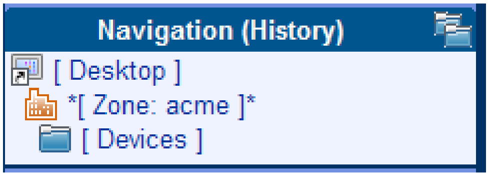
or

— 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).



Navigation (History)

[Desktop]
[Zone: acme]
[Devices]

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 Portal, only the Default Group object appears. If the Portal is not newly installed, you will also see any user-created groups in this container.

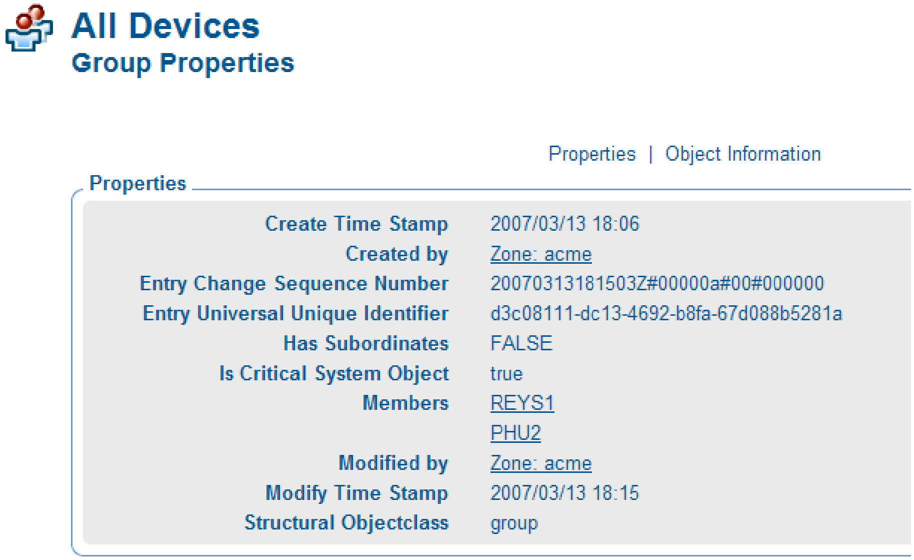
The Groups container is one of the most important containers in the Portal for performing operations. Almost all tasks are performed on Groups of Devices.

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 155 for more information on how to create groups and add or import devices into the groups.

7 Click the **All Devices** object in the workspace, and then click the View Properties icon on the toolbar .

The Group Properties page for the Default Group object opens.



All Devices

Group Properties

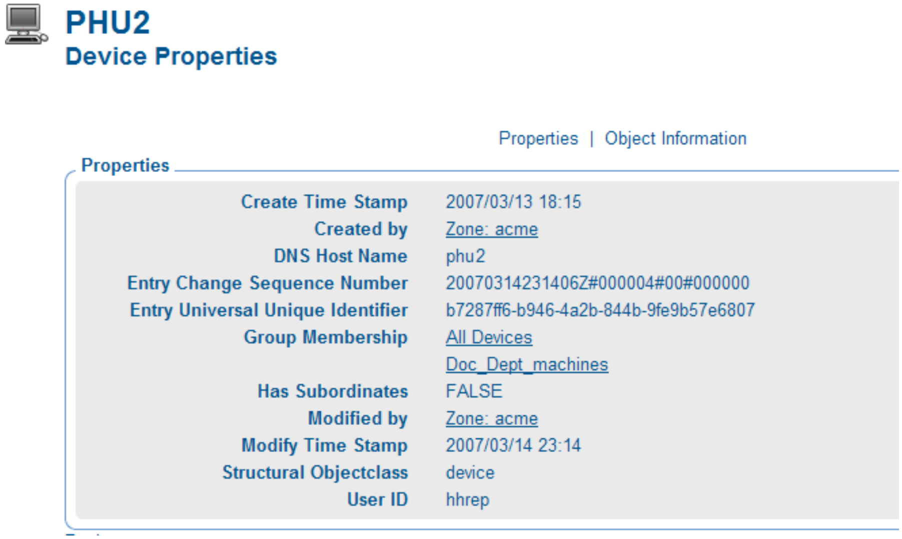
Properties | Object Information

Properties

Create Time Stamp	2007/03/13 18:06
Created by	Zone: acme
Entry Change Sequence Number	20070313181503Z#00000a#00#000000
Entry Universal Unique Identifier	d3c08111-dc13-4692-b8fa-67d088b5281a
Has Subordinates	FALSE
Is Critical System Object	true
Members	REYS1 PHU2
Modified by	Zone: acme
Modify Time Stamp	2007/03/13 18:15
Structural Objectclass	group

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.



PHU2
Device Properties

Properties | Object Information

Properties

Create Time Stamp	2007/03/13 18:15
Created by	Zone: acme
DNS Host Name	phu2
Entry Change Sequence Number	20070314231406Z#000004#00#000000
Entry Universal Unique Identifier	b7287ff6-b946-4a2b-844b-9fe9b57e6807
Group Membership	All Devices Doc_Dept_machines
Has Subordinates	FALSE
Modified by	Zone: acme
Modify Time Stamp	2007/03/14 23:14
Structural Objectclass	device
User ID	hhrep

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:

- HPCA-CS Administration
- Directory Management
- Infrastructure
- Model Administration
- Operations
- Policy Management
- Policy (Advanced)

See Toolbar Tasks on page 67 for information about the tasks that can be initiated directly from icons in the toolbar.

See Configuring Task Groups on page 186 for information about adding, modifying, or removing task groups.

Click ⇊ to maximize or ⇈ to minimize a group of tasks.

HPCA-CS Administration Task Group

Use the HPCA-CS Administration task group to manage instances in the Configuration Server DB. Remember, the tasks listed will vary based on what you have selected in the navigation aid.

The following is a list of the HPCA-CS Administration tasks.

	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 81 for more information.
	Copy Instance ◉ Click **Copy Instance** to create a copy of the selected instance. See Copying Instances on page 82 for more information.
	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 80 for more information.

	Delete Instance Click **Delete Instance** to remove the selected instance from the Configuration Server DB. See Deleting Instances on page 82 for more information.
	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 Admin CSDB Editor. See Modifying Instances on page 83 for more information.
	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 84 for more information.

Directory Management Task Group

Use the Directory Management task group to manage the Portal directory. The available tasks vary according to your navigation location.

	Backup Directory Click **Backup Directory** to back up the OpenLDAP database for the Portal Zone Directory. See Creating a Backup of the Portal Zone Directory on page 205 for more information.
	Export Click **Export** to export a subset of your Portal zone directory to an LDIF (LDAP Data Interchange Format) file. See Exporting Data from the Portal Directory on page 210 for more information.
	Import Click **Import** to import an LDIF file into your Portal zone directory. See Importing Data into the Portal Directory on page 211 for more information.

	Restore The Restore task is a placeholder for the manual procedure needed to use an OpenLDAP database replica, produced from the Backup task, to restore a Portal Zone Directory. Refer to Restoring the Portal Directory on page 207 for more information.
	Update Portal Tasks Click **Update Portal Tasks** when you receive a new build of the Portal to update the tasks available to you. See Updating Portal Tasks on page 214 for more information.

Infrastructure Task Group

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

	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 132 for more information.
	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 Stopping a Directory Service on page 134.for more information.

Model Administration Task Group

Use the Model Administration task group to manage the Portal directory and a zone. The available tasks vary according to your navigation location.

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

	Add object-type ⊕ Click an **Add** task to create an object in your selected authority, such as a device, group of devices, server, person, user group, delegated administration, task group, or directory service. As of version 2.1, you can also add objects types for racks, blade enclosures, enclosure configurations, and slots. See Configuring Blades, Enclosures, and Racks for more information.
	Add Device ⊕ Click **Add Device** to define a new device to the zone and also give it membership in the Default Group or other group within the Zone Groups container. This task automatically creates an entry for the device in the Zone Device container. See Adding Devices to a Portal Zone on page 140 for more information.
	Add Directory Service ⊕ Click the new **Add Directory Service** task to configure a connection between the Portal zone and another directory service, including the Configuration Server ZTOPTASK service. The task is available from the **Zone** → **Configuration** → **Directory Service** container. See Adding a Directory Service on page 111 for more information.
	Add Group (of Devices) ⊕ Click **Add Group** from the Devices container to create a new Group of Devices for organizing devices for operations. See Adding Groups on page 160 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.
	Add Install Profile ⊕ Click **Add Install Profile** to define a custom profile for selection during the Install Client Automation Agent task. The Add Install Profile task is available from the following navigation location: **Zone** → **Configuration** → **Profiles** → **Radia Products** → **Client Installs**. See Adding, Modifying, and Deleting Install Profiles on page 266 for more information.
	Disable ⏹ Click **Disable** to prevent a job or job group from being processed. See Disabling Jobs or Job Groups on page 220 for more information.

Enable

Click **Enable** to restart a job or job group the next time it is scheduled to run. See Enabling Jobs or Job Groups on page 221 for more information.

Import Device

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 168 for more information.

Modify

Click **Modify** to change an object. For example, you might want to change the areas of the Portal that an administrator can access, or change a job group's schedule. See Modifying Objects on page 172 or Modifying Job Groups on page 217 for more information.

Move Device

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 163 for more information.

Query

Click **Query** (also available from the toolbar) to extract information from the directory tree or to narrow the scope of a job. For example, you might want to search for a specific audience for whom you want to schedule a task. See Performing Queries on page 235 for more information.

Query Jobs

Click **Query Jobs** to locate existing jobs, review their status, and make changes to them. See Querying Jobs or Job Groups on page 218 for more information.

Query User's Delegated Administration

Click **Query User's Delegated Administration** to display information about a user's role. See Querying a User's Delegated Administration on page 197 for more information.

Remove

Click **Remove** to remove an object and all of its children from the Portal directory. See Removing Objects on page 172 or Removing Jobs or Job Groups on page 221 for more information.

Remove Shortcuts from Desktop
Click **Remove Shortcuts from Desktop** to remove any previously added shortcuts from your Desktop location. See Removing Shortcuts from Your Desktop on page 52 for more information.

Restart Failed Jobs
Click **Restart Failed Jobs** to restart the failed jobs displayed in the current Job Group. See Restarting Failed Jobs in a Job Group on page 219 for more information.

Stop
Click **Stop** to stop an active job group from running. See Stopping Job Groups on page 220.

View Properties
Click **View Properties** from the Model Administration task group or click 🔍 from the toolbar to display the properties of an object. See Viewing Properties on page 222 for more information.

Operations Task Group

Use the Operations task group to perform operations on your Client Automation infrastructure.

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

Add Task Template
Add Task Template is available from the Task Template container within the Zone, Configuration container. Use Add Task Template to preset the options for a Task Type, such as Notify or Install 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 279 for more information.

Assign Proxy Server
Use the Assign Proxy Server task to have a Proxy Server assist in the remote installation of Client Automation agents. Devices assigned to a Proxy Server will obtain their agent installation scripts from that Proxy Server instead of from the Portal. See Assigning Proxy Servers on page 269 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 244 for more information.
	Install Client Automation Agent Click **Install Client Automation Agent** to install the Client Automation agent on remote computers. See Installing the Client Automation Agent on page 262 for more information. Multiple agent install profiles are supported. For details, see Supporting Remote Installs Using Multiple Profiles on page 266.
	Install Portal Agent Click **Install Portal Agent** to install the Portal Agent on remote computers. For more information, see Prerequisites for Installing Portal Agents onto Linux Devices on page 252 and Installing the Portal Agent on page 252.
	Install Subordinate Portal Click **Install Subordinate Portal** to remotely install another Portal Zone in your infrastructure. See Installing Additional Portal Zones (Subordinate Zones) on page 282 for more information. Also refer to the tasks: Update Portal, Open Subordinate Zone, and Schedule Zone Operation.
	Install Proxy Server Click **Install Proxy Server** to install the Proxy Server on remote computers. See Installing the Proxy Server on page 272 for more information.
	Notify Use the Notify tasks to perform an action on the selected audience. See Using the Notify Tasks on page 240 for more information.
	Open Subordinate Zone Click **Open Subordinate Zone** to quickly access the Portal of another zone in your enterprise from the Zone Access Points container. See Opening a Subordinate Zone on page 292 for more information.
	Purge Proxy Server Dynamic Cache Click **Purge Proxy Server Dynamic Cache** to purge the dynamic cache of one or more Proxy Servers. See Purging the Dynamic Cache of the Proxy Server on page 277 for more information.

Restart

Click **Restart** to stop a service and then start it again. See Managing Services on page 278 for more information.

Resume

Click **Resume** to resume execution of a service that has been paused. See Managing Services on page 278 for more information.

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 287 for more information.

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 294 for more information.

Set Password

Click **Set Password** to set the VNC Authentication password prior to the first time you use remote control to access a VNC Server on a Client Automation agent. See Using Remote Control on page 297 for more information.

Start

Click **Start** to run a service. See Managing Services on page 278 for more information.

Start Viewer

Click **Start Viewer** to start a VNC session on a remote Client Automation agent. See Using Remote Control on page 297 for more information.

Stop

Click **Stop** to stop a service. See Managing Services on page 278 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 276 for more information.

	Update Subordinate Portal Click **Update Subordinate Portal** to remotely update the code delivered with a new build to the subordinate Portal Zones in your infrastructure. See Updating Subordinate Portal Zones on page 286 for more information.
	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 287 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.

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 an LDAP Directory. See on page for more information. See Adding a Policy Object on page 86 for more information.
	Modify Policies Click **Modify Policies** to assign services to the selected policy object. See on page for more information. See Modifying Policies on page 88 for more information.
	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 89 for more information.
	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 87 for more information.

	Refresh Services Catalog Click **Refresh Services Catalog** to refresh the list of services displayed in the Portal. This list is created from information in the Configuration Server DB. See Refreshing the Services Catalog on page 93 for more information.
	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 89 for more information.

Policy (Advanced) Task Group

Use the Policy (Advanced) task group to modify the 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 its attributes before using these tasks.

The tasks 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. See Modifying Policy Defaults on page 97 for more information.
	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. See Modifying Policy Dependencies on page 95 for more information.
	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. See Modifying Policy Flags on page 96 for more information.

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. See Modifying Policy Overrides on page 98 for more information.

Toolbar Tasks

Add Shortcut to Desktop
Click **Add Shortcut to Desktop** to add a shortcut icon to the desktop location within the 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 51 for more information.

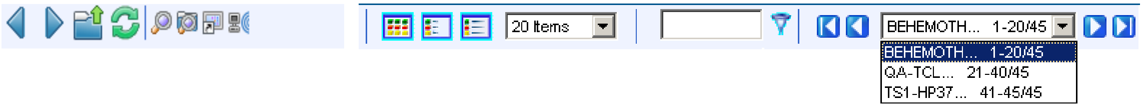
Help Desk Notify
This release introduces a streamlined task to Notify a computer from the new Help Desk Notify icon. Use the toolbar icon for Help Desk Notify to quickly Notify a single computer. Typically, this is used by Help Desk staff working on an issue. Available from any location within the desktop or zone. A computer DNS name must be entered and cannot be selected from a list. See Using Help Desk Notify on page 244 for more information.

View Properties
Click **View Properties** from the toolbar to display the properties of an object. See Viewing Properties on page 222 for more information.

Toolbar

The toolbar appears at the top of the workspace when you are viewing objects in your Portal 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 7 Sample Portal toolbar



Some figures throughout this book may show an earlier version of the toolbar. 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 Portal directory.
- Click 🔄 to refresh the information displayed in the workspace.

Task Icons

See Toolbar Tasks on page 67 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 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.

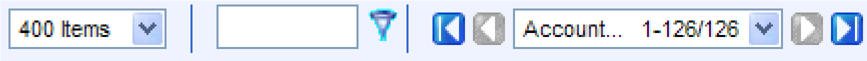
Paging and Filtering Icons

About LDAP Paging

For increased performance, the 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 Portal immediately retrieves up to one page of items using the revised page size.
- P**age 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 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.

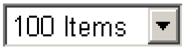
2. If necessary, page forward until the next page icon turns gray.

   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 Portal zone directories as well as external LDAP directories, such as an Active Directory.

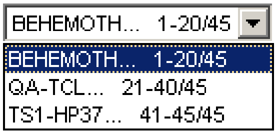
- In the filter text box, type a filter value and click ▽ to filter the retrieved objects according to their display names, common names, and cn= values.

  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:

  BEHEMOTH... 1-20/45

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

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

Portal OpenLDAP Directory and Zone Objects

Once you are familiar with the 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 Portal Directory and zone in the 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 Portal at this location. Other Portal Zones are accessed from the connections available from the Zone Access Points container.

- **Active Directory**
  An external Active Directory configured for access by a Portal administrator appears at the directory level in the workspace.

- **PRIMARY File**
  The PRIMARY File is in a Configuration Server DB on a Configuration Server, whose common name has been assigned cn=primary. Use the HPCA-CS Administration Tasks from the Portal to perform instance-level tasks on the Configuration Server DB. To configure the PRIMARY File, see Adding a Directory Service on page 111.

- **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 Portal Zone are discussed in About the Zone Containers on page 73. 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 Portal. A server must be addressable by an IP address. An example of a server would be a Windows 2003 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 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 Device Categories container.

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

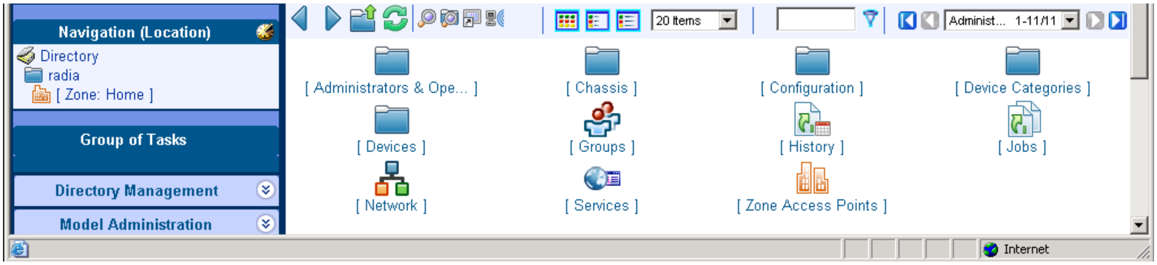
- **Directory Service**
  External Services are defined to the Portal Zone to enable a connection to

that service from within the Portal. An Active Directory, the Configuration Server DB 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 Portal zone containers that are directly beneath the zone node. Containers designated as self-managed are directory areas where no administrative operations are performed.



➤ The containers and objects allow Portal administrators to perform these tasks:

  - Perform operations against groups that are automatically created and managed by the 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 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 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 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:

  - Configuration Services – Contains an object for the default Configuration Server Database (HPCA-CS Database) and it's Primary file (cn=primary,cn=config) and schema.
  - Delegated Administrators – Container for Entitlements.
  - Device Discovery Types – Container for objects needed to discover LDAP Devices, NT Domains and HPCA Reporting Servers.
  - Directory Services (cn=ds, cn=config) – Container of available directory services. See below for more information.
  - Portal Task Groups and Tasks – Container defining the Portal Task Groups and Tasks available from the User Interface.
  - Profiles – Container for Client Automation product profiles, such as Agent installation profiles.
  - Session -- Containers with user-session objects and history
  - Web Services – Container of HTTP Service configurations. These define the URLs invoked by the Portal web services for DSML, media downloads, and processes.

- **Directory Services Container**
  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 (CSDB). Additional CSDBs can also be defined for access from this container.

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

  - **Device Architecture**
  - **Device Manufacturers** – For example, Hewlett-Packard, Dell, and Gateway device groups.

- **Enclosure Manufacturers** – For example, Hewlett-Packard and IBM are groups listed under the enclosure manufacturers for server blades.

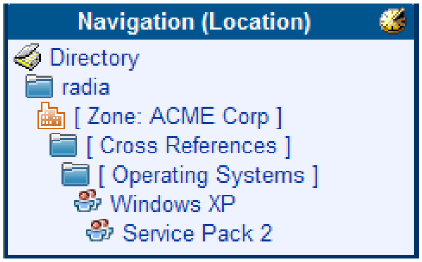
- **Infrastructure Services** – For example, Proxy Server, Portal Agent, and Configuration Server device groups.

- **Load Balancer Types** Category to hold Load Balancer Type objects; for future use.

- **Managed Services** – For example, groups for each service being managed on devices through the CM Application Manager or CM Application Self-service 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 Portal Zone. For more information, see Posting Agent Objects to the Portal on page 37.

- **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:



Navigation (Location)

Directory
radia
[Zone: ACME Corp]
[Cross References]
[Operating Systems]
Windows XP
Service Pack 2

- **OS Management** - For example, Invalid OS, No Resolved OS, Pending Hardware Configuration, Pending OS Selection and Un-Managed OS.

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

  Subnet addresses for devices use the format `nnn.nnn.nnn.nnn`.

- **VM Services** – Virtual Management Services; for example, ESX Servers.

- **Devices Container (cn=device) Self Managed**
  The Devices container holds the object properties for all devices being

managed by this Portal zone. Entries are automatically created in this container when other operations are performed, such as adding a device to a group in the Groups 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 Device Categories container entries, based on what hardware, software, managed services, and Client Automation infrastructure they contain.

- **Groups Container (cn=group)**
  Most Portal Operations are performed against groups of devices, as opposed to individual devices. The Group container holds the provided All Devices 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 Group A1.

  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.

- **History Container (cn=history)**
  Holds the daily records of completed jobs.

- **Jobs Container (cn=jobs)**
  Holds the objects for jobs and job groups scheduled or recently run by the Portal.

- **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 Portal zone.

- **Services Container (cn=service)**
  Holds the Services Catalog of all managed-service instances (ZSERVICE class instances) that are in the CSDB identified to the Portal as Primary. Within the Service catalog are sub-containers for Inventory Management, OS Management, Security Management to discover vulnerabilities, Patch Management and Sofware Management services.

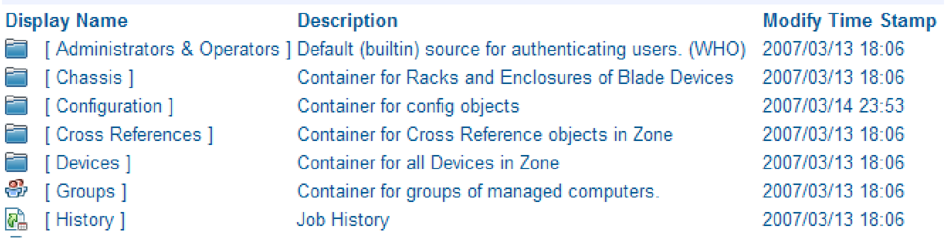
- **Zone Access Points Container (cn=zone-sap)**
  Holds an entry for the current zone and any remote zones in your enterprise that have been configured for access. From this container, you can use the Operations task to open a subordinate zone's Portal, or schedule zone operations to launch jobs across 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 8 Details view includes descriptions



Display Name	Description	Modify Time Stamp
[Administrators & Operators]	Default (builtin) source for authenticating users. (WHO)	2007/03/13 18:06
[Chassis]	Container for Racks and Enclosures of Blade Devices	2007/03/13 18:06
[Configuration]	Container for config objects	2007/03/14 23:53
[Cross References]	Container for Cross Reference objects in Zone	2007/03/13 18:06
[Devices]	Container for all Devices in Zone	2007/03/13 18:06
[Groups]	Container for groups of managed computers.	2007/03/13 18:06
[History]	Job History	2007/03/13 18:06

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

- To configure your Portal zone and bring devices under management, see Chapter 4, Administrative Functions.
- To perform operations on devices in your Portal Zone, see Chapter 5, Operations Functions.
- To perform HPCA-CS Administration Tasks on the instances in the Configuration Server DB, see Using the HPCA-CS Administration Tasks on page 79.
- To perform policy using an LDAP directory, see Using the Portal to Assign Policy through an LDAP Directory on page 85.

Using the HPCA-CS Administration Tasks

The Portal contains several tasks, stored in the HPCA-CS Administration task group, that allow you to manipulate instances in the Configuration Server DB.

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 Portal must be connected to that directory service. For details, see the following topics in Adding a Directory Service on page 111 and Starting a Directory Service on page 132.

About the HPCA-CS Administration Tasks

Use the HPCA-CS Administration task group to manage instances in the Configuration Server DB.

The following is a list of the HPCA-CS 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 connections 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 Configuration Server DB.
- **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 CSDB Editor.

- **Remove Component from Instance**
  Click **Remove Component from Instance** to remove connection(s) from the selected instance.

Creating Instances

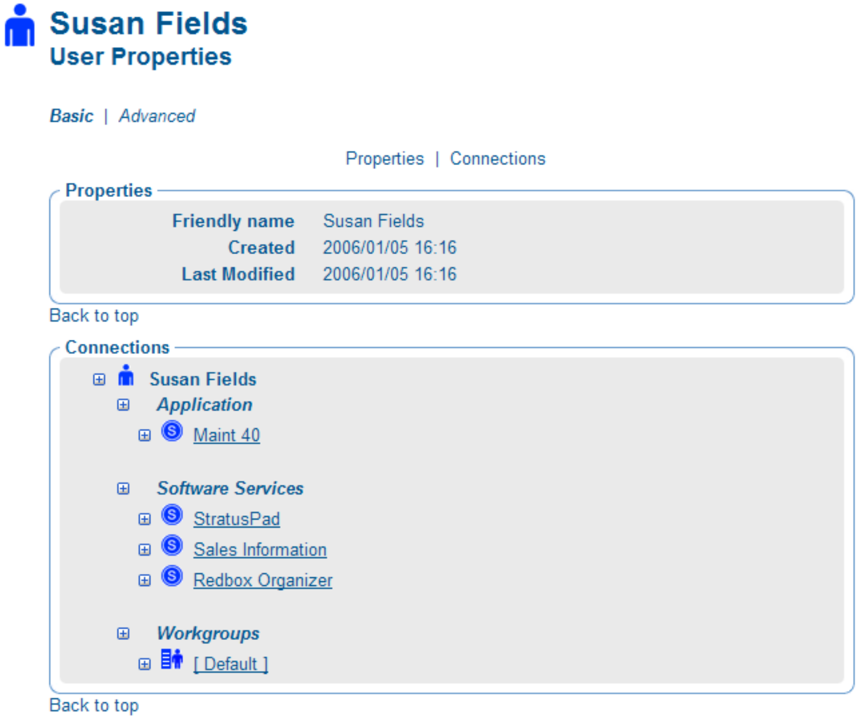
Use the Create Instance task in the HPCA-CS Administration task group to add new instances to the selected class.

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 Users class in the POLICY Domain.
2. In the HPCA-CS Administration task group, click **Create Instance**.

   The Create window opens.
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 HPCA-CS 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.

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.

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

The Connections area opens.

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 HPCA-CS Administration task group, click **Copy Instance**.

   The Copy window opens.
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 Configuration Server DB**.**

To delete an instance

1. Use the navigation aid and workspace to go to the instance that you want to delete.
2. In the HPCA-CS 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

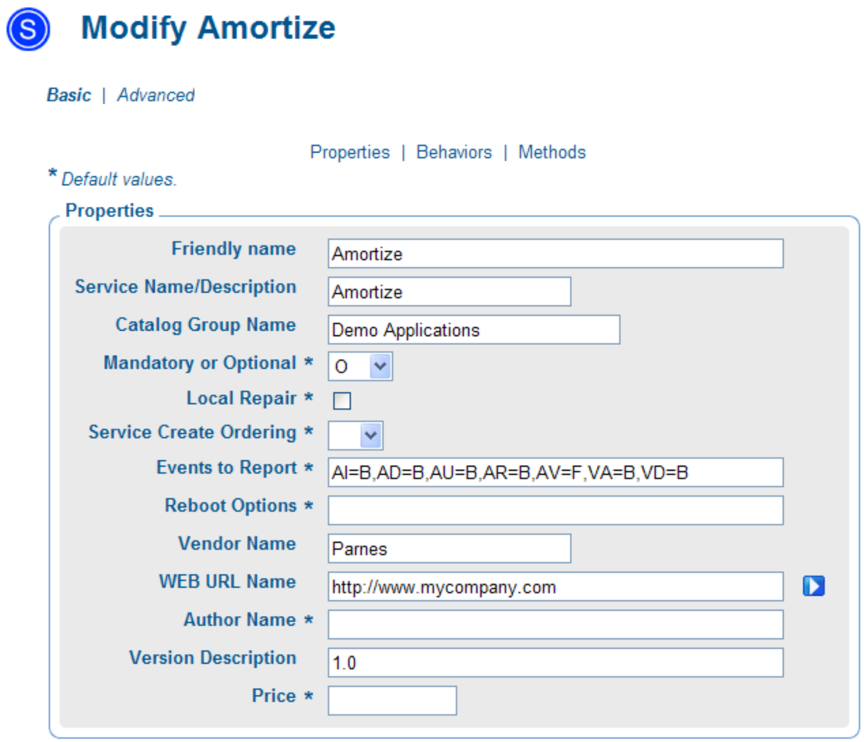
Use the Modify Instance task to modify the selected instance.

To modify an instance

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

2 In the HPCA-CS Administration task group, click **Modify Instance**.

The Modify window opens.



Modify Amortize

* Default values.

Properties

Friendly name	Amortize
Service Name/Description	Amortize
Catalog Group Name	Demo Applications
Mandatory or Optional *	O
Local Repair *	□
Service Create Ordering *	
Events to Report *	AI=B,AD=B,AU=B,AR=B,AV=F,VA=B,VD=B
Reboot Options *	
Vendor Name	Parnes
WEB URL Name	http://www.mycompany.com
Author Name *	
Version Description	1.0
Price *	

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 HPCA-CS Administration task group, click **Remove Component from Instance**.

The Remove Connections window opens.

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 the Portal to Assign Policy through an LDAP Directory

The Portal contains several tasks used to assign and manage policy through an LDAP directory. Examples of LDAP directories include Active Directory and the 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 Configuration Server Database Directory Service Properties on page 120 for more information.

- A connection to the LDAP Directory service. See Starting a Directory Service on page 132 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 128.
- 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 Portal. This is done using the PREFIX parameter in the `rmp.cfg` file. See Configuring for a Custom LDAP Policy Extension Prefix on page 138 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 *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. 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 Services Catalog**
  Click **Refresh Services Catalog** to refresh the list of services displayed in the Portal. This list is created from information in the Configuration Server DB.
- **Resolve Policy**
  Click **Resolve Policy** to resolve the service entitlements for an object. The list is grouped by product type and then policy source, and may be viewed for a given domain filter (DNAME). For LDAP objects, you can add values for the attributes, such as Hostname, OS, UserID, and Context, which are normally available when the LDAP policy is resolved.

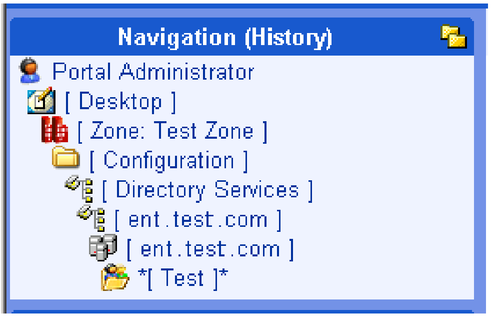
Adding a Policy Object

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

To add a policy object

1 Use the navigation aid 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 [ent.test.com]. A policy object will be added to the [Test] container.



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

The Add Policies window opens.

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

The Add Group window opens.

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 Portal.

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.

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.

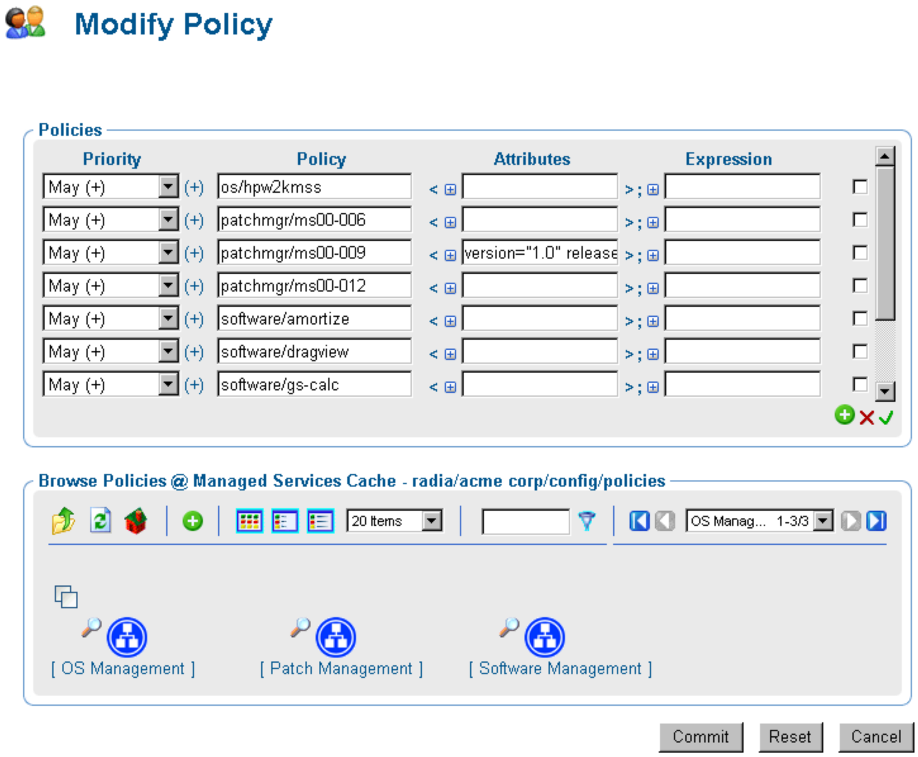
To modify policies

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

2 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

Policies

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/gs-calc	< ⊞		>; ⊞		□

Browse Policies @ Managed Services Cache - radia/acme corp/config/policies

20 Items

OS Manag... 1-3/3

[OS Management] [Patch Management] [Software Management]

3 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 142 for information on how to use this window. Within that section, see Using the Attribute Editor on page 147 for information on how to modify service attributes, and see

Using the Expression Editor on page 150 for information on how to modify the constraints for a service using the expressions editor.

4 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.

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.

3 Use the Modify Policy Targets window to select the appropriate targets. See Basic Procedures for Modifying Groups on page 142 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.

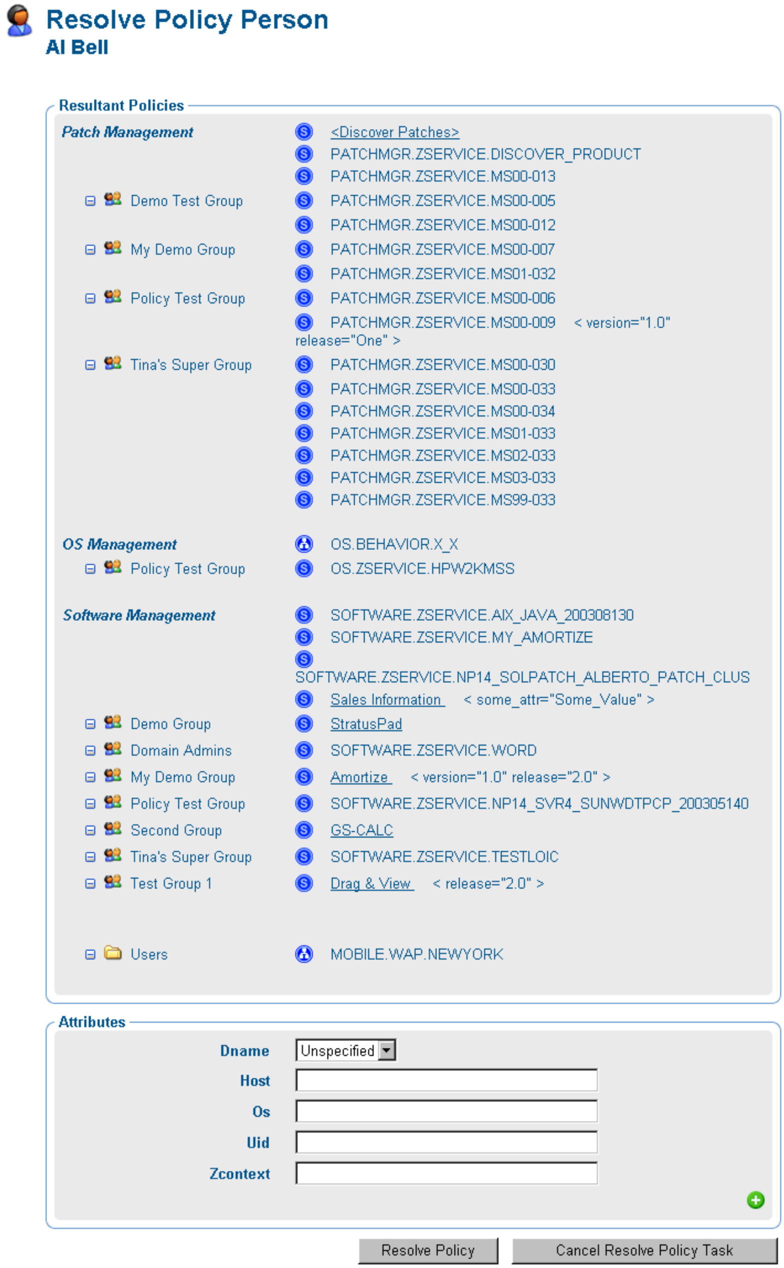
> If you customized the set of domain filters (DNAMEs) in the Policy Server configuration file (`pm.cfg`), you can also customize the domain filters available in the Resolve Policy task of the Portal. See Customizing Domain Filters (DNAMEs) in the Resolve Policy Task on page 92 for details.

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.



Resolve Policy Person
Al Bell

Resultant Policies

Patch Management	<Discover Patches> PATCHMGR.ZSERVICE.DISCOVER_PRODUCT PATCHMGR.ZSERVICE.MS00-013
⊟ Demo Test Group	PATCHMGR.ZSERVICE.MS00-005 PATCHMGR.ZSERVICE.MS00-012
⊟ My Demo Group	PATCHMGR.ZSERVICE.MS00-007 PATCHMGR.ZSERVICE.MS01-032
⊟ Policy Test Group	PATCHMGR.ZSERVICE.MS00-006 PATCHMGR.ZSERVICE.MS00-009 < version="1.0" release="One" >
⊟ Tina's Super Group	PATCHMGR.ZSERVICE.MS00-030 PATCHMGR.ZSERVICE.MS00-033 PATCHMGR.ZSERVICE.MS00-034 PATCHMGR.ZSERVICE.MS01-033 PATCHMGR.ZSERVICE.MS02-033 PATCHMGR.ZSERVICE.MS03-033 PATCHMGR.ZSERVICE.MS99-033
OS Management	OS.BEHAVIOR.X_X
⊟ Policy Test Group	OS.ZSERVICE.HPW2KMSS
Software Management	SOFTWARE.ZSERVICE.AIX_JAVA_200308130 SOFTWARE.ZSERVICE.MY_AMORTIZE SOFTWARE.ZSERVICE.NP14_SOLPATCH_ALBERTO_PATCH_CLUS Sales Information < some_attr="Some_Value" >
⊟ Demo Group	StratusPad
⊟ Domain Admins	SOFTWARE.ZSERVICE.WORD
⊟ My Demo Group	Amortize < version="1.0" release="2.0" >
⊟ Policy Test Group	SOFTWARE.ZSERVICE.NP14_SVR4_SUNWDTPCP_200305140
⊟ Second Group	GS-CALC
⊟ Tina's Super Group	SOFTWARE.ZSERVICE.TESTLOIC
⊟ Test Group 1	Drag & View < release="2.0" >
⊟ Users	MOBILE.WAP.NEWYORK

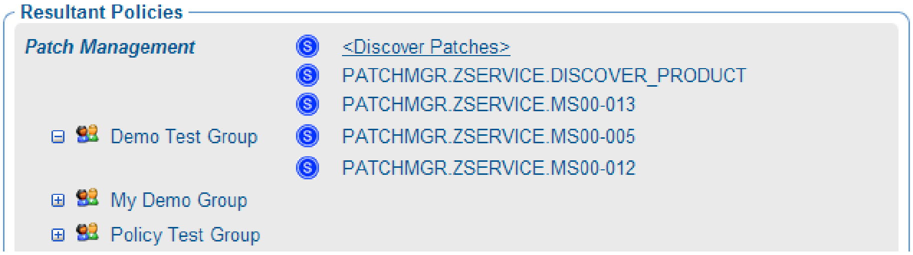
Attributes

Dname	Unspecified
Host	
Os	
Uid	
Zcontext	

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, Security 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.



Resultant Policies

Patch Management

<Discover Patches>
PATCHMGR.ZSERVICE.DISCOVER_PRODUCT
PATCHMGR.ZSERVICE.MS00-013

⊟ Demo Test Group

PATCHMGR.ZSERVICE.MS00-005
PATCHMGR.ZSERVICE.MS00-012

⊞ My Demo Group

⊞ Policy Test Group

- — 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 Client Automation to the LDAP Policy Adapter.

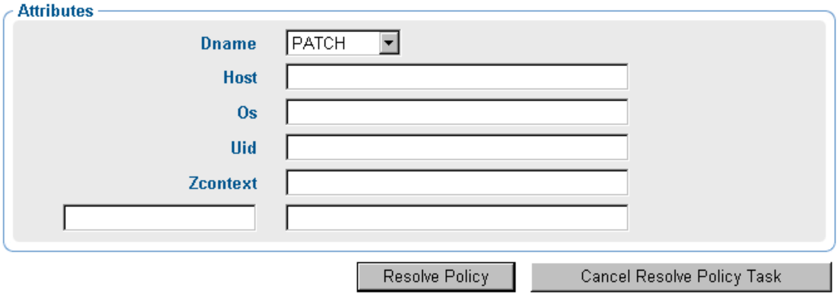
If you customized the set of DNAMEs in your `pm.cfg` file, you can modify the Dname selection list values for the Resolve Policy task. See Customizing Domain Filters (DNAMEs) in the Resolve Policy Task on page 92 for more information.

- — 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 WINVISTA, 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 Configuration Server DB.

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.



Dname: PATCH

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.

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 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 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 Portal Resolve Policy task you must modify the `httpd.rc` file, which is located in the etc directory of where the 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 }

}
```

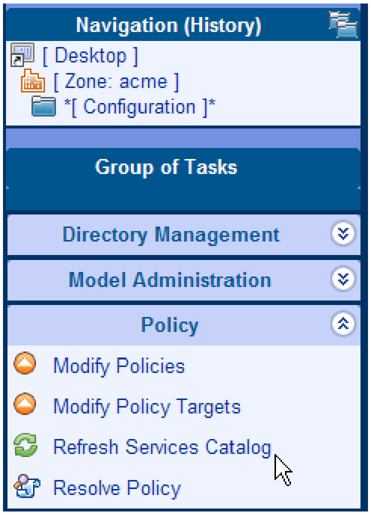
Save the changes to the `httpd.rc` file and restart the Portal service. The modified filter settings will be available from the Dname drop-down list on the Resolve Policy task.

Refreshing the Services Catalog

Use the Refresh Services Catalog task to periodically refresh the list of services displayed in the Portal. This list is created from information in the Configuration Server DB that is connected to the Portal using a Directory Service type of ds-rcs.

To refresh the services catalog

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



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

About the Policy (Advanced) Tasks

Use the Policy (Advanced) task group to modify the 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 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. We recommend that you use this task sparingly.

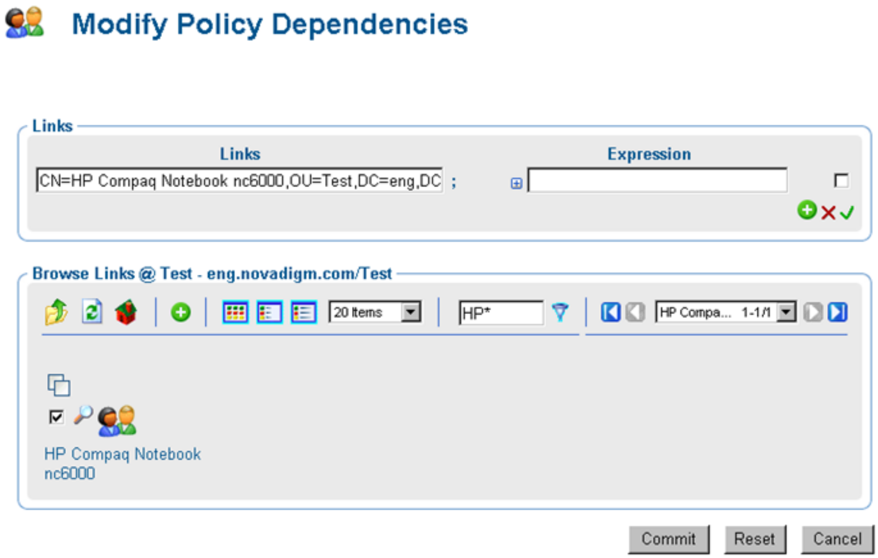
Example

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 142 for information about how to use this window.



Modify Policy Dependencies
Links
Links
Expression
Browse Links @ Test - eng.novadigm.com/Test
20 Items
HP*
HP Compa... 1-1/1
HP Compaq Notebook nc6000
Commit
Reset
Cancel

Links: CN=HP Compaq Notebook nc6000,OU=Test,DC=eng,DC ;

4 If you want to add any additional constraints use the Expression Editor. See Using the Expression Editor on page 150 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.

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

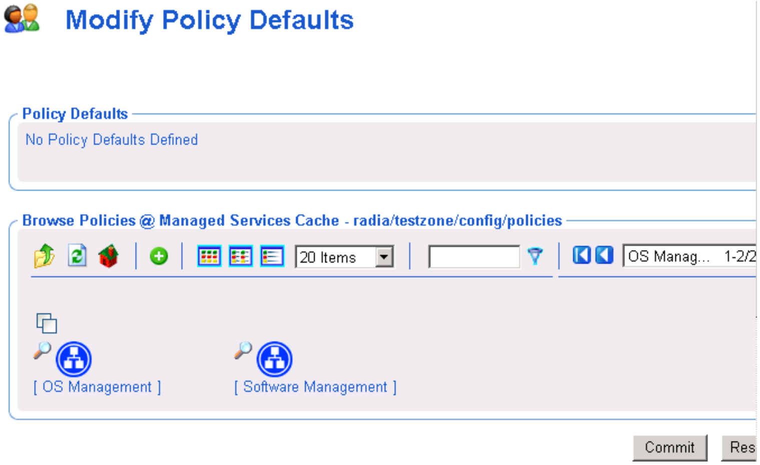
If the Sales application does not have a version specified, you can use this task to specify the default version to be deployed to the target machines.

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.



Modify Policy Defaults

Policy Defaults

No Policy Defaults Defined

Browse Policies @ Managed Services Cache - radia/testzone/config/policies

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 147 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 150 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

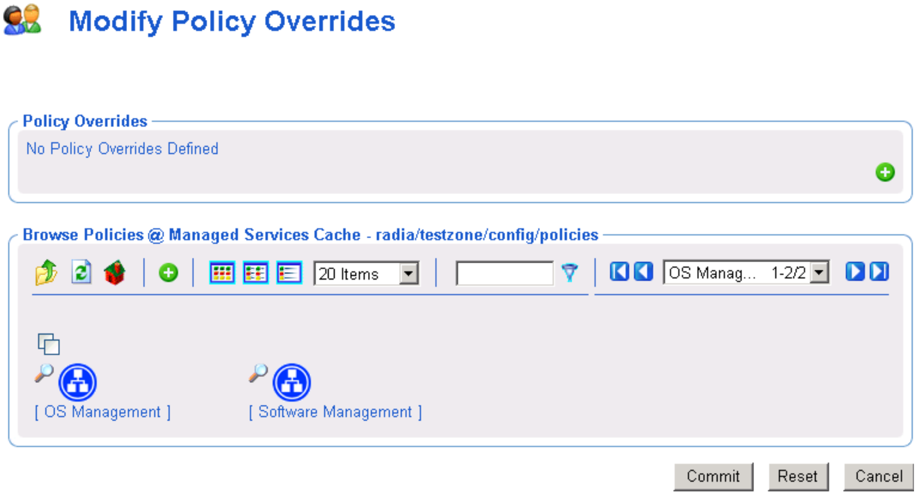
Bob Smith is entitled to the Sales application, version 1. Use this task to override the version information for Bob alone, and entitle him to version 2.

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.



No Policy Overrides Defined

3 Use this window to select the service whose overrides you want to define. See Basic Procedures for Modifying Groups to learn how to use it.

4 After you select a service, use the Attribute Editor to specify the override values. See Using the Attribute Editor on page 147 to learn 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 150 to learn how to use this editor and the *Policy Server Guide* for details about expressions.

Summary

- The Portal has a consistent user interface, which means that you can follow the same basic procedure to complete any task.
- The 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 Zone, by default. You can add or remove Shortcuts to your Desktop that link to frequently used navigation locations.
- The 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 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 Portal contains several tasks, stored in the HPCA-CS Administration task group, that allow you to manipulate instances in the Configuration Server DB.
- The 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 Portal Zone for Network Discovery and Directory Services.
- Be able to connect to and disconnect from a Directory Service or Configuration Server Database, or other object defined in the Directory Services container.
- Understand the various methods of bringing devices under management by a 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 Portal Directory.
- Be able to manage the 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 Portal.

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

New for this release is the configuration of Directory Services to allow users access to the PRIMARY File and your existing LDAP directories, such as Active Directory for Policy administration. For details, see Configuring Directory Services on page 111.

Also new for this release are the containers and tasks used to bring devices under management by the Portal Zone. For details, see Establishing Devices and Device Groups on page 140.

Configuring a Portal Zone

⚠ If your environment uses Core and Satellite servers, first read the *Core and Satellite Servers Getting Started Guide* as the installation, configuration and troubleshooting information in that guide may override the information in this guide.

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 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 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 Portal Zone can be further clustered into different groups to expedite common operations.
- **Subordinate Zones**
  From the initial Portal, run the Install Zone task to remotely install subordinate zones in your enterprise, each with a unique name. All zones

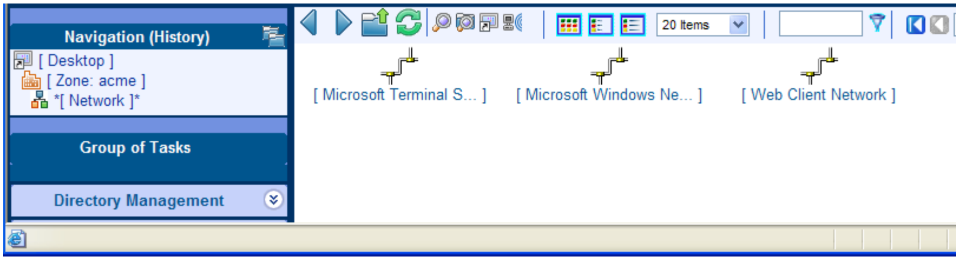
retain an entry in the Zone Access Points container, which can be used to schedule Zone Operations on devices in all zones in your enterprise.

- **Task Templates**
  Task templates need to be added before scheduling jobs for Zone Operations.
- **Device Categories Container**
  The groups in the Device Categories container are self-managed. They are automatically created after the Portal Agent is installed on devices in the Device container, and dynamically maintained.

Understanding Network Discovery

If enabled during the install, the 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 → Network** location, where they can be selected for management by the Portal Zone.

Figure 9 Sample Network containers with discovered objects

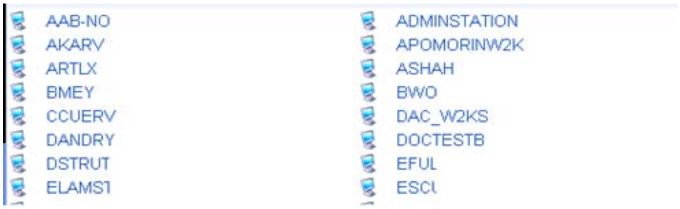


To view the objects discovered in a specific network, navigate to the **Zone →Network** container and then click the specific network object in the workspace. For example:

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

Figure 10 on page 104 shows the objects discovered in a sample Microsoft Windows Network domain.

Figure 10 Sample Microsoft Windows Network domain devices



AAB-NO
AKARV
ARTLX
BMEY
CCUERV
DANDRY
DSTRUT
ELAMS1
ADMINSTATION
APOMORINW2K
ASHAH
BWO
DAC_W2KS
DOCTESTB
EFUL
ESCL

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 HPCA Portal service (httpd-managementportal).

2 Use a text editor to open the Portal configuration file, `rmp.cfg`, located by default in *SystemDrive*`:\Program Files\Hewlett-Packard\CM\ManagementPortal\etc`.

3 Look for these lines defining the the initial parameters. Your entries will vary from the code sample below.

```
rmp::init {
    ENABLE_BACKUP           1
    NETSCAN                 Yes
    NETSCAN_POLL            86400
    NETSCAN_START_DELAY     900
    URL                     /
    ZONE                    "cn=myzone, cn=radia"
    ZONE_BACKUP_PORT        3475
    ZONE_PORT               3474
}
#
```

```
# END OF CONFIG

#
```

4 You can insert any of the parameters in Table 3 below into this file before the finishing curly bracket (}) as shown in the code sample above.

5 Use a space to separate the parameter and its value.

Table 3 Parameters to Configure Network Discovery

Parameters	Explanation
NETSCAN	Enables or disables network discovery. Default is disabled. During the install the user can set this value to enabled or disabled. • Type **NETSCAN 0** to disable network discovery. • Type **NETSCAN 1** to enable network discovery.

NETSCAN_START _DELAY	The time to wait (in seconds) before starting network discovery when the Portal starts up. Default is 15 minutes (900 seconds).
	You can specify this value as:
	`NETSCAN_START_DELAY 900`
	Another way to specify this value is by using a Tcl expression, which would read as follows:
	`NETSCAN_START_DELAY {15*60}`
	where 15 is the number of minutes. When multiplied by 60 seconds, the value becomes 900 seconds.

NETSCAN_POLL	Network Discovery Interval (in seconds). Default setting is 86400 seconds, or 24 hours. Optionally, specify this value using a Tcl expression in curly brackets. For example: to specify 12 hours, enter: **NETSCAN_POLL {12*60*60}** where 12 is the number of hours, multiplied by 60 minutes, multiplied by 60 seconds.
NETSCAN _INCLUDE	For each object class specified, limits network discovery to only those objects named in the include list. Default is to include all discovered objects in all classes within the network.

Parameters	Explanation

	Use the following syntax:
	`NETSCAN_INCLUDE { object_class {object_list} object_classn {object_list} }`
	where:
	object_class is a class whose discovered objects are to be restricted to the members specified in the following object list. Valid object classes include, but are not limited to: network, tree, domain, computer. Your network may include other classes. Tip: Any object's class is listed when you hover the mouse pointer over its icon.
	object_list is a space-separated list of common names within curly brackets. These are the only objects to be included in network discovery for the given object class. Unnamed objects in the specified class are excluded.
	All names are case-insensitive.
	Example: The following limits discovery to all objects found in the two listed domains in the Microsoft Windows Network. No other networks will be discovered.
	`NETSCAN_INCLUDE { network {lanmanredirector} domain {domain1 domain2} }`
	For additional examples, see Using NETSCAN_INCLUDE to Limit Network Discovery on page 106.

6 Save and close the file.

7 Restart the HPCA Portal service (httpd-managmentportal) and open the 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 3 on page 105. 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:

- Nnetwork discovery (see page 104)
- LDAP authentication (see page 135)
- Managing Portal Agent Signal Processing (see page 318)

Table 4 below, lists the parameters you can add to or modify in the `rmp.cfg` file for options that are not related to any of the topics listed above.

For detailed steps on how to modify parameters in the `rmp.cfg` file, refer to the procedure To configure network discovery on page 104.

Table 4 Additional Portal Configuration Parameters in RMP.CFG

Parameter	Definition
`ENABLE_BACKUP`	Creates the resources needed to replicate the Portal's OpenLDAP database and enables the Backup Directory task in the Directory Management task group. Refer to Setting Backup Configuration Parameters on page 205 for more information. Default is Y. Valid values are Y or N.
`LINKS`	Specifies the policy configuration links to enable when policy has been applied to the objects in the Chassis container and related Device Categories containers for server blade devices. Refer to Enabling Policy Configurations for Blades, Enclosures and Racks on page 185 for the details on specifying the attributes for this parameter.

Parameter	Definition

`LISTENING_ADDRESS`	Specifies a valid network address (either an IP address, hostname, or DNS address) that is to be passed to Portal Agents, and then used by them to connect back to the Portal.
	Use a LISTENING_ADDRESS when the Management Agents are experiencing communication failures with the Portal and are successful in registering back to the Portal or performing remote tasks on behalf of the Portal. This can occur when the Portal 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:
	`LISTENING_ADDRESS` *`IPaddress`*
	or
	`LISTENING_ADDRESS` *`hostname`*
	`or`
	`LISTENING_ADDRESS` *`DNS`*
	Ensure the network address you enter points to the current Portal Zone. If it does not, results are unpredictable.

`RCS_AUTO_CONNECT`	When a Primary Configuration Server directory service is defined for the Portal, controls an automatic connection to the Primary Configuration Server whenever the Portal is started and the ds-rcs Startup property is set to Auto or Manual. The `RCS_AUTO_CONNECT` is not enforced when Startup is set to Disabled. Default value is 1 (enabled). Enter `RCS_AUTO_CONNECT 0` to disable the automatic connection to the Primary Configuration Server; and revert to the connections as defined by the ds-rcs Startup property in Table 7 on page 121.

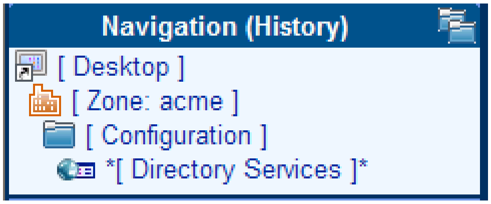
Parameter	Definition
REFRESHMSC	When a Primary Configuration Server directory service is defined for the Portal, controls how often the Portal updates its *Managed Services Catalog* with those available in the source Configuration Server database. The Managed Services Catalog serves as the CM Definitive Software Library, and is accessible from the Services object (cn=services) located in the root of the Portal directory. Default value is 600 seconds, or 10 minutes. Specify a different interval for the refresh of the Managed Services Catalog in seconds.
USE_FQDNSHOST_NAME	Specifies that Portal 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 Portal Agent, and contacting the Portal Agent. • Type **USE_FQDNSHOST_NAME 0** to use short names (that is, the left-most portion of a fully qualified name). Customers whose DNS tables contain imperfect entries may want to switch to the use of short names. • Type **USE_FQDNSHOST_NAME 1** to return to the use of fully qualified domain names (the default).

Parameter	Definition
WOL_MCAST_ADDR	Permits Wake-on-LAN (WOL) support in multicast-enabled environments. Default is no support for multicast WOL. • Type **WOL_MCAST_ADDR <***IP_address***>** where the <*IP address*> specifies the multicast address to use to revolve a WOL request. • Type **WOL_MCAST_ADDR 0** to return to standard WOL support (no multicast WOL support). This is the default.
ZONE_PORT_BACKUP	Port used to communicate with the backup (replicated) database. Refer to Setting Backup Configuration Parameters on page 205 for more information. Required if ENABLE_BACKUP is set to 1. Default is port 3475.

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 below.

Figure 11 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 Portal Zone directory service to another directory service. You can add any of the following types of directory services to your Portal 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 113 for more information.
- **RCS**
  Use this type to connect a Configuration Server and access the PRIMARY File in the Configuration Server DB.
- **DSML**
  Use this type to connect to another Portal zone in your enterprise.

  When you install another Portal zone using the Install Subordinate Portal task, this type of Directory Service connection is created automatically.

  To secure a Portal to Portal connection using SSL, refer to the instructions in the *HP Client Automation SSL Implementation Guide (SSL Implementation Guide).*
- **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 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 Portal startups.

- — An automatic connection will always connect to the Directory Service when the Portal starts up, as long as the directory is available.
- — A manual connection will not always connect to the Directory Service when the Portal starts up; it will reconnect if the Directory Service was connected when the Portal last shut down, or, it will connect if there are certain overrides in place. Otherwise, it requires user to connect to the Directory Service manually; this is discussed in To start a predefined Directory Service on page 161.

  For more information on the Manual Startup behavior, see Directory Service Connection Status upon Portal Restart on page 126.
- — 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 161.

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.

- 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.
- Ensure the latest version of the `ldaps82.dll` distributed with the Portal is currently located the Portal base install directory: `C:\Program Files\Hewlett-Packard\CM\ManagementPortal`.
- If the server hosting the LDAP directory uses 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 Portal. By default, the Portal installs a folder and certificate file which can be used to store the public key:

CACertficate File	`cacert.pem`
CACertficate Directory	`\`*`Portal_dir`*`\etc\CACertficates`

  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 Portal.

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

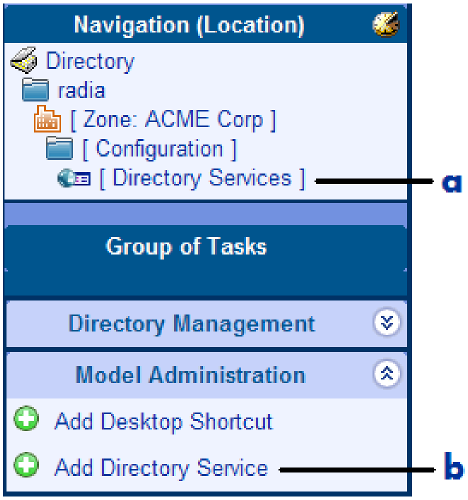
You will need to reference this file and its location when you add an LDAPS directory service in the CA Certificate File and CA Certificate Directory properties on the Add Directory Service page.

- 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.
- Refer to the *SSL Implementation Guide* for more information regarding certificates and securing your Client Automation environment.

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 5 Adding a directory service by type

Type	Directory Service Connection
ds-dsml	`DSML`: an external Directory Service, such as another Portal 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 service that hosts the Configuration Server Database. Note: The Configuration Server 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 116

— Specifying Configuration Server Database Directory Service Properties on page 120

— Specifying DSML Directory Service Properties on page 124

— Specifying Metakit Directory Service Properties on page 125

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 on page 132.

Specifying LDAP or LDAPS Directory Service Properties

Use Table 6 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 113 prior to adding an LDAPS directory service.

Table 6 Directory Service properties for Type ds-ldap or ds-ldaps

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

Field	**Description**
Startup	Select auto, manual, or disabled. For more information, refer to Directory Service Connection Status upon Portal Restart on page 126. **Auto** Specifies the connection to this Directory Service will be automatic whenever the Portal Zone starts up. **Manual** Upon startup or restart, the Portal will connect to this LDAP Directory Service if either of the following are true: • The Used for Policy property is set to True. • The Directory Service was connected when the Portal last stopped. Otherwise, the Portal will not connect to this Directory Service at startup. If necessary, use the Start Directory Service task to connect to this Directory Service during a Portal session. **Disabled** Upon Portal startup or restart, restricts any connection to or mounting of this Directory Service. The startup status must be changed to auto or manual before a connection to this Directory Service can take place.
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 113.

URL
(Web Page Address)
	LDAP Format and Examples:
	`ldap://`*`<IP address or qualified computer name>`*`:`*`<LDAP port>`*`/`*`<qualified username>`*
	`ldap://10.10.10.1:389/administrator@eng.acme.com`
	`ldap://svr209.usa.mycompany.com:389/admin@usa.mycompany.com`
	Novell Directory Server (NDS) Format and Examples:

Field	Description

	`ldap://<IP address or qualified computer name>:<LDAP port>/<full dn of binding User>`
	`ldap://10.10.10.55:389/cn=rpolicymgr,ou=pcbadm,o=pcb`
	LDAPS Format and Examples:
	`ldaps://<LDAP hostname in certificate>:<LDAP secure port>/<bind User>@<domain>`
	`ldaps://svr3.eng.acme.com:636/administrator@eng.acme.com`
	Do not enter an IP address to specify the URL for ldaps; SSL does not verify IP addresses.

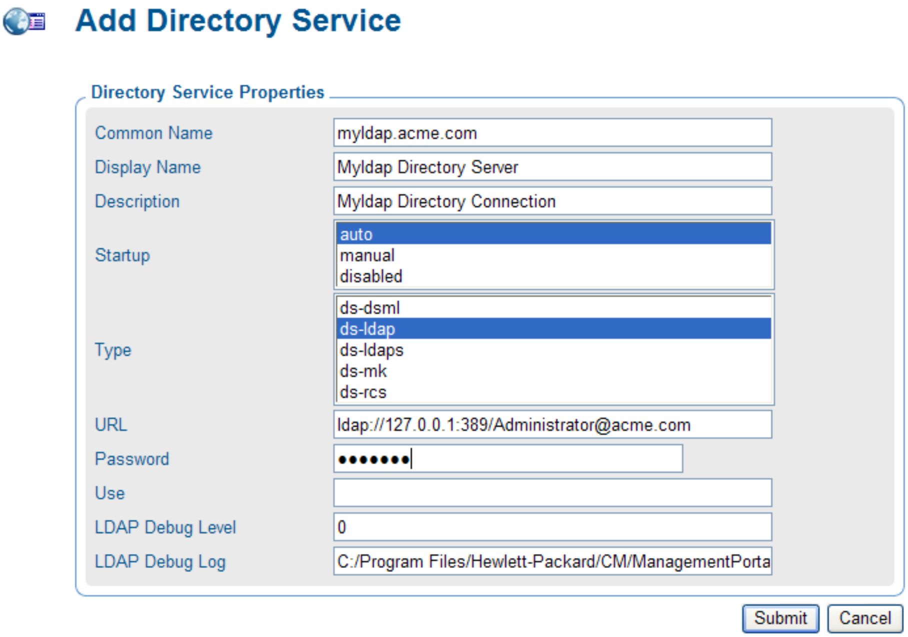
Password	Password for the username entered in the URL
Used for Policy	Default: false **False** indicates this LDAP directory service is not to be used for policy tasks. **True** enables the use of this Directory Service for all policy tasks. To set this field, use the Modify task from the Model Administration task group.
Use	Specifies a fully-qualified domain at which to mount the directory service. This mount point becomes the highest level of the directory structure that can be accessed from the Portal. For example, to mount and limit the use of the eng.acme.com directory to the Computers domain, specify the properties for this Directory Service with a Use value of: cn=computers,dc=eng,dc=acme,dc=com For NDS, a typical Use value is: cn=pcb If left blank, the common name is used to mount the directory service at the highest level.

Field	Description
CA Certificate Directory	Available with Type **ds-ldaps** only. Default: `<ManagementPortalDir>/etc/CACertificates` 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 113 for more information.
CA Certificate File	Available with Type **ds-ldaps** only. Default: `cacert.pem` File name containing the CA Certificate public key for the LDAP host server. See Preparing for an LDAPS Directory Service Connection on page 113 for more information.
LDAP Debug Level	Default: 0 (no LDAP logging) We do 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.
LDAP Debug Log	Default: `<<ManagementPortalDir>/logs/ldap.log` The path and filename used for logging LDAP debug entries when the LDAP Debug Level is greater than 0.

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 12 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 manual disabled
Type	ds-dsml ds-ldap ds-ldaps ds-mk ds-rcs
URL	ldap://127.0.0.1:389/Administrator@acme.com
Password	•••••••
Use	
LDAP Debug Level	0
LDAP Debug Log	C:/Program Files/Hewlett-Packard/CM/ManagementPorta

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 128.

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 138.

Specifying Configuration Server Database Directory Service Properties

Refer to the following table to complete the Directory Service Properties for a Configuration Server (HPCA-CS) Database Directory Service connection.

The Portal will build a Managed Services Catalog from the managed services in the specified database of the Primary Configuration Server service and automatically refresh the catalog every 10 minutes. To adjust the refresh rate, use the REFRESHMSC configuration parameter listed in Table 4 on page 108.

Table 7 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 Configuration Servers may be defined as Directory Service objects. However, only the Configuration Server 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. For more information, refer to Directory Service Connection Status upon Portal Restart on page 126. **Auto** Specifies that connection to this Directory Service is automatic whenever the Portal Zone starts up. **Manual** For a Primary ds-rcs only, a default entry in the `rmp.cfg` file overrides the usual Manual startup behavior, and the Portal **automatically** connects to the Primary Configuration Server at startup whenever the Startup value is Auto or Manual. If the RCS_AUTO_CONNECT parameter in the rmp.cfg file is reset to 0, the Manual startup behavior applies. Manual startup behavior: If the Directory Service was connected when the Portal last stopped, it will resume the connection to the Directory Service upon a restart. If the Directory Service was not connected when the Portal last stopped, the Portal will not connect to it. If necessary, use the Start Directory Service task to connect to this Directory Service during a Portal session. **Disabled** Upon Portal startup or restart, restricts any

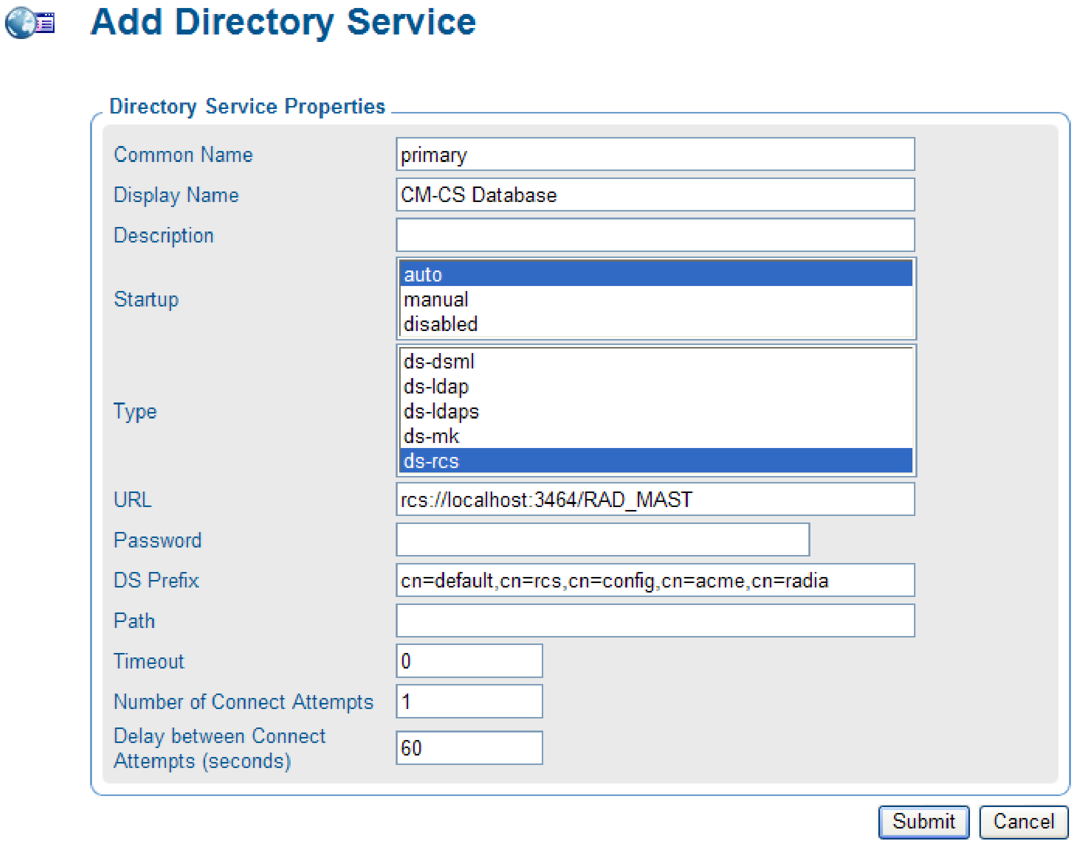
Field	Description
	connection to or mounting of this Directory Service. The startup status must be changed to auto or manual before a connection to this Directory Service can take place.
Type	**ds-rcs** Type required to connect to a Configuration Server directory service.
URL (Web Page Address)	Default entry: `rcs://localhost:3464/RAD_MAST` Format: `rcs://`*`<hostname or IP address>`*`:`*`<port #>`*`/`*`<Username>`* Example: `rcs://myserver600:3464/RAD_MAST` Change *`<localhost>`* to specify the qualified host name or IP address of your Configuration Server, and if necessary, change the Username from the RAD_MAST default to the one used at your installation. The port number is normally 3464.
Password (User Password)	Password for the username entered in the URL.
Path (see Modify task)	Optional entry for expediting a connection to the PRIMARY File. Specifies the fully qualified path of `ZTOPTASK.EXE` on the Configuration Server. Use forward slashes for Windows and UNIX. For example: `C:/Program Files/Hewlett-Packard/CM/ConfigurationServer/bin/ztoptask.exe`
Timeout	Period of inactivity (defined in seconds) after which a Configuration Server connection will timeout and the connection will be dropped. Leave the default value of 0 to never have a Configuration Server connection timeout. To have the Configuration Server connection timeout after a specific period of inactivity, type the timeout period in seconds in the **Timeout** text box.

Field	Description
Number of Connect Attempts	Default is 1 attempt. Enter the number of times the Portal will attempt to connect to the Configuration Server Database after an automatic or manual startup request. Multiple attempts may be necessary if the Configuration Server is not already started when the Portal makes its first connection attempt.
Delay between Connect Attempts (in seconds)	Enter the number of seconds to wait between a failed connection attempt and the next try. The default is one minute, or 60 seconds.

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

The following figure shows a sample set of directory service properties for accessing the PRIMARY File on a Configuration Server.

Figure 13 Sample Configuration Server Directory Service Properties



Add Directory Service

Directory Service Properties

Common Name	primary
Display Name	CM-CS Database
Description	
Startup	[✓ auto] manual disabled
Type	ds-dsml ds-ldap ds-ldaps ds-mk [✓ ds-rcs]
URL	rcs://localhost:3464/RAD_MAST
Password	
DS Prefix	cn=default,cn=rcs,cn=config,cn=acme,cn=radia
Path	
Timeout	0
Number of Connect Attempts	1
Delay between Connect Attempts (seconds)	60

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 the directory service for another Portal Zone.

URL for a Secured DSML Connection

The DSML connection may be secured using SSL. The information on the prerequisites and details are in the *SSL Implementation Guide*.

The URL format for a secured DSML connection must use the HTTPS protocol, and the port that is specified must be the secure port of the subordinate Portal. The following is an example of an acceptable URL.

https://subportal:443/proc/dsml

where...

subrmp is the *subordinate Portal hostname*

443 is the *secure port*

Specifying Metakit Directory Service Properties

Advanced users can extend the capabilities of their 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 Table 8 below for guidance on specifying Directory Service properties.

Table 8 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.

Field	Description
Startup	Select auto, manual, or disabled. For more information, refer to Directory Service Connection Status upon Portal Restart on page 126. **Auto** Specifies the connection to or mounting of this Directory Service will be automatic whenever the Portal Zone starts up. **Manual** Upon startup, the Portal will resume the same connection status with the Directory Service as when the Portal was last stopped. If the Directory Service was connected, it Portal will reconnect to it; if the Directory Service was not connected, the Portal will not automatically reconnect to it. If necessary, use the Start Directory Service task to connect to this Directory Service during a Portal session. **Disabled** Upon Portal startup or restart, restricts any connection to or mounting of this Directory Service. The startup status must be changed to auto or manual before a 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.

Directory Service Connection Status upon Portal Restart

Startup Property Set to Auto or Disabled

Without exception, when a Directory Service’s Startup property is set to Auto, the Directory Service will be reconnected when the Portal is restarted.

Likewise, without exception, when a Directory Service's Startup property is set to Disabled, the Directory Service will not be connected when the Portal is restarted.

Startup Directory Service Property - Set to Manual

When a Directory Service's Startup property is set to Manual, there are several conditions and parameter-based overrides that affect whether or not the Directory Service will be connected after a Portal restart.

1. For a ds-ldap Directory Service, if the **Use for Policy** property is set to True, it will override a Manual startup setting and the Portal will always reconnect to the Directory Service upon restart.
2. For the Primary ds-rcs Directory Service, a Manual setting is overridden by the default **RCS_AUTO_CONNECT** 1 setting in the rmp.cfg file, which means the Portal will always reconnect to the Primary Configuration Server Directory Service upon restart.

   To disable the RCS_AUTO_CONNECT 1 entry, edit the rmp.cfg file and add the configuration parameter: RCS_AUTO_CONNECT 0. Save the rmp.cfg file and restart the HPCA Portal Service.
3. If the above overrides do not apply, the Portal will resume a previous Directory Service connection upon restart, but will not connect to the Directory Service if it was not connected when the Portal shut down.

The following tables also summarize the Manual Startup behavior for an LDAP, Primary ds-rcs and Non-primary ds-rcs Directory Service. If the Directory Service is connected to the Portal, its **Job activity** property indicates **started**.

Table 9 LDAP Directory Service Connection - Startup Property is Manual

Properties upon Portal shut-down		**Property upon Restart**
Used for Policy?	**Job activity**	**Job activity**
Yes	Does not matter	Started
No	Started	Started
No	Stopped	Stopped

Table 10 Primary CS Directory Service Connection - Startup Property is Manual

Configuration upon Portal shut-down		Property upon Restart
RCS_AUTO_CONNECT	**Job activity**	**Job activity**
1 (default)	Does not matter	Started
0 (set in rmp.cfg)	Started	Started
0 (set in rmp.cfg)	Stopped	Stopped

Table 11 Non-primary CS Directory Service Connection - Startup is Manual

Property upon Portal shut-down	Property upon Restart
Job activity	**Job activity**
Started	Started
Stopped	Stopped

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.

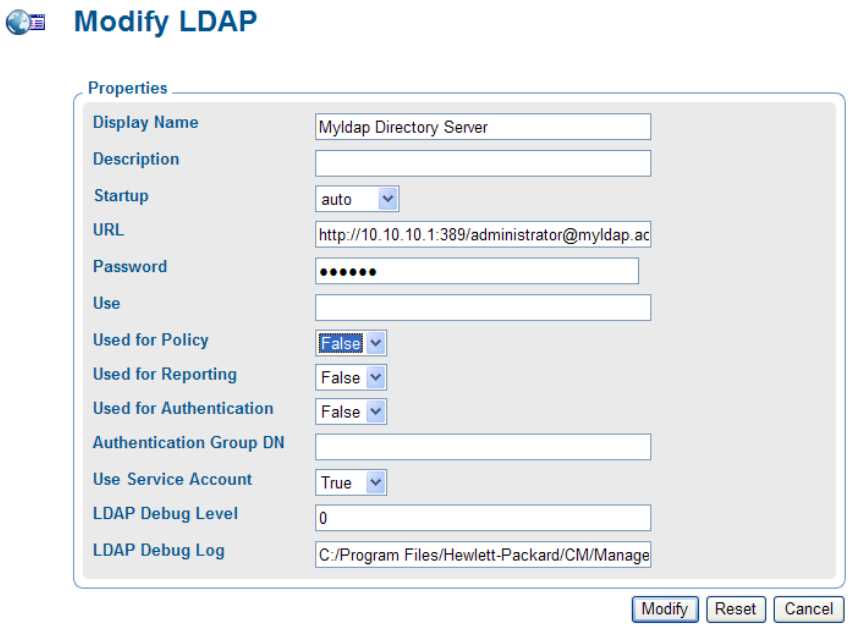
To modify a Directory Service Property

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

Properties

Display Name	Myldap Directory Server
Description	
Startup	auto
URL	http://10.10.10.1:389/administrator@myldap.ac
Password	••••••
Use	
Used for Policy	False
Used for Reporting	False
Used for Authentication	False
Authentication Group DN	
Use Service Account	True
LDAP Debug Level	0
LDAP Debug Log	C:/Program Files/Hewlett-Packard/CM/Manage

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 111.

4 For details on using the **Used for Reporting, Used for Authentication** and **Authentication Group DN** fields, refer to Modify LDAP Directory Service Options (for Web Services External Authentication and Filtering) on page 130.

5 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 138 for more information.

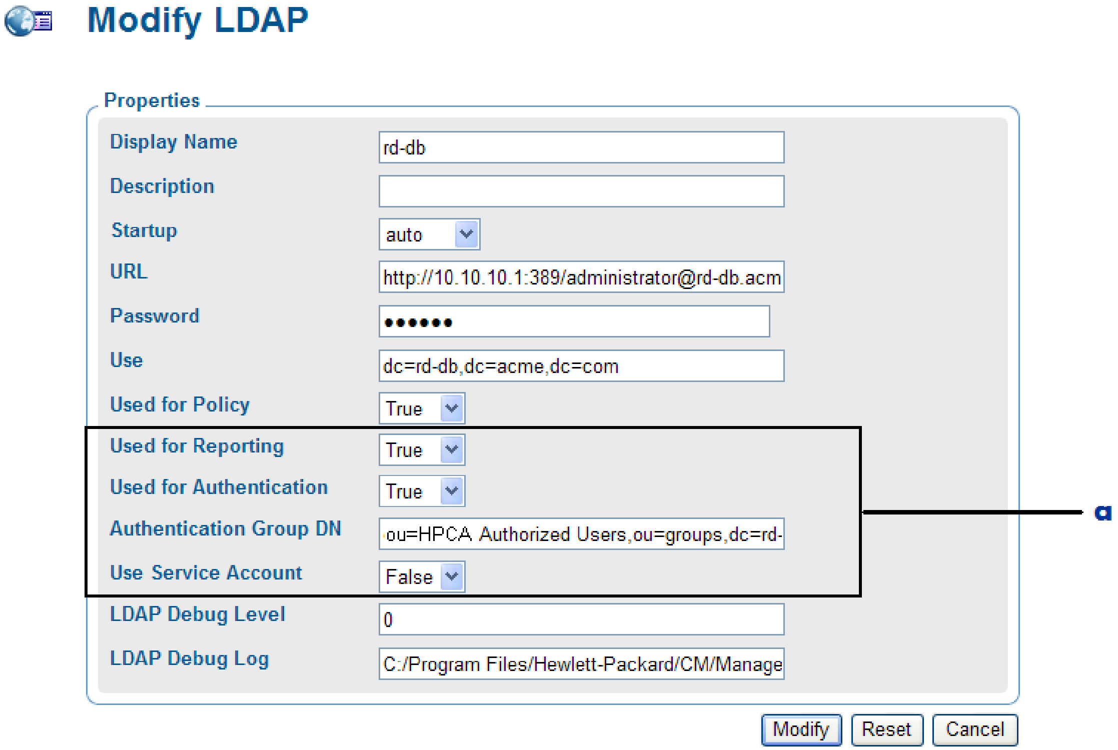
6 To save the property changes, click **Modify**. The Directory Service Properties page opens and displays the modified properties.

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

Modify LDAP Directory Service Options (for Web Services External Authentication and Filtering)

Enhancements to the Portal Web Services allow for an LDAP Directory Service, defined in the Portal, to be used by the Reporting Server for filtering and external user authentication, and by other products, such as the Enterprise Manager, as a user authentication source for login as well as a credential source for read/write operations. The settings inside the Portal that enable these features are shown below on the Modify LDAP page.

Figure 14 Modify LDAP Page Includes External Web Services Fields



Modify LDAP

Properties

Display Name	rd-db
Description	
Startup	auto
URL	http://10.10.10.1:389/administrator@rd-db.acm
Password	••••••
Use	dc=rd-db,dc=acme,dc=com
Used for Policy	True
Used for Reporting	True
Used for Authentication	True
Authentication Group DN	ou=HPCA Authorized Users,ou=groups,dc=rd-
Use Service Account	False
LDAP Debug Level	0
LDAP Debug Log	C:/Program Files/Hewlett-Packard/CM/Manage

Legend

a These fields specify external uses of this LDAP directory, offered through Portal Web Services

After adding an LDAP Directory Service to the Portal, navigate to the Directory Service object and use the **Modify** task to set the following options that relate to these new Portal Web Service features:

- **Used for Reporting --** Select True or False. Default is True. When set to True, this directory service is accessible from the Reporting Server and can be browsed and used for filtering reports. The Reporting Server must be configured to use the Portal as its directory source for this feature to work.
- **Used for Authentication --** Select True or False. Default is True. When enabled, this directory service becomes enabled as an authentication source when authenticating using Web Services. When set to true, users can login to the Enterprise Manager or Reporting Server using their external directory service account credentials.

  This field does not affect users when they login to the Portal directly; it only applies when users login to another HP Client Automation product UI that makes uses of the Portal web services.

- **Authentication Group DN** – Enter a Group DN source for user authentication when authenticating using Web Services, such as: ou=Authorized Users,ou=groups,dc=rd-db,dc=hp,dc=com. When **Used for Authentication** is set to True, the Authentication Group DN is used as the source for authorizing users via the Portal Webs Services. For example, any user that is a member of this group will be authorized to log into a console such as the Enterprise Manager Console or Reporting Server.
- **Use Service Account –** Set to True or False. Default is False. This field does not affect users when they login using the Portal UI. When enabled and a user is logged into the Enteprise Manager using external account credentials, all read/write operations to this directory source will use the service account credentials as defined in the URL and Password fields for this LDAP Object. (All users have the same access – which is the service account access.) When disabled, read/write operations to this directory source will use the logged on user credentials. (Users only see and are able to modify the objects in the directory service to which they are entitled.)

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 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 a Configuration Server Service connection from its Device location in your Zone Directory, use the procedure starting on page 133. 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 111 or Modifying Directory Service Properties on page 128.

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.

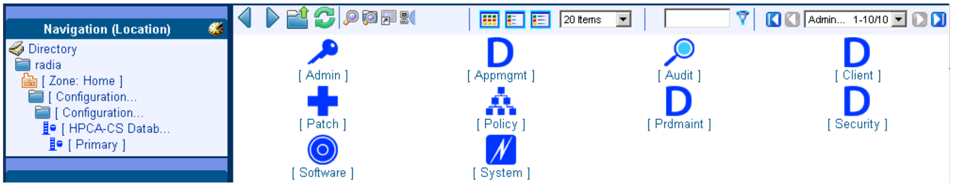
The directory service connection starts immediately. The workspace displays the objects at the mount point of the directory. The mount point is defined by the USE value of the Directory Services properties.

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 12 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 Configuration Server	Zone → Configuration→ Configuration Server → Configuration Server Database → Configuration Server Database object → Primary object
Network mount point	Zone → Networks container
DSML (Subordinate Zone)	Zone → Zone Access Points container
Metakit directory service (Advanced User)	Defined by Template

The next figure shows a sample connection to a Configuration Server DB 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 Configuration Server DB 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 a Configuration Server whose service has not been added as a Directory Service to the Zone Configuration container, a message opens asking whether you want to add and connect to the new directory service.

— Click **Add** to first add the Configuration Server 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 Configuration Server directory whenever the Portal Zone starts up. If this is the first Configuration Server being added to the Zone, the Common Name will default to primary. If a primary Configuration Server exists in this zone, the Common Name will default to rcs1. For details on adding the Configuration Server as a Directory Service, see Specifying Configuration Server Database Directory Service Properties on page 120.

— Click **Connect** to connect to the Configuration Server 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 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 a Configuration Server Service from its Service Properties page within the Device container, use the procedure To stop a service defined for a Device on page 135.

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 Portal. The LDAP_AUTH parameters specify:

- the default external authentication setting for all users of the 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 Portal 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 73. To disable LDAP authentication for individual users, see Modifying the Default LDAP Authentication for Specific Users on page 137.

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 Portal

1. Stop the HPCA Portal service (httpd-managementportal).
2. Use a text editor to open the Portal configuration file, `rmp.cfg`, located by default in *SystemDrive*`:\Program Files\Hewlett-Packard\CM\ManagementPortal\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::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 137.

4 Use one or more spaces to separate the parameter and its value. See Table 13 below for details.

Table 13 rmp.cfg parameters for external LDAP authentication

Parameter and Value	Definition and Examples

`LDAP_AUTH 1`
or
`LDAP_AUTH 0`
	Sets the default value of external authentication for all users logging onto the Portal. Use the External Authentication? field on the Person properties page to override the default value for any user.
	• Set to **1** to enable external LDAP authentication, by default, for all users.
	• Set to **0** to disable external authentication, by default, for all users.
	• If unspecified, LDAP_AUTH is set to **0**.

`LDAP_AUTH_DN <<`*`user`*`>>@<`*`mydomain`*`.com>`	Defines the domain that a user will bind to. Replace *`mydomain.com`* with the domain that users will bind to. The `<<user>>` portion will be substituted with the value entered on the login page.
	`LDAP_AUTH_DN <<user>>@`*`mydomain.com`*
	`LDAP_AUTH_DN <<user>>@domainA.com`

LDAP_AUTH_HOST hostname:389	The hostname and port of the LDAP server. Where "myldaphostname" is the hostname of the LDAP server.

5 Save and close the file.

6 Restart the HPCA Portal service (httpd-managementportal) and open the Portal.

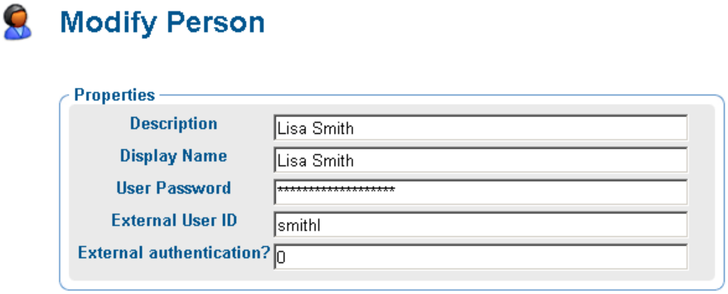
Modifying the Default LDAP Authentication for Specific Users

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 199 and Modifying Users on page 201.

Figure 15 Modify Person dialog box



Modify Person

Properties

Description: Lisa Smith

Display Name: Lisa Smith

User Password: ********************

External User ID: smithl

External authentication?: 0

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 Portal.

Configuring for a Custom LDAP Policy Extension Prefix

Many 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 Portal. This procedure adds a PREFIX parameter to the `rmp.cfg` file where you specify a policy prefix value other than edm.

See the *Policy Server Guide* for more information on configuring the Policy Server and the LDAP Policy Extension.

To configure the Portal for a Custom LDAP Policy Prefix (other than edm)

1 Stop the HPCA Portal service (httpd-managementportal).

2 Use a text editor to open the Portal configuration file, `rmp.cfg`, located by default in `*SystemDrive*:\Program Files\Hewlett-Packard\CM\ManagementPortal\etc`.

3 Insert the PREFIX parameter (must be uppercase) into this file before the finishing curly bracket (}) as shown in the code sample here.

```
#
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 Policy Server.

Table 14 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.

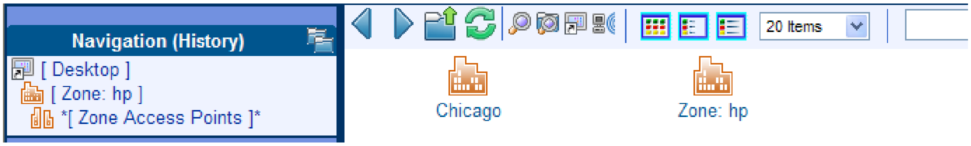
6 Restart the lHPCA Portal service (httpd-managementportal) and open the Portal.

Configuring Zone Access Points

Access Points to other Portal Zones in your enterprise are automatically configured whenever you install multiple portal zones using the Install Subordinate Portal task.

To access another zone in your Client Automation infrastructure, go to the Zone Access Points container, and click on the icon for the Zone you want to view.

Figure 16 Zone Access Points container



Establishing Devices and Device Groups

There are threeways to bring devices under the control of a Portal Zone.

- First, 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 a Portal Zone below.

  ➤ You can perform the install tasks in the Operations task group directly from a discovered Network or LDAP directory. The Portal will add the selected computers to the Devices container of the Zone automatically, and create links between the Network or LDAP directory location and the Zone Device location.

- Second, create Groups to facilitate operations on the members of the groups. Topics related to Adding Groups of Devices begin on page 160.
- Third, install the Portal Agent on devices. By installing the Portal Agent on devices, they automatically become members of the appropriate Device Categories container groups, which is an advantage when you need to Notify all devices with specific operating, software, or hardware configurations. See Installing the Portal Agent on page 252.

Adding Devices to a Portal Zone

There are various ways to add devices to your Portal Zone. Table 15 on page 141 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 15 Methods to Add Computers to a Zone Devices Container

Method	Description and Reference
Network Selection	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 before the install task is performed. A link is created between the Network location and Portal Zone location of each device. or Browse to computers in your Networks container and select **Manage Computer** from the Operations task group. See Managing Computers in Your Portal Zone on page 230.
Active Directory Selection	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 Portal Zone location of each device. or Browse to a computer in your LDAP directory and select the **Manage Computer** task in the Operations task group. See Managing Computers in Your Portal Zone on page 230.
Hostname List	Prepare a list of hostnames and use the Import Devices task. See Importing Devices on page 168.
Individual Entry	Browse to a group in the Groups container and click **Add Device** from the Model Administration task group. See Adding a Single Device on page 156.
Installed Portal Agent	Any computer that has the Portal Agent 5.00 installed on it will automatically be added to the Device container when it contacts the Portal.

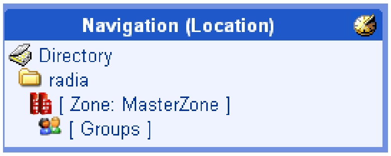
Several tasks used to bring devices under control of the Portal employ a common browse and select window. Before continuing, we recommend you know how to use the window's features. See Basic Procedures for Modifying Groups on page 142.

Basic Procedures for Modifying Groups

Many tasks in the 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.

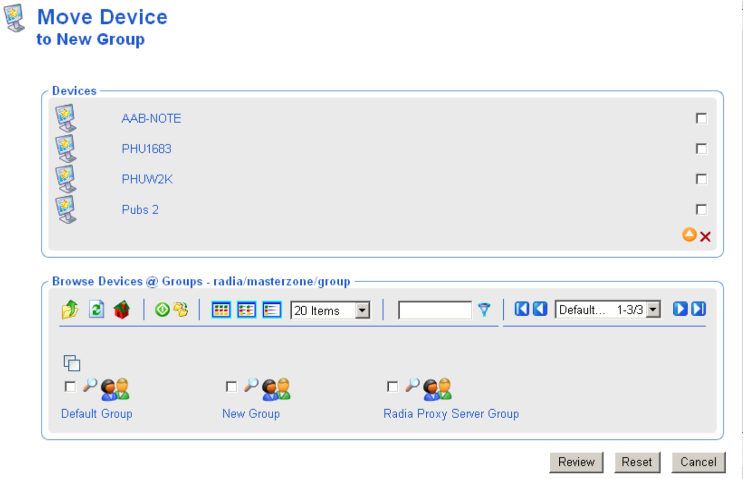
Task 1 Navigate to the target group and click the appropriate Portal task.



Navigation (Location)

Directory
radia
[Zone: MasterZone]
[Groups]

Task 2 Change the items in the group.



Move Device
to New Group

Devices

AAB-NOTE	□
PHU1683	□
PHUW2K	□
Pubs 2	□

Browse Devices @ Groups - radia/masterzone/group

20 Items · Default... 1-3/3

□ Default Group · □ New Group · □ Radia Proxy Server Group

Review · Reset · Cancel

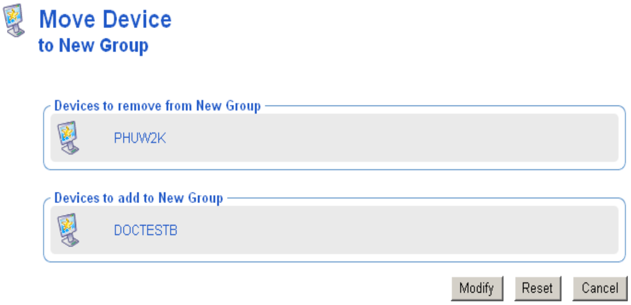
Task 3 Modify/Commit/Review changes.

Modify

or

Review

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



Move Device to New Group

Devices to remove from New Group

PHUW2K

Devices to add to New Group

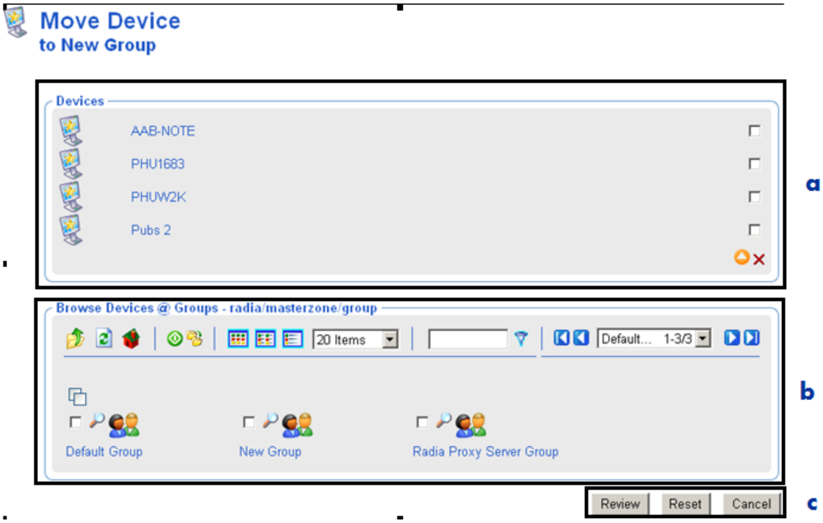
DOCTESTB

Using the Browse and Modify Window

Figure 17 on page 144 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.

This figure shows 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 17 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 145.

  When working with Client Automation 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 147 for more information.

  When working with Client Automation 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 150 for more information.

- **Browse area**
  The bottom area allows you to browse your 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 153.
- **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.

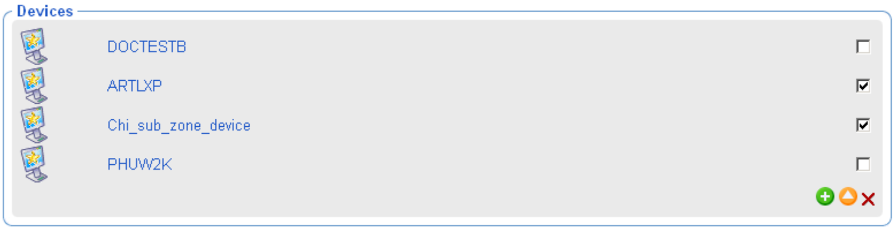
Using the Group List Area

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.



Devices

DOCTESTB	□
ARTLXP	☑
Chi_sub_zone_device	☑
PHUW2K	□

2 Click ✕ to delete the items from the list.

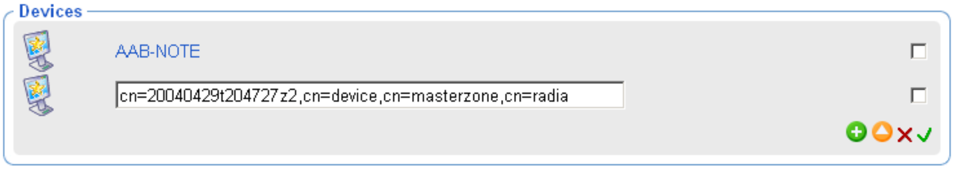
3 Click the **Modify** or **Commit** button below the Browse group area to save the modified list.

> 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.



Devices

AAB-NOTE □

cn=20040429t204727z2,cn=device,cn=masterzone,cn=radia □

⊕ ⬆ ✕ ✓

3 In the text box, modify the X500 Distinguished Name for the item.

4 Click ✓ to accept the changes.

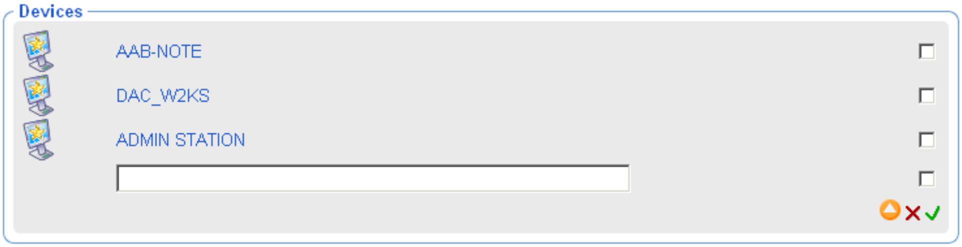
5 Click **Modify** at the bottom of the page to save the modified list.

> 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.



Devices

AAB-NOTE □

DAC_W2KS □

ADMIN STATION □

□

⬆ ✕ ✓

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.

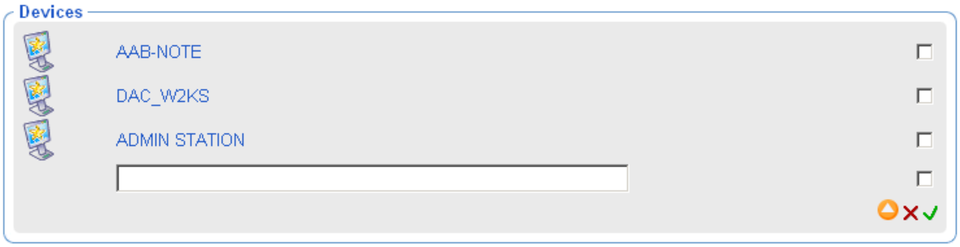
2 In the text-box, type the X500 Distinguished Name for the object to be added. For example, the X500 Distinguished Name for the Default Group of devices is:

```
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.

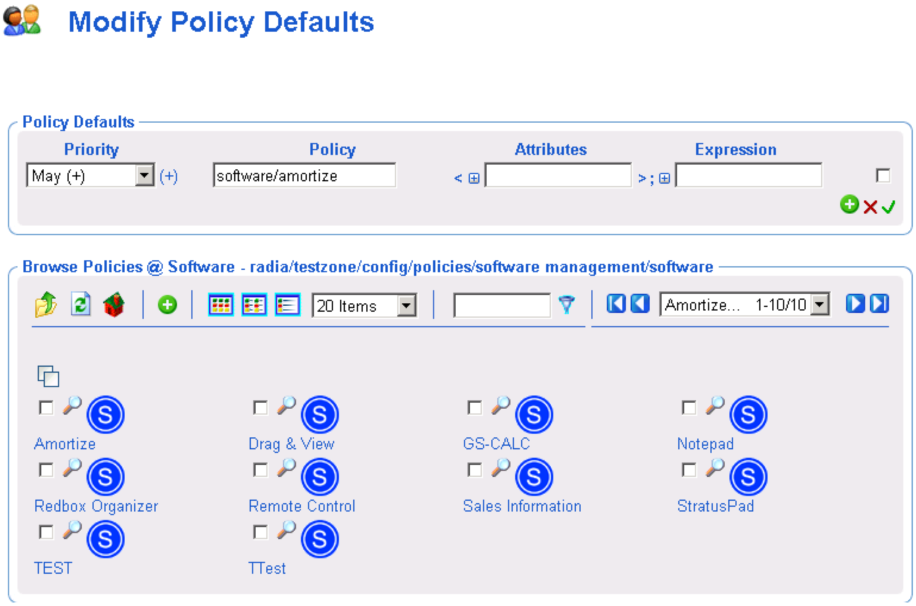
Using the Attribute Editor

After selecting a service in the Browse and Modify window, use the Attribute Editor to specify values for the attributes for Client Automation services. The values that you are specifying are for policy (see Modifying Policies on page 88), defaults (see Modifying Policy Defaults on page 97) or overrides (see Modifying Policy Overrides on page 98).

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

Policy Defaults

Priority	Policy	Attributes	Expression
May (+) (+)	software/amortize	< ⊞	> ; ⊞

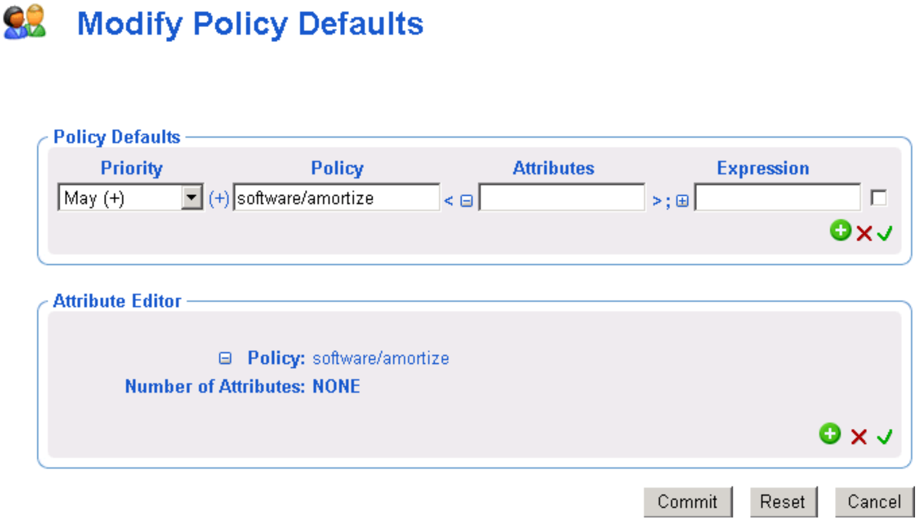
Browse Policies @ Software - radia/testzone/config/policies/software management/software

20 Items

Amortize... 1-10/10

2 Click the ⊞ to the left of the Attributes text box.

The Attributes Editor area opens.



Modify Policy Defaults

Policy Defaults

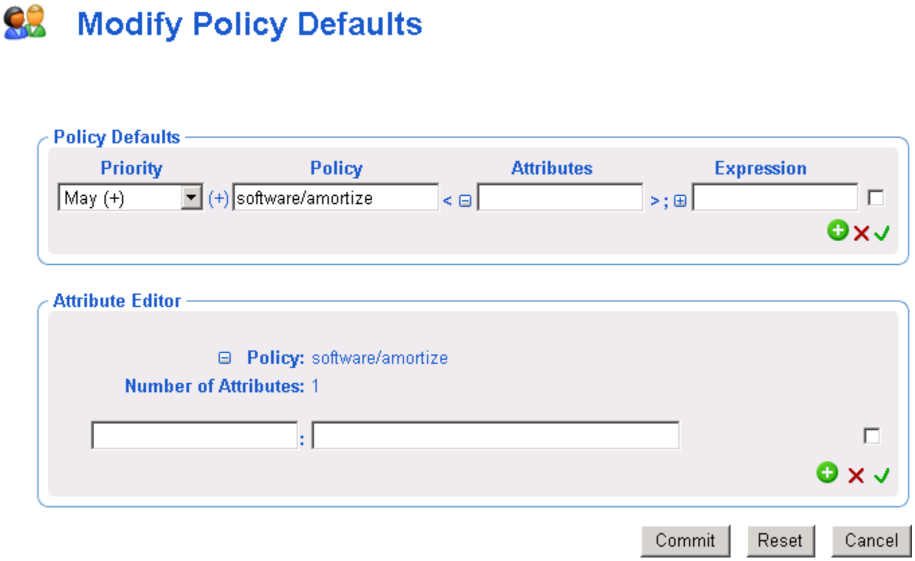
Priority	Policy	Attributes	Expression
May (+) (+)	software/amortize	< ⊟	> ; ⊞

Attribute Editor

⊟ **Policy:** software/amortize

Number of Attributes: NONE

3 In the Attribute Editor area, click ⊕ to add a new attribute.



Modify Policy Defaults

Policy Defaults

Priority		Policy		Attributes		Expression	
May (+)	(+)	software/amortize	< ⊟		> ; ⊞		□

Attribute Editor

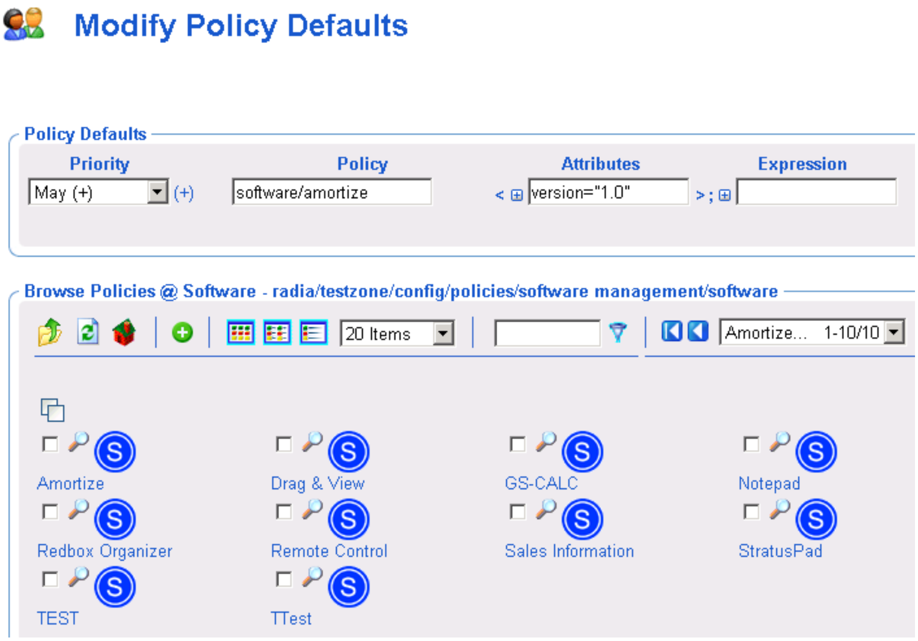
⊟ **Policy:** software/amortize

Number of Attributes: 1

4 In the text box on the left, type the name of the attribute to be added, such as version. You can specify any attribute that is available for the service.

5 In the text box on the right, type the value for the attribute, such as 1.0.

6 Click ✓ to accept the changes to the attribute.



Modify Policy Defaults

Policy Defaults

Priority	Policy	Attributes	Expression
May (+) (+)	software/amortize	< ⊞ version="1.0" >; ⊞	

Browse Policies @ Software - radia/testzone/config/policies/software management/software

20 Items

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 88), defaults (see Modifying Policy Defaults on page 97) or overrides (see Modifying Policy Overrides on page 98).

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 147), this service will only be deployed to machines with a Windows NT operating system.

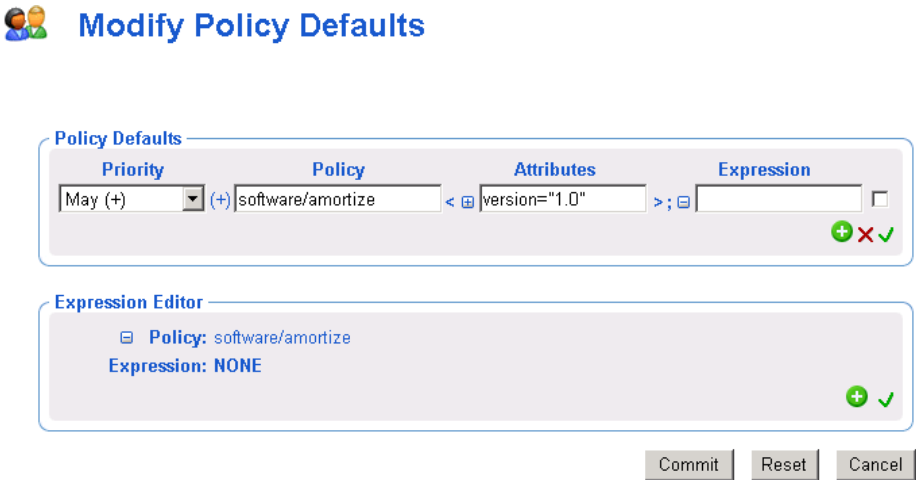
To use the Expression Editor

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

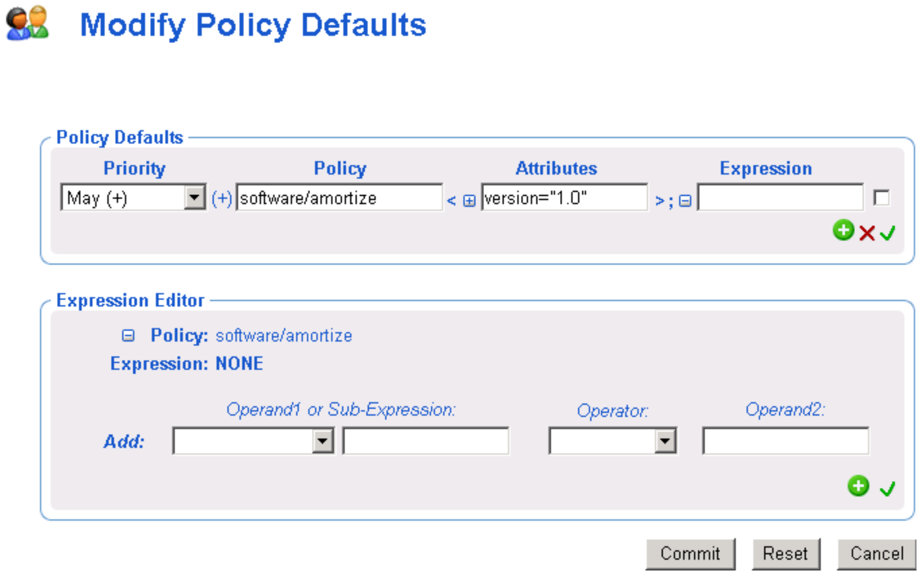
Priority	Policy	Attributes	Expression
May (+)	(+) software/amortize	< ⊞ version="1.0"	>; ⊟ □

Expression Editor

⊟ Policy: software/amortize

Expression: NONE

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



Modify Policy Defaults

Policy Defaults

Priority	Policy	Attributes	Expression
May (+)	(+) software/amortize	< ⊞ version="1.0"	>; ⊟ □

Expression Editor

⊟ Policy: software/amortize

Expression: NONE

	Operand1 or Sub-Expression:		Operator:	Operand2:
Add:				

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 predefined 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 *HP Configuration Managment Application Manager Installation and Configuration Guide* for more information about this attribute.

Each of these options represents substitution of attributes that were supplied as input during policy resolution. See the *Policy Server Guide* for more information.

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

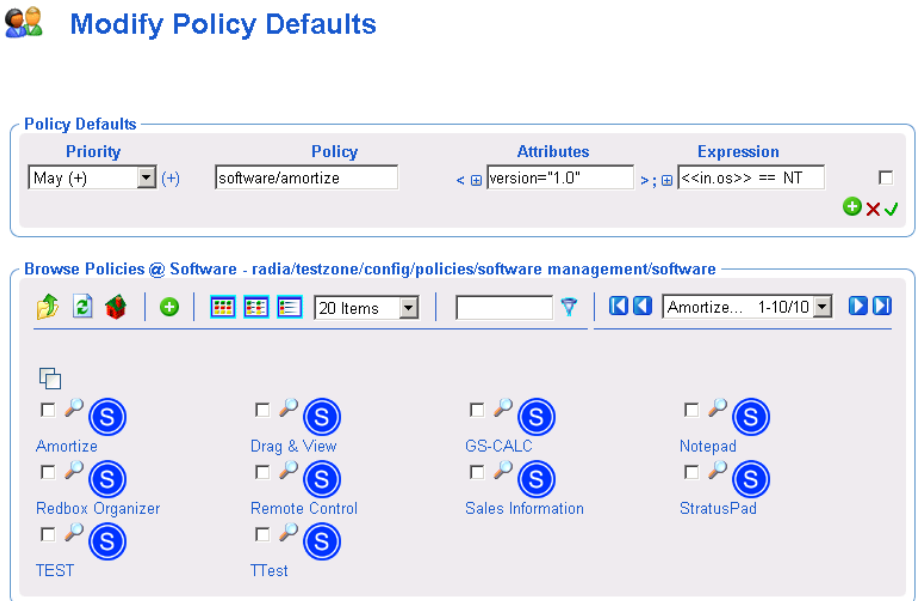
Table 16 Operators

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.

Expression	Meaning
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

Policy Defaults

Priority	Policy	Attributes	Expression
May (+)	software/amortize	version="1.0"	<<in.os>> == NT

Browse Policies @ Software - radia/testzone/config/policies/software management/software

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.

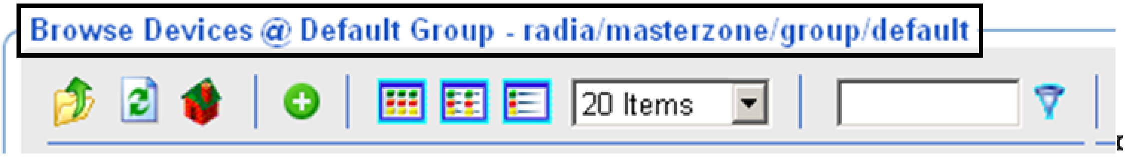
- Use this topic to become familiar with the browse area toolbar icons and how to use the browse area.
- To become familiar with browsing, selecting and adding items from the browse area to the group list area, we recommend you follow the step-by-step procedures in Moving Devices into a Group on page 156.

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 Zone named MasterZone.

Figure 18 Browse area label identifies current navigation location


Browse Devices @ Default Group - radia/masterzone/group/default
20 Items

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

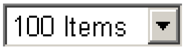
- Click ▦ to show the potential targets with large icons.

- 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:



100 Items

- 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 Portal Zone.

Before proceeding, you should be familiar with the use of the Browse and Select Windows. See Basic Procedures for Modifying Groups on page 142.

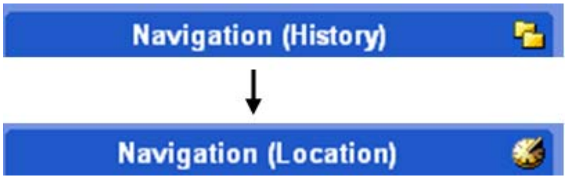
Adding a Single Device

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.

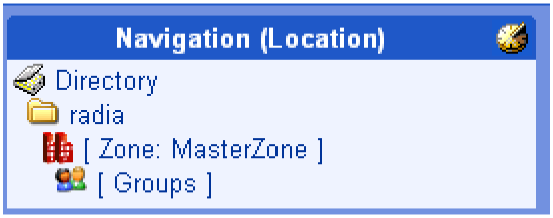
If you want to have this device added to a new group, first create the group using the procedure To add a Group of devices on page 160, and then use the **Add Device** task, below.

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.

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 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**.

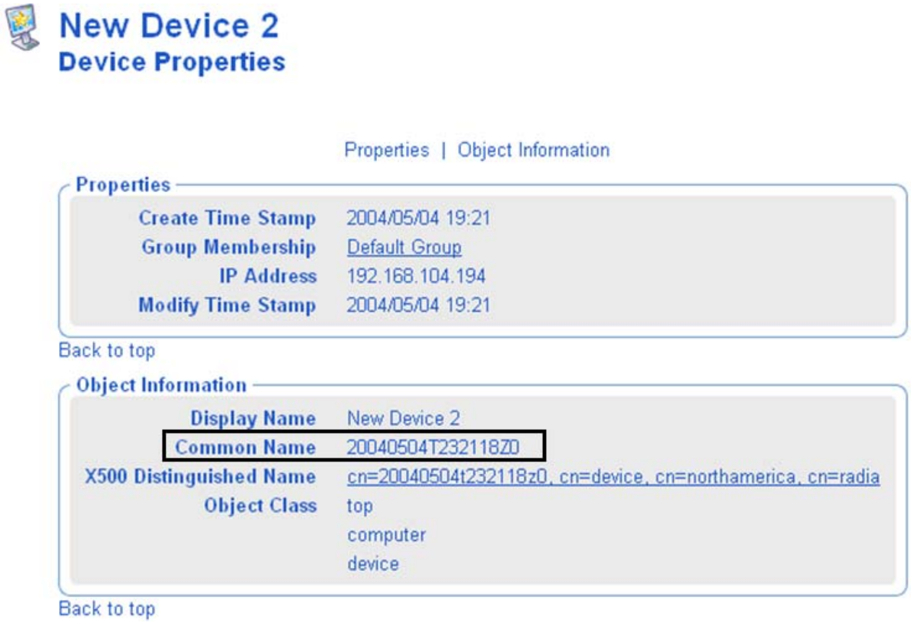
The Portal adds the device to the Devices container.

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

Figure 19 Sample Common Name generated for a device



New Device 2

Device Properties

Properties | 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	20040504T232118Z0
X500 Distinguished Name	cn=20040504t232118z0, cn=device, cn=northamerica, cn=radia
Object Class	top computer device

Back to top

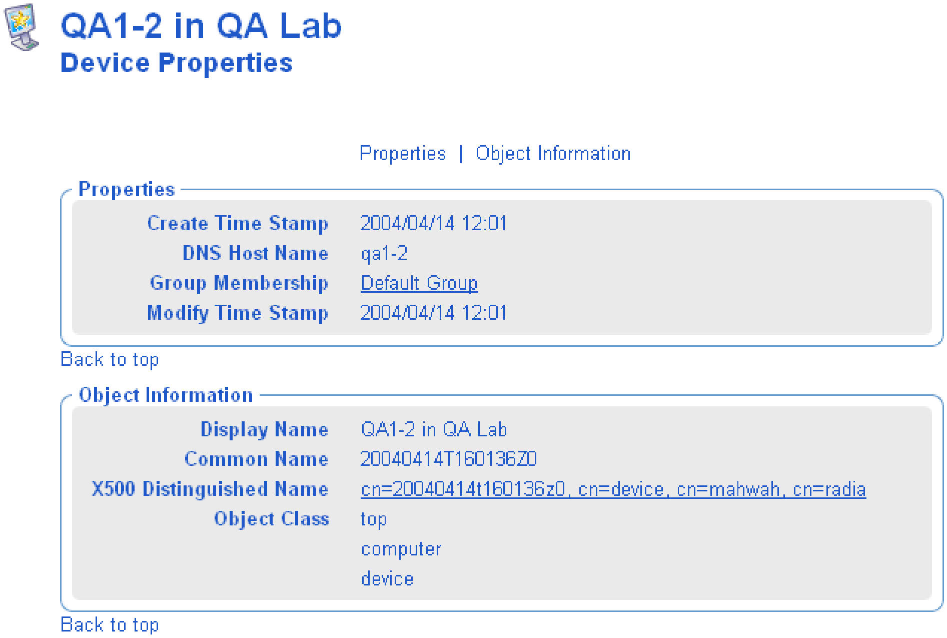
Viewing Device Properties

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 20 below shows the Device Properties for a new device when no Portal Agent is installed.

Figure 20 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

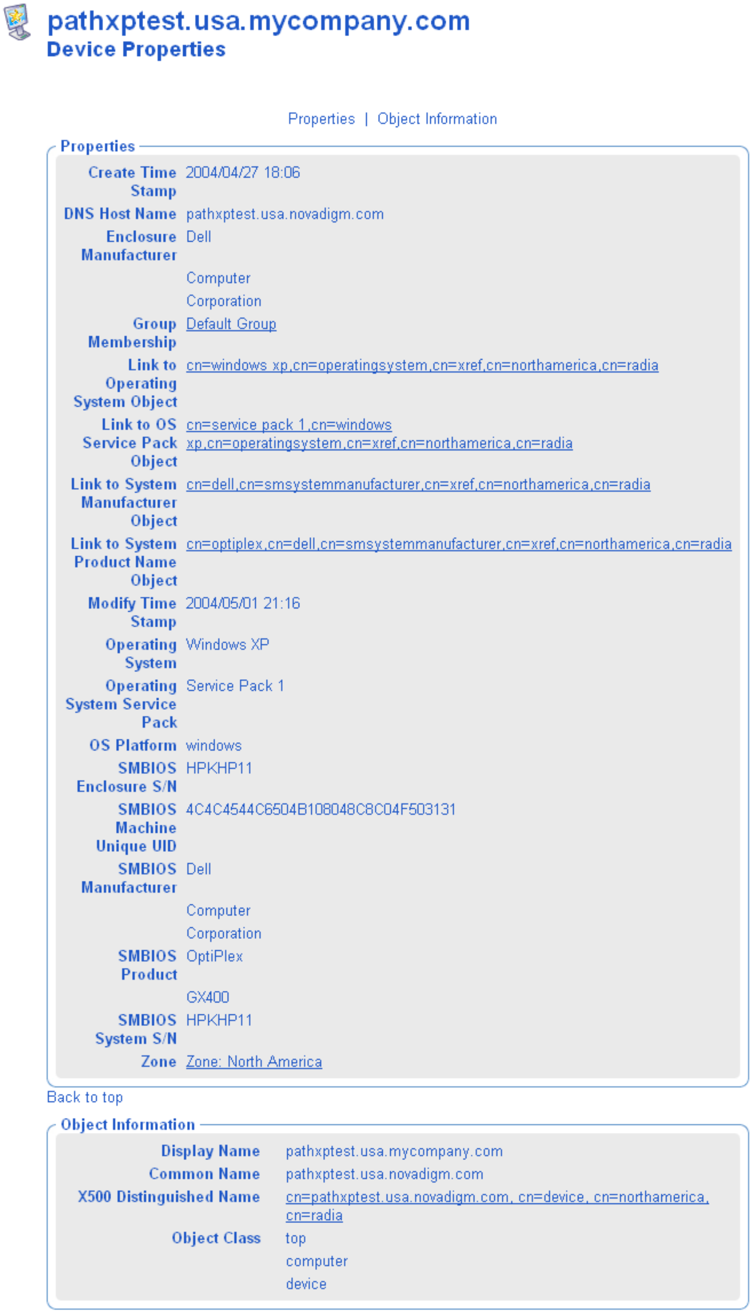
Display Name	QA1-2 in QA Lab
Common Name	20040414T160136Z0
X500 Distinguished Name	cn=20040414t160136z0, cn=device, cn=mahwah, cn=radia
Object Class	top computer device

Back to top

After a Portal Agent is installed on a Device, the next figure. The Portal uses this information to create memberships for the device in the appropriate Device Categories 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 21 Device Properties after installing the Portal Agent



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 161.
- 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 168.

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.

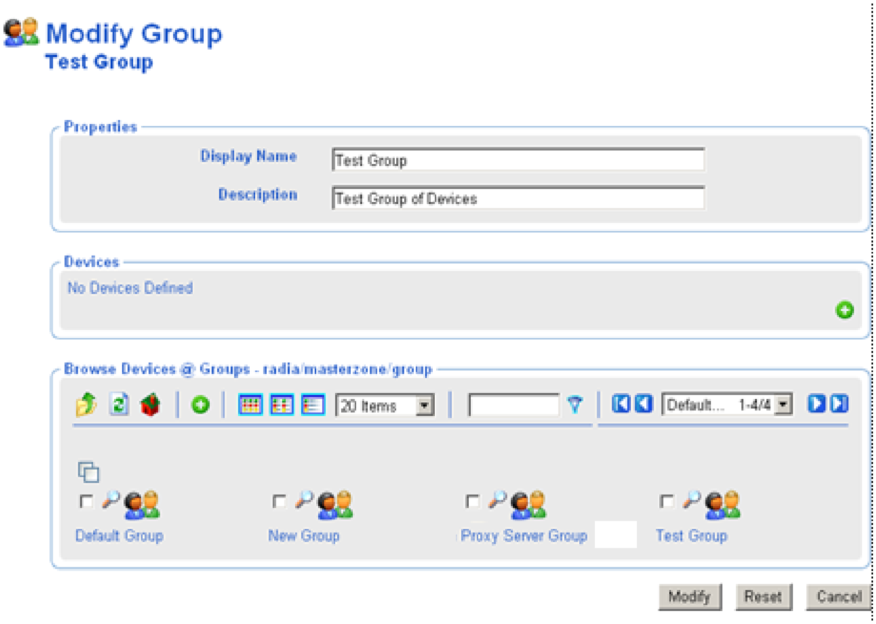
     > The Common Name for the object must be unique. If you attempt to create an object with a name that has already been used, an error appears in the workspace indicating that the object already exists.

   - 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

Properties

Display Name: Test Group

Description: Test Group of Devices

Devices

No Devices Defined

Browse Devices @ Groups - radia/masterzone/group

6 To save the group, click **Modify**.

The task ends, and the Navigation aid indicates the new group location in the Groups container. There will not 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 **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**.

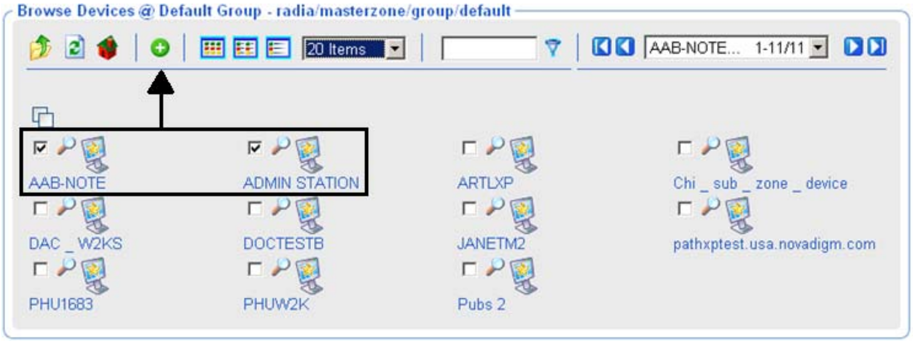
   The Modify Group dialog box opens. It shows:
   - Properties previously entered.
   - No devices defined in the group list.
   - Browse area containing current Groups in the zone.

   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.

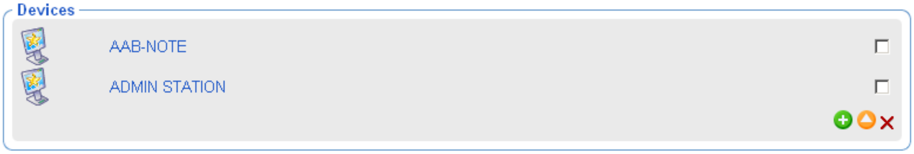
   Typically, there will be a large number of devices in the Default Group, since all devices are automatically added to this group unless specified otherwise.

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

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

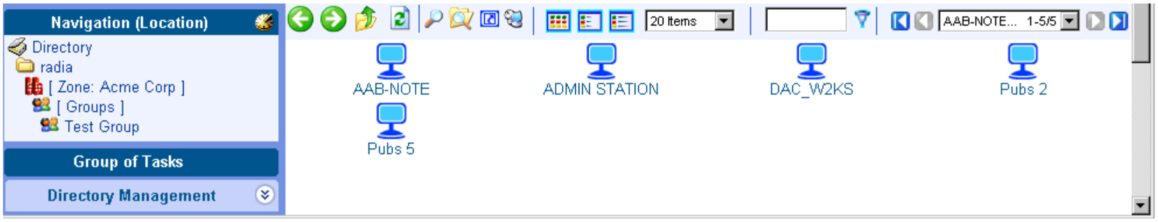

Browse Devices @ Default Group - radia/masterzone/group/default
20 Items
AAB-NOTE... 1-11/11
☑ AAB-NOTE
☑ ADMIN STATION
□ ARTLXP
□ Chi _ sub _ zone _ device
□ DAC _ W2KS
□ DOCTESTB
□ JANETM2
□ pathxptest.usa.novadigm.com
□ PHU1683
□ PHUW2K
□ Pubs 2

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 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.

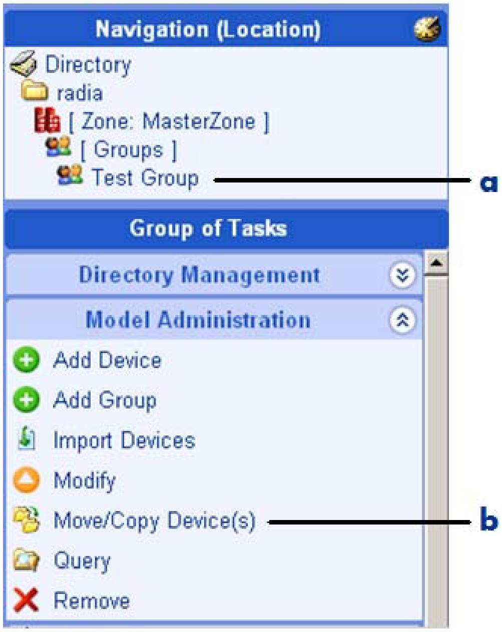
To create a new group for devices, see Adding User Groups on page 161.

To remove devices from a group, see the procedure To remove devices from a Group on page 166.

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 142.

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 Device Categories 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 168, 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.

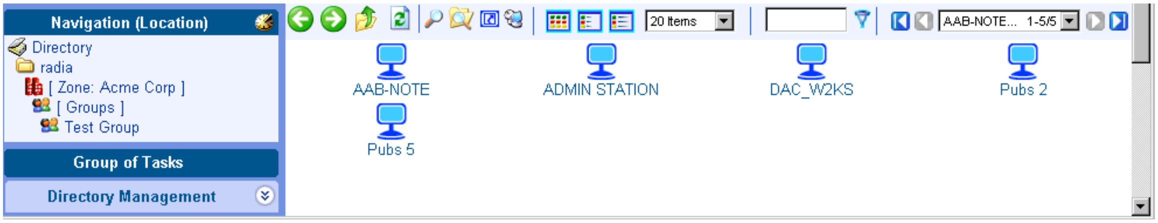
5 If necessary, repeat the browse and move steps until all devices and groups are listed in the Devices area.

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.

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.



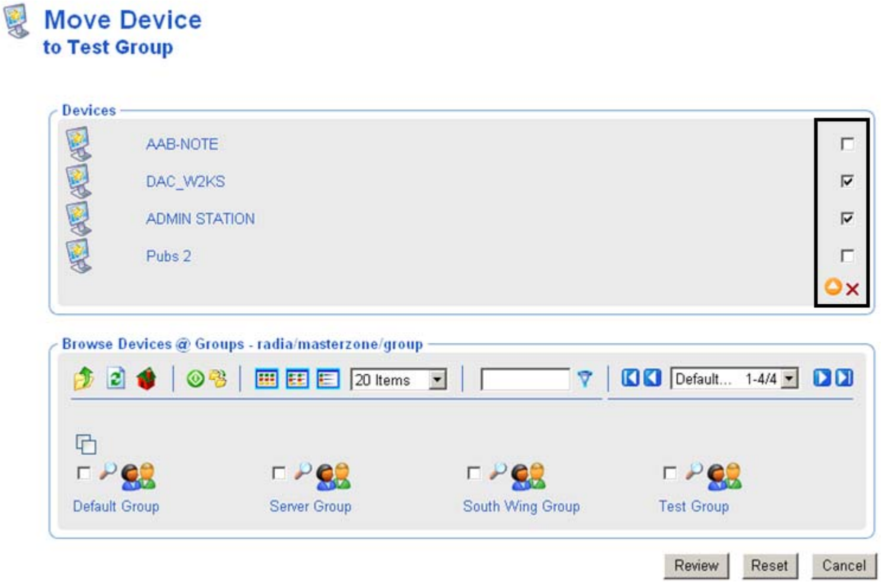
To remove devices from a Group

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

Devices

AAB-NOTE	□
DAC_W2KS	☑
ADMIN STATION	☑
Pubs 2	□

Browse Devices @ Groups - radia/masterzone/group

20 Items

Default... 1-4/4

□ Default Group
□ Server Group
□ South Wing Group
□ Test Group

4 After selecting the devices to be deleted, click ✕ to delete the checked items.

5 Click **Review** to review the changes.

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

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 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.
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 Portal Directory.

   or

   Click ✗ to indicate that you do not want to remove the group and its group members. The remove is cancelled; none of the groups or memberships is removed.

Importing Devices

Use the Import 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 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 using ASCII characters, only; non-ASCII characters are not supported.

> 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 169, 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 Portal location. By default, this location is:

```
SystemDrive:\Program Files\Hewlett-
Packard\CM\ManagementPortal\etc\group
```

2 From the 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 160.

> 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.

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. An Import Devices dialog box opens.

  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 Portal installation directory. The Import Devices dialog box opens.

  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 163.
- To move some of the devices into a new group, see Adding Devices to a New Group on page 161.

Dynamic Job Scheduling Against Groups of Devices

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

- Install Client Automation Agent
- Install Portal 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.

You can use this dynamic feature to notify a series of devices, for example, with minimal effort. You can create a group of devices and schedule a daily Notify for it. 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 Portal Agent is installed on the Device to manually enable a connection to the service, or to enable the 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 Portal Agent has been installed on a Device, its Client Automation-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.
2. In the Model Administration task group, click **Add Service**.

   The Add Service dialog box opens.
3. 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 **Configuration Server** to add a `ZTOPTASK.EXE` service on a Configuration Server.
- Select **HTTPD** to add a service running under the Integration Server (httpd), such a service for the legacy Proxy Server.

The page refreshes after your selection to display the appropriate fields for the selected service type.

4 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.

5 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 an HPCA Integration Server (httpd) service, such as one used by the legacy Proxy Server.

> The following fields apply to a Service Type of `ds-rcs`, only. If you are adding a different Service Type, skip to Step 12.

8 In the Path text box, type the exact path of `ztoptask.exe` on the Configuration Server machine. Use forward slashes. For example: `C:/Program Files/Hewlett-Packard/CM/ConfigurationServer /bin/ztoptask.exe`.

9 In the User text box, type the Username needed to use to connect to the Configuration Server.

10 In the User Password text box, type the password for the user to connect to the Configuration Server.

11 In the Timeout text box, leave the default value of 0 to never have a Configuration Server connection timeout. To have the Configuration Server 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 Starting a Directory Service on page 134.

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 142.

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.

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 have 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 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.

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 Portal directory.

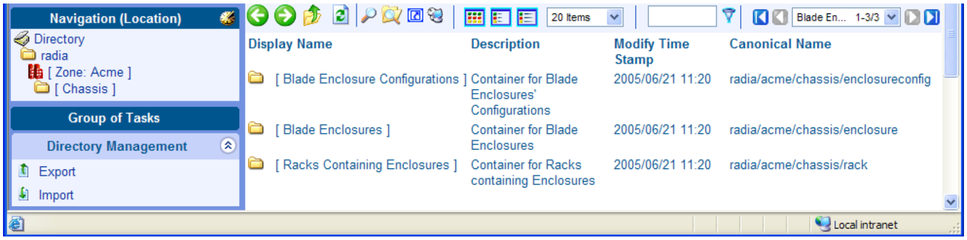
or

Click ✗ to indicate that you do not want to remove the object and its children. The remove is cancelled; none of the objects is removed.

Configuring Blades, Enclosures, and Racks

The Chassis container extends the device-based Client Automation 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 22 Chassis Container Contents



Display Name	Description	Modify Time Stamp	Canonical Name
[Blade Enclosure Configurations]	Container for Blade Enclosures' Configurations	2005/06/21 11:20	radia/acme/chassis/enclosureconfig
[Blade Enclosures]	Container for Blade Enclosures	2005/06/21 11:20	radia/acme/chassis/enclosure
[Racks Containing Enclosures]	Container for Racks containing Enclosures	2005/06/21 11:20	radia/acme/chassis/rack

Table 17 below lists the Chassis container contents and Table 18 on page 175 lists the related Device Categories containers for these objects.

Table 17 Chassis Container Objects

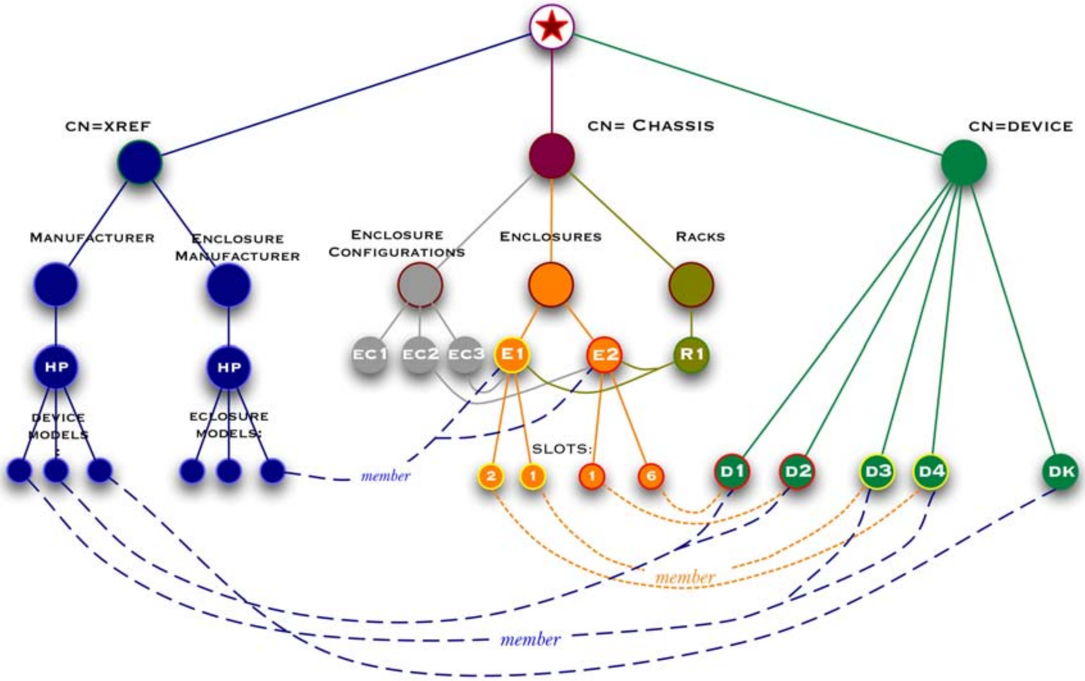
Chassis Container Group	Contents and Notes
Racks Containing Enclosures	Rack instances containing enclosures. • Physical racks IDs must be unique within all racks in a Zone. • Multiple enclosure instances may be linked to a single rack.
Blade Enclosures	Planned or actual enclosure instances. Each instance contains a set of slots. Slots are either *occupied* by a server blade or *empty*. • 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 Device Categories 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	Predefined enclosure configurations (an enclosure model number and a predefined set of slots and server blades). • To add configurations, see the Add Enclosure Configuration task on page 177.

Table 18 Device Categories Groups for Blade Enclosures

Device Categories 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 23 on page 176 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 23 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 Device Categories containers. Device D1 is a member of the HP Device Models listed in the **Device Categories → 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 **Device Categories → 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 described in Table 19 on page 177.

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

Table 19 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 enclosureconfig 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. We recommend 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.

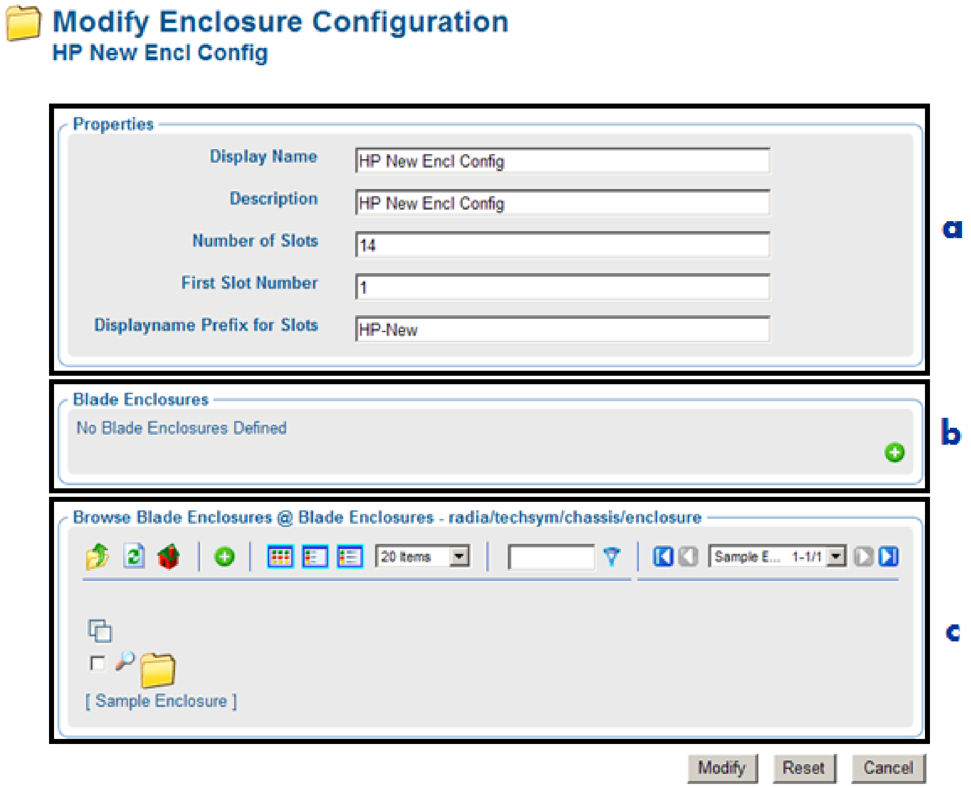
Number of Slots – Defines the number of slots to create for this enclosure configuration.

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]

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.

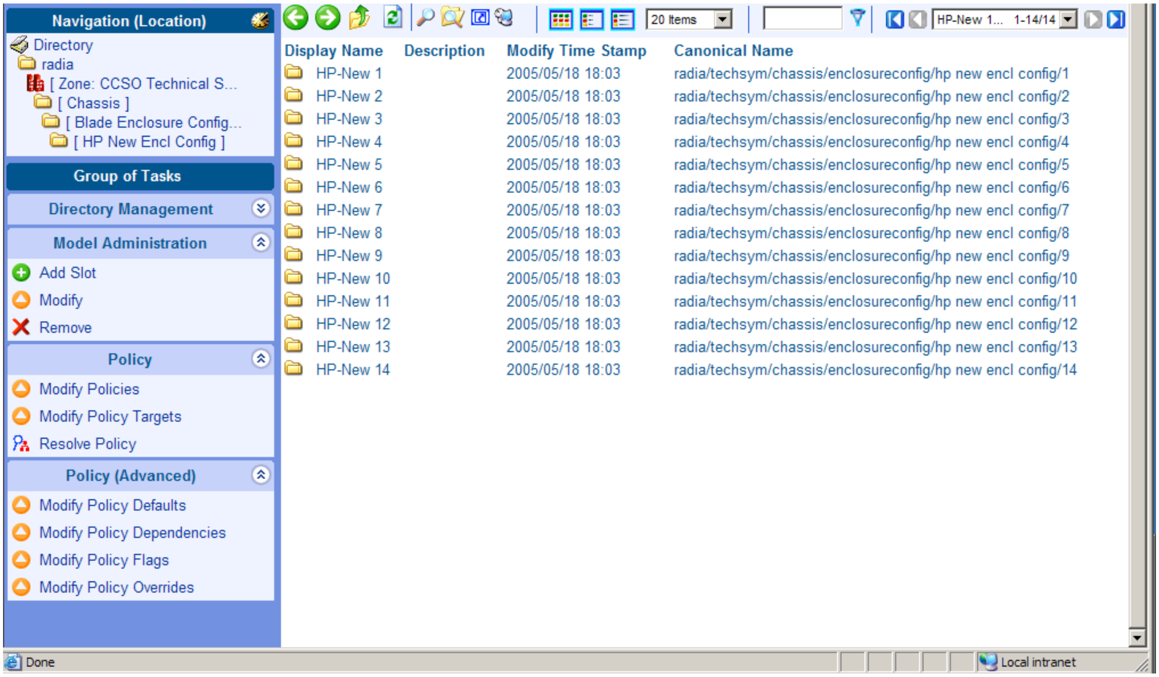
c Browse Blade Enclosures area is used to select blade enclosures to define as members of this configuration.

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 143 for more information on how to use this area.

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

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



Display Name	Description	Modify Time Stamp	Canonical Name
HP-New 1		2005/05/18 18:03	radia/techsym/chassis/enclosureconfig/hp new encl config/1
HP-New 2		2005/05/18 18:03	radia/techsym/chassis/enclosureconfig/hp new encl config/2
HP-New 3		2005/05/18 18:03	radia/techsym/chassis/enclosureconfig/hp new encl config/3
HP-New 4		2005/05/18 18:03	radia/techsym/chassis/enclosureconfig/hp new encl config/4
HP-New 5		2005/05/18 18:03	radia/techsym/chassis/enclosureconfig/hp new encl config/5
HP-New 6		2005/05/18 18:03	radia/techsym/chassis/enclosureconfig/hp new encl config/6
HP-New 7		2005/05/18 18:03	radia/techsym/chassis/enclosureconfig/hp new encl config/7
HP-New 8		2005/05/18 18:03	radia/techsym/chassis/enclosureconfig/hp new encl config/8
HP-New 9		2005/05/18 18:03	radia/techsym/chassis/enclosureconfig/hp new encl config/9
HP-New 10		2005/05/18 18:03	radia/techsym/chassis/enclosureconfig/hp new encl config/10
HP-New 11		2005/05/18 18:03	radia/techsym/chassis/enclosureconfig/hp new encl config/11
HP-New 12		2005/05/18 18:03	radia/techsym/chassis/enclosureconfig/hp new encl config/12
HP-New 13		2005/05/18 18:03	radia/techsym/chassis/enclosureconfig/hp new encl config/13
HP-New 14		2005/05/18 18:03	radia/techsym/chassis/enclosureconfig/hp new encl config/14

8 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 **Device Categories → 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.
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 Device Categories container for Enclosure Manufacturers. Match the name exactly if the manufacturer is already listed in the Device Categories containers.

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

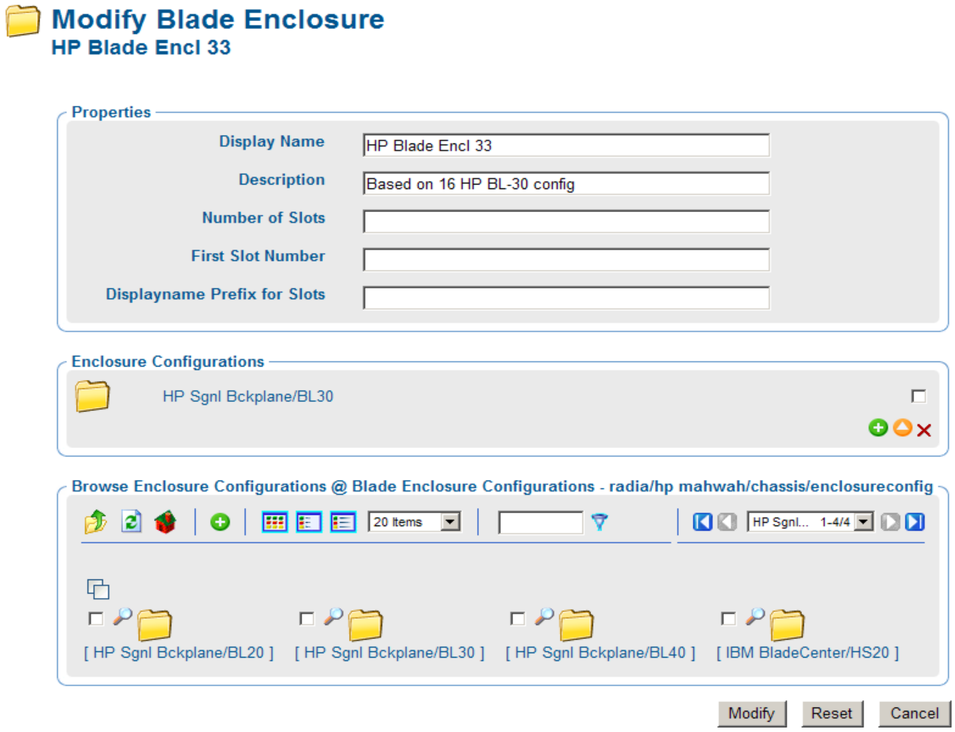
Fist Slot Number – The first slot number of an enclosure is either 1 or 0 (zero). The default value is 1. Enter 0 if this enclosure assigns 0 to the first slot number.

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]

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:

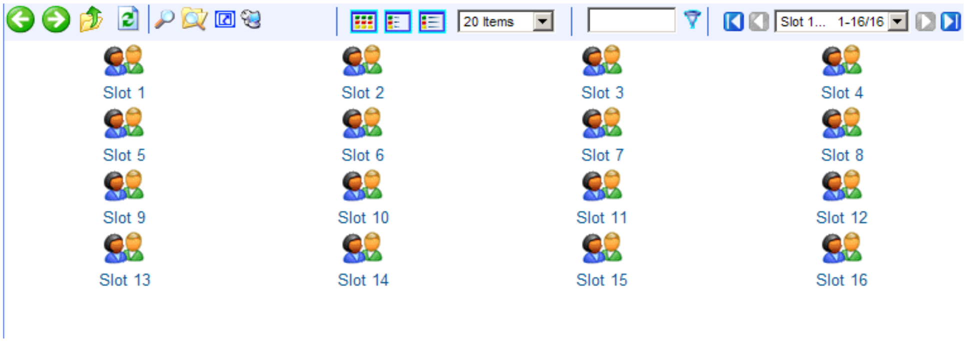
   a. Slot names are automatically generated using the format "Slot n". To add a prefix to these slot names, enter the prefix in the Displayname Prefix for Slots text area.

   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 143 for more information on how to use the Browse area features.

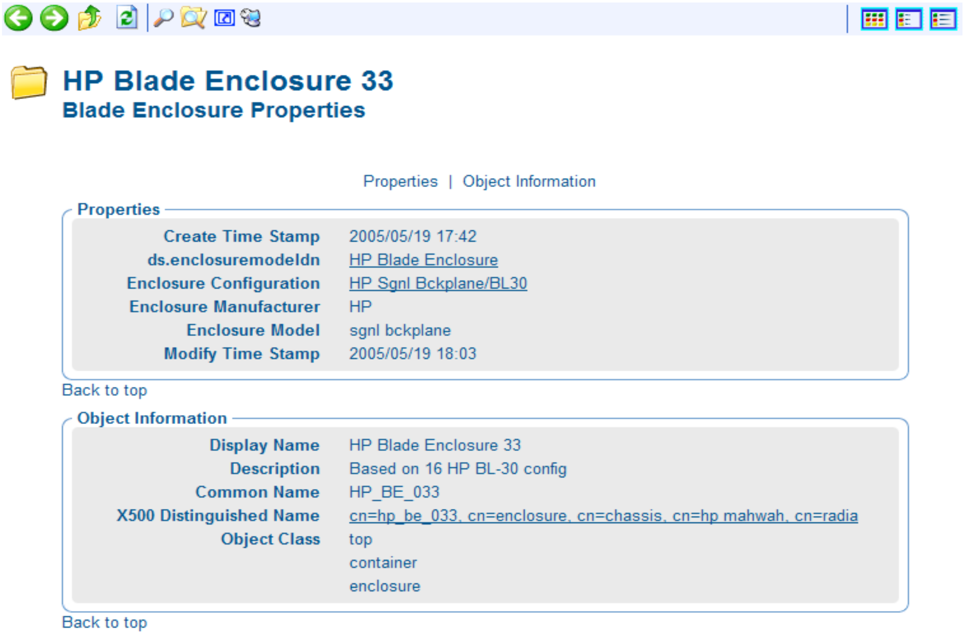
   c. After selecting a configuration from the Browse area, click ⊕ to add it to the Enclosure Configurations area.

8. 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.



9. Click 🔍 on the toolbar to view the Blade Enclosure Properties.



HP Blade Enclosure 33
Blade Enclosure Properties

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

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

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 Portal configuration file, `rmp.cfg`, as discussed in Enabling Policy Configurations for Blades, Enclosures and Racks on page 185.
- 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 the Portal to Assign Policy through an LDAP Directory on page 85.

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 20 below 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 20 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 above.

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 Device Categories 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 185.

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 179 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 56 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.

2 In the Model Administration task group, click **Add Task Group**.

The Add Task Container dialog box opens.

3 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.

4 In the Description text box, type a description that will appear in the Details view.

5 In the Display Name text box, type a name for the task group. If omitted, the Common Name is used.

6 Click **Add**.

The Modify Task Container dialog box opens.

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**.

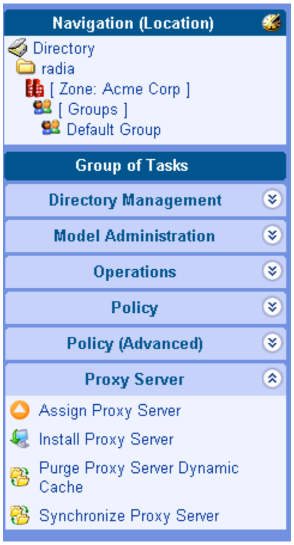
The workspace displays the contents of the new task group.

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

The Task Container Properties for the new task group opens.

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 Portal so that only some administrators can access this task group, see Configuring Delegated Administration on page 189 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.
4. Make any necessary changes. For detailed information about configuring task groups, see Adding Task Groups on page 187 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 Portal Directory.

   or

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

Configuring Delegated Administration

Use the 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 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 Portal operations:

- **Global Default Policy**
  Allows the 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 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 Portal.
- **Test Global Policy**
  Allows you to experiment with entitlement options.

The following roles are used to administer the Configuration Server DB and Policy:

- **Account Administration**
- **Advanced Policy Administration**
- **Auditing Administration**
- **Infrastructure Administration**
- **Package Administration**
- **Policy Administration**
- **HPCA-CS 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.

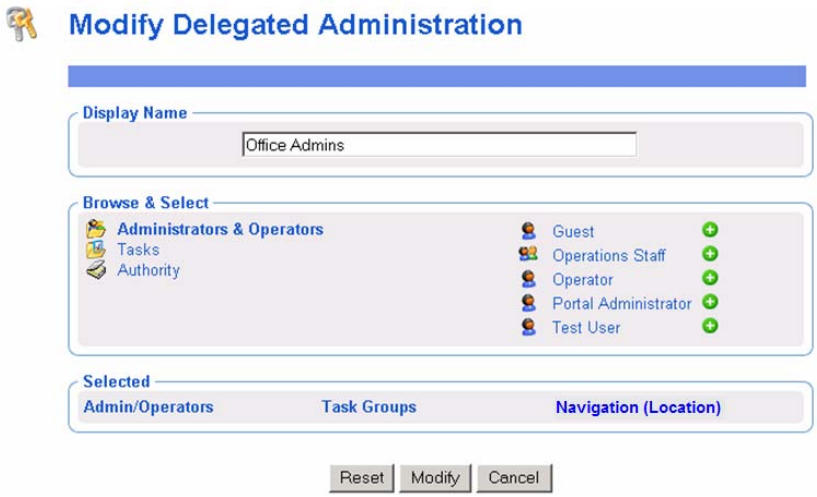
To add a delegated administration role

The figures in this procedure do not reflect the latest changes to the 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.
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

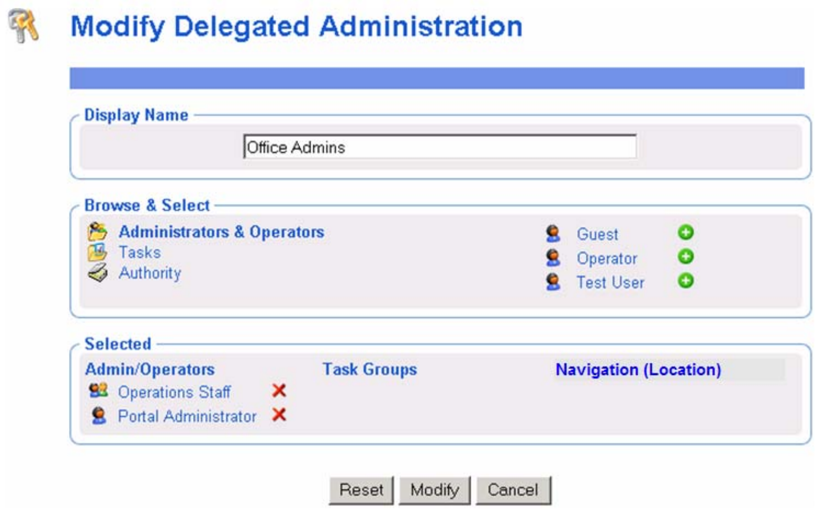
Guest	⊕
Operations Staff	⊕
Operator	⊕
Portal Administrator	⊕
Test User	⊕

Selected

Admin/Operators	Task Groups	Navigation (Location)

6. In the Browse & Select area of the dialog box, make sure that Administrators & Operators is selected. Selected text is bold.
7. Click ⊕ next to the each of the administrators and operators that you want to add.

   Notice that as you select administrators and operators, they appear in the Selected area of the dialog box under the Admin/Operators column.



Modify Delegated Administration

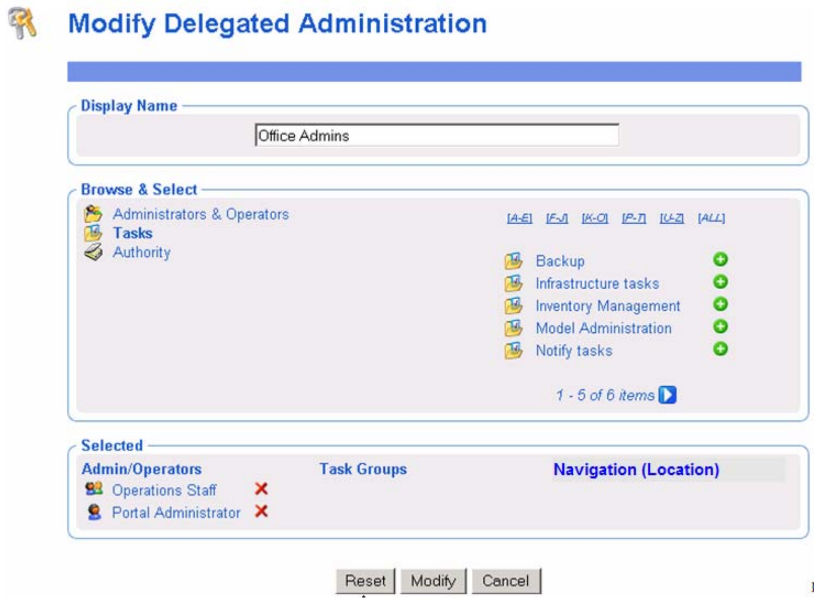
Display Name: Office Admins

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.



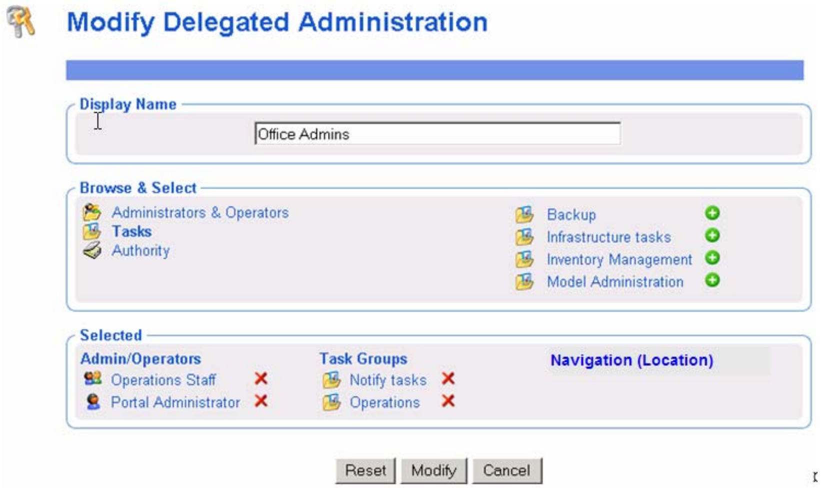
Modify Delegated Administration

Display Name: Office Admins

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: Office Admins

Browse & Select

- Administrators & Operators
- Tasks
- Authority

Backup	⊕
Infrastructure tasks	⊕
Inventory Management	⊕
Model Administration	⊕

Selected

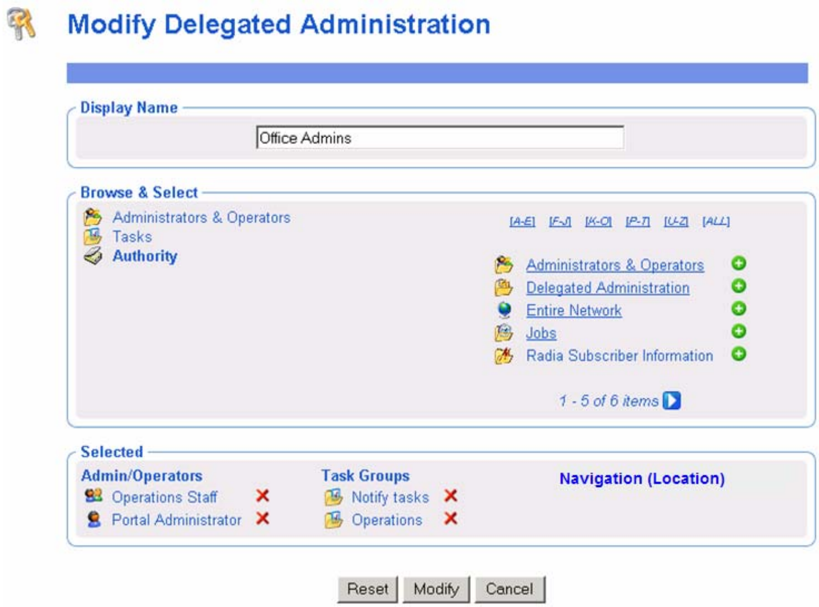
Admin/Operators		Task Groups		Navigation (Location)
Operations Staff	✕	Notify tasks	✕	
Portal Administrator	✕	Operations	✕	

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: Office Admins

Browse & Select

- Administrators & Operators
- Tasks
- **Authority**

[A-E] [F-J] [K-O] [P-T] [U-Z] [ALL]

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

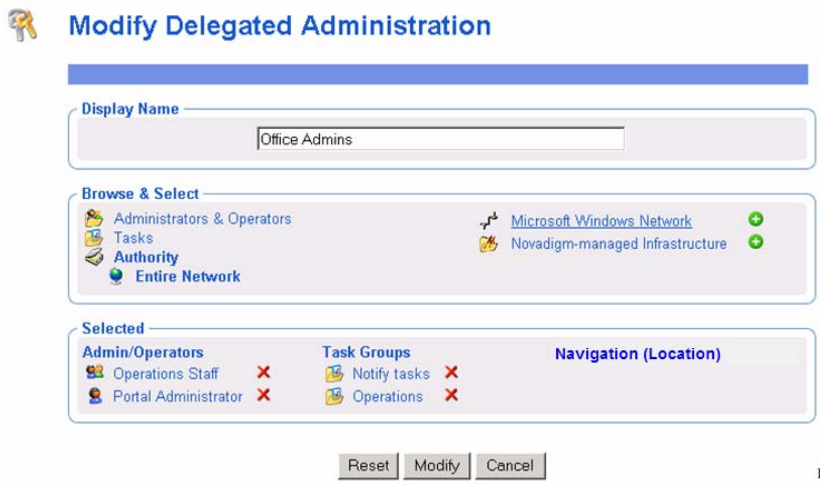
1 - 5 of 6 items ▶

Selected

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

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: Office Admins

Browse & Select

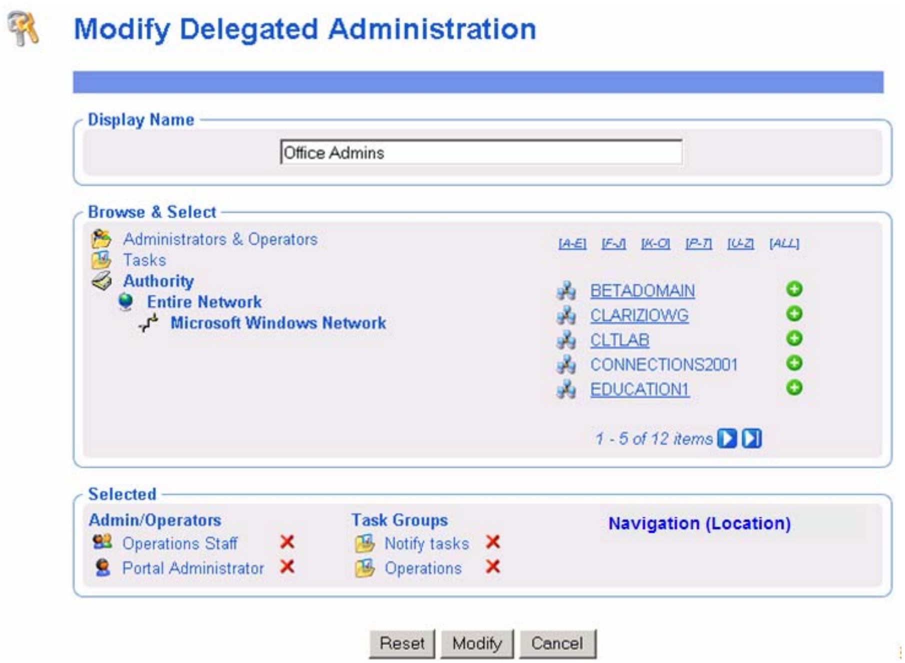
- Administrators & Operators
- Tasks
- **Authority**
  - **Entire Network**

- 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

Office Admins

Browse & Select

- Administrators & Operators
- Tasks
- **Authority**
  - **Entire Network**
    - **Microsoft Windows Network**

[A-E] [F-J] [K-O] [P-T] [U-Z] [ALL]

BETADOMAIN	⊕
CLARIZIOWG	⊕
CLTLAB	⊕
CONNECTIONS2001	⊕
EDUCATION1	⊕

1 - 5 of 12 items

Selected

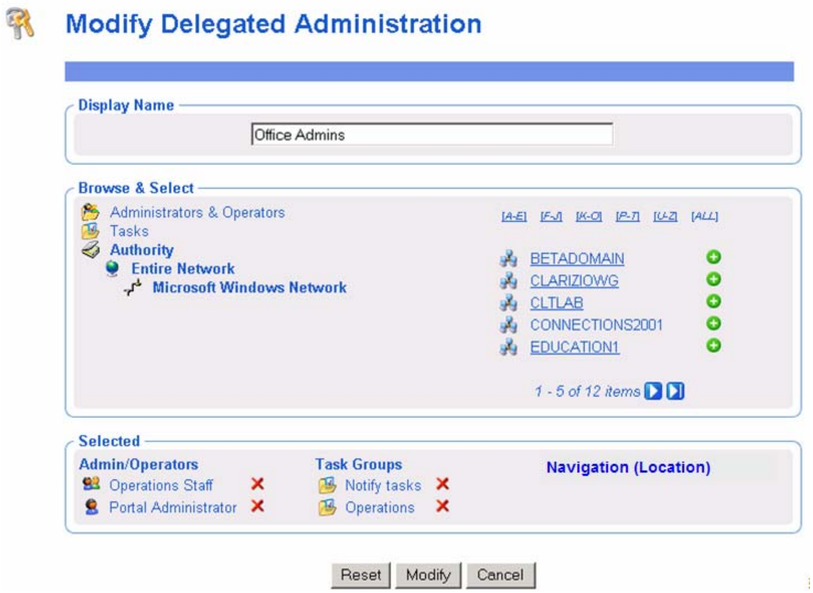
Admin/Operators		Task Groups		Navigation (Location)
Operations Staff	✕	Notify tasks	✕	
Portal Administrator	✕	Operations	✕	

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

[A-E] [F-J] [K-O] [P-T] [U-Z] [ALL]

- BETADOMAIN
- CLARIZIOWG
- CLTLAB
- CONNECTIONS2001
- EDUCATION1

1 - 5 of 12 items

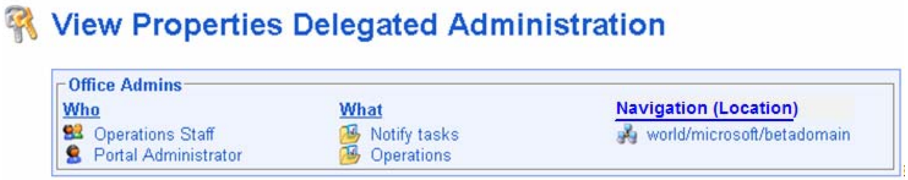
Selected

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

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.

4 Make any necessary changes. For detailed information about configuring delegated administration roles, see Adding Delegated Administration Roles on page 190.

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 Portal Directory.

or

Click ✗ to indicate that you do not want to remove the Delegated Administration role.

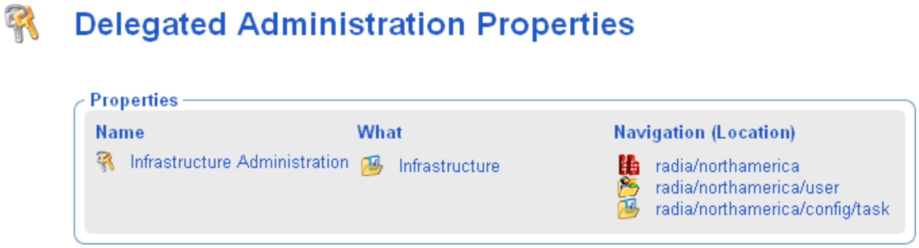
Querying a User's Delegated Administration

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 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 196 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 135 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.

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 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 135.

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 Portal 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 237 for more information about how to use this dialog box.

13. Click **Modify**.

    The Person Properties dialog box opens.

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.
5. Make any necessary changes. For detailed information about configuring users, see Adding Users on page 199.

   ➤ 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 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.

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 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.

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

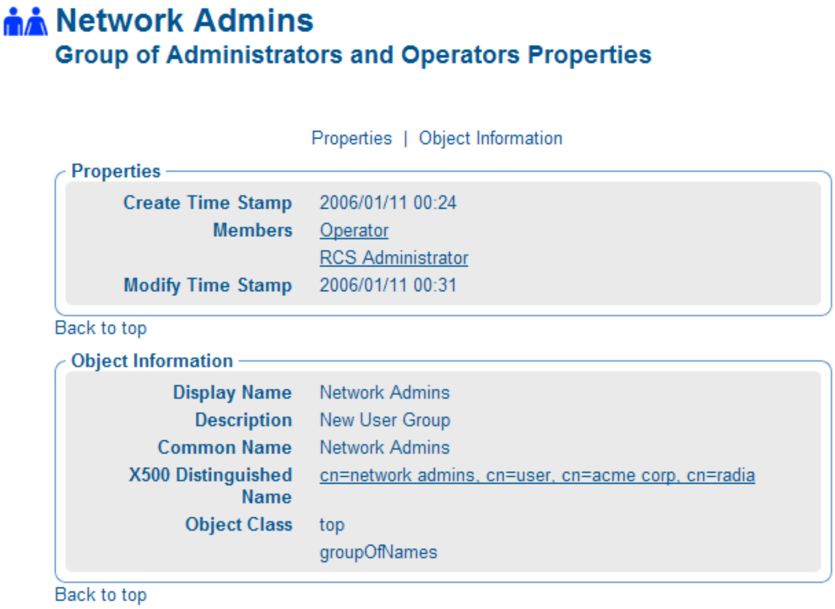
If you want to select all of the users in the list, you do not need to select anything from the Available list. Simply click ⏭ to add all of the users to the Selected list. See Selecting an Audience on page 237 for more information about how to use this dialog box.

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 Operators 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.

5 Make any necessary changes. For detailed information about configuring users, see Adding User Groups on page 202.

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 Portal Directory.

   or

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

Managing the Portal Zone Directory

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

For information on Portal Directory Troubleshooting and logging the Slapd service, refer to page 316 of Chapter , Troubleshooting.

Setting Backup Configuration Parameters

The following configuration parameters are required to enable the Backup Directory task of the Portal. If the Backup was not enabled during the initial Portal installation, it can be enabled by doing the following:

1. Use a text editor to edit the RMP.CFG file, located in the \etc folder of where the Portal was installed.
2. Set the value of ENABLE_BACKUP to 1, and set a valid port number for the ZONE_PORT_BACKUP (default is 3475). The following lines from an rmp.cfg file show entries to enable the Backup Directory facility.

```
#
rmp::init {
    ENABLE_BACKUP        1
    . . .
    . . .
    ZONE_BACKUP_PORT      3475
```

3. Save your changes to RMP.CFG, and restart the Portal service.

Table 21 Backup Directory Parameters in RMP.CFG

RMP.CFG Parameter	Description
ENABLE_BACKUP	Set to 1 to enable the Backup Directory task. Recommended. When enabled, requires a valid ZONE_PORT_BACKUP entry. Set to 0 to disable the Backup Directory task. Not recommended unless you have an external procedure in place to replicate and restore the Portal database.
ZONE_PORT_BACKUP	Port used to communicate with the backup (replicated) database. Required if ENABLE_BACKUP is set to 1. Default is port 3475.

Creating a Backup of the Portal Zone Directory

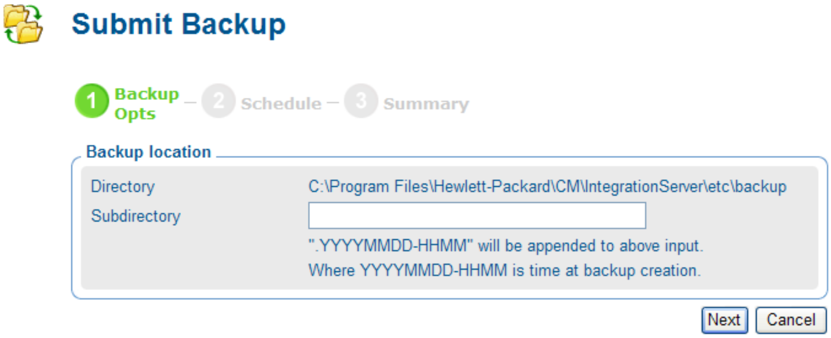
The Portal maintains up to seven backup directories with the same assigned name, and then automatically purges the oldest one if an eighth one is created. This allows you to keep seven daily backups with the same name, and keep seven weekly backups with the same assigned name.

To backup the OpenLDAP Database for the Portal Zone

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

Directory C:\Program Files\Hewlett-Packard\CM\IntegrationServer\etc\backup

Subdirectory

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

3 In the Filename text box, type a name for the subdirectory for this backup within the backup directory, for example: daily or weekly. 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
```

➤ The 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.

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 238.

6 Click **Next**.

The Submit Backup—Summary dialog box opens.

7 Click **Submit**.

A job window opens, listing all jobs and including the Backup Directory job. Use the View Properties task to view detailed information, such as the status of the job. See Viewing Properties on page 222 for more information.

8 To access the backup directories for the Portal, go to the `\etc\backup` directory of where the Portal was installed.

Restoring the Portal Directory

Use these manual Restore procedures to restore a Portal OpenLDAP database that has been backed-up using the online Backup Directory task or manually.

The backup, or replicated database, is also called a slave database. If disaster recovery is necessary, the slave database is used to restore a damaged Portal OpenLDAP master database.

Terms for Database Recovery

slapd - The stand-alone LDAP daemon. A master slapd is an LDAP directory server for the Portal database; a slave slapd is an LDAP directory server for a replicated Portal database.

slurpd – The stand-alone LDAP update replication daemon. Responsible for all activities related to distributing changes made to the master Portal database out to the various Portal database replicas.

For more information on the use of these services with an OpenLDAP directory, refer to **http://www.openldap.org/**. Slapd and slurp are discussed on this page: **http://www.openldap.org/doc/admin23/intro.html**.

Restore Procedures

To restore the master database from a Portal Backup slave database:

2 Stop the HPCA Portal service, `httpd-managementportal`.

2 Copy the slave slapd's database(s) from the `\openldap\Database\rmp-backup` location of the Portal to the master database location at `\openldap\Database\rmp`.

You should paste all files in the slave database location to the master database location.

3 Restart the Portal service.

To manually restore the database from an external backup directory

1 Stop the HPCA Portal service, `httpd-managementportal`.

2 Stop the Master Slapd.

3 Stop Slurpd.

4 Stop the Slave Slapd.

5 Copy the backup database from the desired << backup_directory>> to both `\Database\rmp` and `\Database\rmp-backup`.

6 Restart all services.

Querying the Portal Directory

Use the Query task icon on the Toolbar to locate objects in the 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 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 Portal `\etc\export` directory.

To export the 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 235 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 237 for more information.
6. Click **Next**.

   The Submit Export—Exp opts dialog box opens.
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.

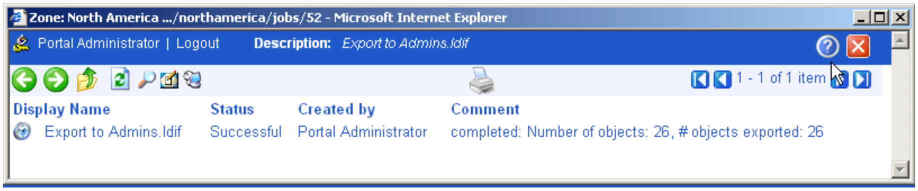
9 In the Schedule dialog box, specify when you want this job to run. For more information, see Scheduling Jobs on page 238.

10 Click **Next**.

The Submit Export—Summary dialog box opens.

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 222 for more information.


Zone: North America .../northamerica/jobs/52 - Microsoft Internet Explorer

Portal Administrator | Logout **Description:** *Export to Admins.ldif*

1 - 1 of 1 item

Display Name	Status	Created by	Comment
Export to Admins.ldif	Successful	Portal Administrator	completed: Number of objects: 26, # objects exported: 26

12 Go to *SystemDrive*:\Program Files\Hewlett-Packard\CM\ManagementPortal\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 Portal Directory. For example, if you prefer to modify the Portal Directory manually, in a text file, rather than through the Portal user interface, you can export the directory, make your modifications, and then import the file into the Portal Directory.

Be sure to back up your Portal Directory before importing any data. See Creating a Backup of the Portal Zone Directory on page 205 for more information.

To import the 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 Portal \etc\export\ directory).

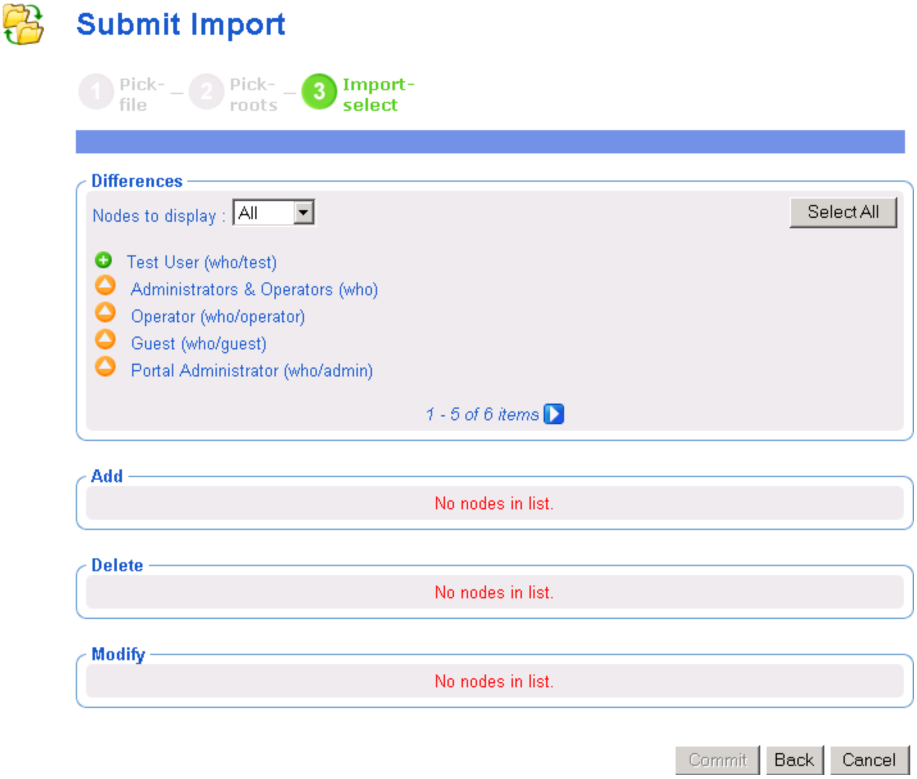
3 Click the file that you want to import.

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.

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 : All

Test User (who/test)
Administrators & Operators (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.

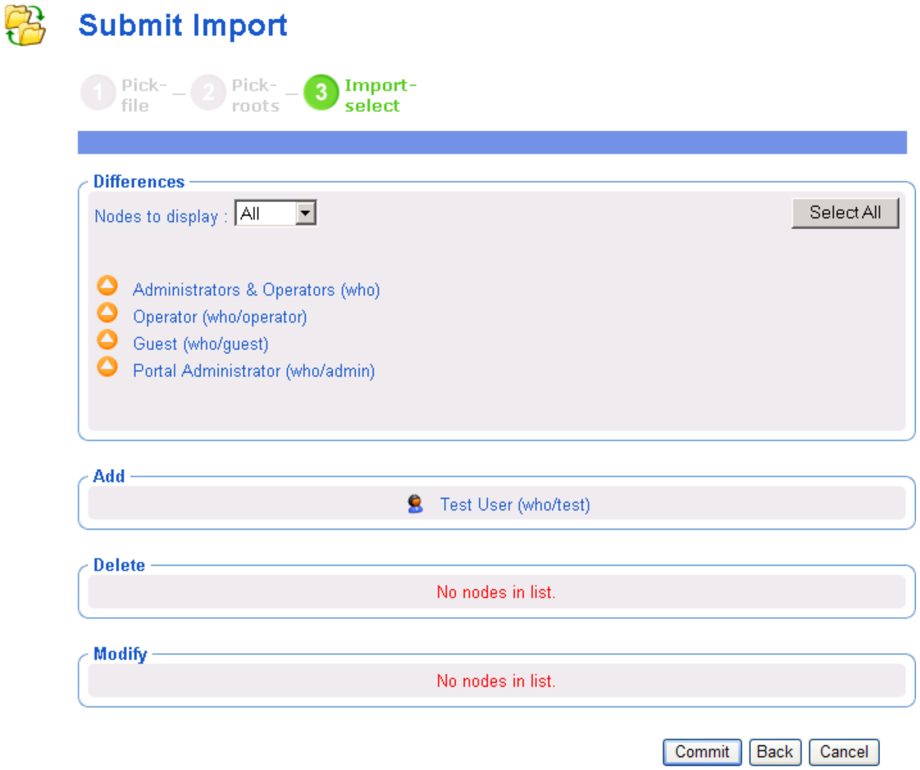
- Select **Add** to review only those items that have been added to the LDIF file.
- Select **Delete** to review only those items that have been removed from the LDIF file.
- Select **Modify** to review only those items that have been modified in the LDIF file.

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

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

Add

Test User (who/test)

Delete

No nodes in list.

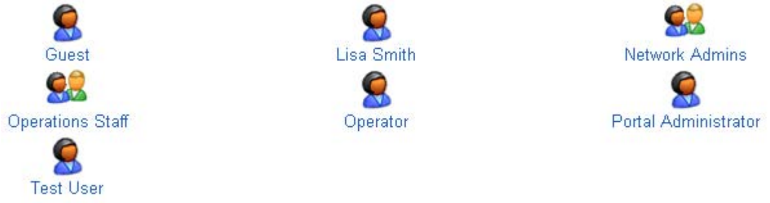
Modify

No nodes in list.

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.



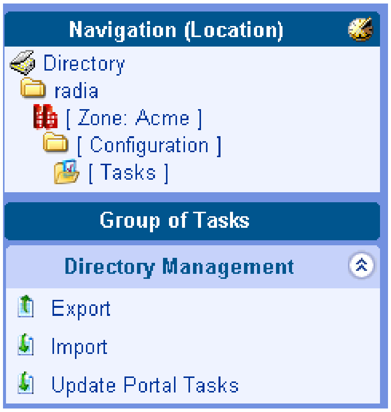
Updating Portal Tasks

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

This task is not enabled in the initial build of a major Portal release, such as version 5.00.

To update Portal tasks

1. Stop the Portal. See Starting and Stopping the Portal on page 37 for more information.
2. Copy the new `rmp.tkd` into the `\modules` folder of your Portal directory (by default `*Drive*:\Program Files\Hewlett-Packard\CM\ManagementPortal\modules`).
3. Start the Portal. See Starting and Stopping the Portal on page 37 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.

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

9 Click **Commit**.

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

Managing Jobs

The Jobs container in the 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 222.

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.

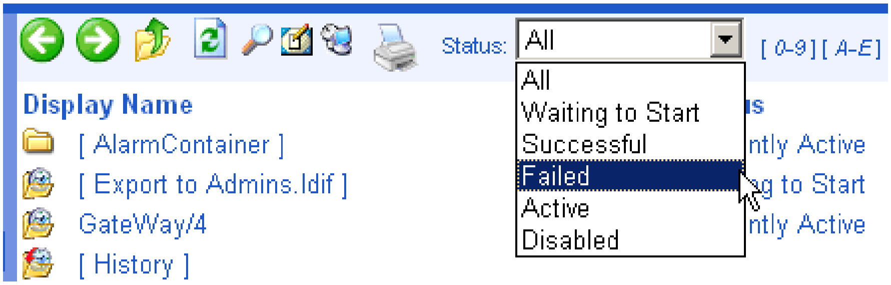
Use the Query Jobs task to further locate a set of jobs that meet additional criteria, such as a scheduled start time or period, the target audience, and who submitted the job or job group. For details, see Querying Jobs or Job Groups on page 218.

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.

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.

4 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.

- In the Scheduled From Time drop-down lists, select the earliest date and time when the job or job group was scheduled to start.
- In the Scheduled To Time drop-down lists, select the latest date and time when the job or job group is scheduled to start.

5 In the Display drop-down list, select **Jobs** or **Job Groups** to specify how you want to limit your query.

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.

6 Use the Job Characteristics area to further limit your query.

- 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.
- 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.
- 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.
- 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.

7 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.

- 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.

8 Click **Next**.

A list of the jobs or job groups that match the selected criteria opens.

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.

2 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.

3 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 **History**.

3 Job histories are listed in reverse chronological order by date and time. History files include the date in the format: `YYYYMMDD`.

4 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.

5 Click a specific job group from those displayed in the workspace.

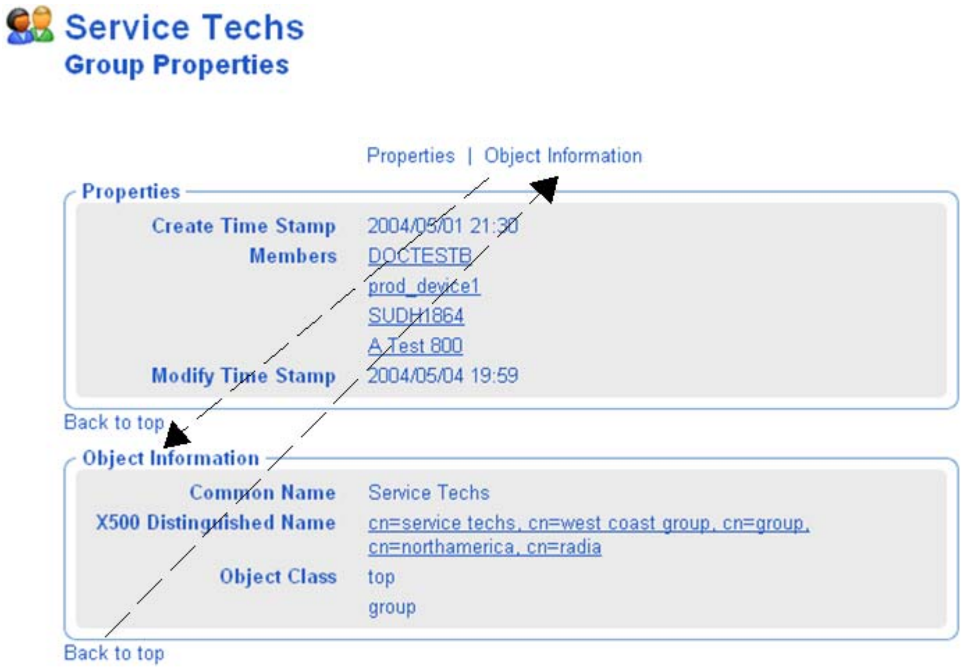
The workspace lists the jobs that ran in that job group.

6 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 Test 800
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 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 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 Portal Zone Directory.
- Use the Export task to export a subset of your Portal Directory to an LDIF file.
- Use the Import task to import an LDIF file into your 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 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 notify quickly a computer by name.
- Be able to install the Client Automation agents using default or customized profiles.
- Be able to add, modify, or delete Agent install profiles.
- Be able to install the Portal 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 Portal zone.
- Be able to add task templates for scheduling jobs.
- Be able to schedule jobs to run in multiple Portal zones.
- Be able to run a sequence of jobs in a single task.
- Be able to use remote control to manage Client Automation agents.

The 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. A person (via a task) or a scheduled operation initiates it.

This chapter explains how to use the Portal to perform these tasks and assumes that you understand how to use the Client Automation product suite.

If necessary, refer to the HP Support web site for more information.

The core tasks in the Portal are:

- **Manage Computer**
  Click **Manage Computer** to bring one or more computers into your Portal zone. Managed computers have an entry in the Portal **Zone** → **Devices** container, and an automatic membership in the Default Group. For details, see Managing Computers in Your Portal Zone on page 230.
- **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 Client Automation Agent**
  Click **Install Client Automation Agent** to install the Client Automation agent on remote computers. See Installing the Client Automation Agent on page 262 for more information. Multiple Agent Install Profiles are supported. For details, see Supporting Remote Installs Using Multiple Profiles on page 266.
- **Install Portal Agent**
  Click **Install Portal Agent** to install the Portal agent on remote computers. See Installing the Portal Agent on page 252 for more information.
- **Install Proxy Server**
  Click **Install Proxy Server** to install the Proxy Server on remote computers. See Installing the Proxy Server on page 272 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 276 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 277 for more information.

- **Notify Devices**
  Use the Notify tasks to perform an action on the selected audience. See Using the Notify Tasks on page 240 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 244 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 Subordinate Portal**
  Click **Install Subordinate Portal** to remotely install another Portal zone in your infrastructure. See Installing Additional Portal Zones (Subordinate Zones) on page 282 for more information. Also refer to the tasks for Open Subordinate Zone and Schedule Zone Operation.

- **Update Subordinate Portal**
  Click **Update Subordinate Portal** to remotely update the code delivered with a new build to the subordinate Portal zones in your infrastructure. See Updating Subordinate Portal Zones on page 286 for more information.

- **Open Subordinate Zone**
  Click **Open Subordinate Zone** to quickly access the Portal of another Zone in your enterprise from the Zone Access Points container. See Opening a Subordinate Zone on page 292 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 287 for more information.

Managing Computers in Your Portal Zone

Use the Manage Computer task to bring the computers in your network or external directories under the control of the Portal zone.

> 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 Portal will bring any selected devices under management automatically.
>
> To learn other ways to add devices to your Zone, see Adding Devices to a Portal Zone on page 140.

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.

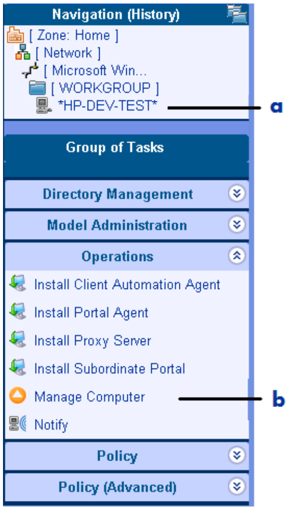
Once a device is under management of the Portal Zone, it can be selected for an operation or for other group memberships.

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

> This task is optional. When you run any install task, the Portal automatically bring the device under Portal management before proceeding with the install.

1. Use the navigation aid and workspace to go to the zone's Network 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 Manage Computer dialog allows you to select one or more Group Memberships. Click **Manage** to add the Device to the selected Group.

The Portal creates a unique device entry in the Zone Devices container for this computer.

The Operations task group displays many tasks that are available for this managed device. To take the best advantage of the 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 163.
- Install the Portal Agent on the device to make use of Device Categories. For more information on the advantages of adding the Portal Agent, see Installing the Portal Agent on page 252.

To manage a group of computers in your network

You do not need to perform this task before performing an install task; any install task will automatically bring the devices in a targeted network group under managemement before proceeding with the installs.

Before selecting a group of computers, you should become familiar with the dialogs to browse and select devices for a group as discussed in Basic Procedures for Modifying Groups on page 142.

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 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 163.

To manage one or more computers located in Active Directory

You do not need to perform this task prior to performing an install task; the install tasks will automatically bring any selected LDAP directory devices under Portal management before proceeding with an install.

An Active Directory can be configured for access by a CM administrator. In this case, it will appear as an object in the 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 111.

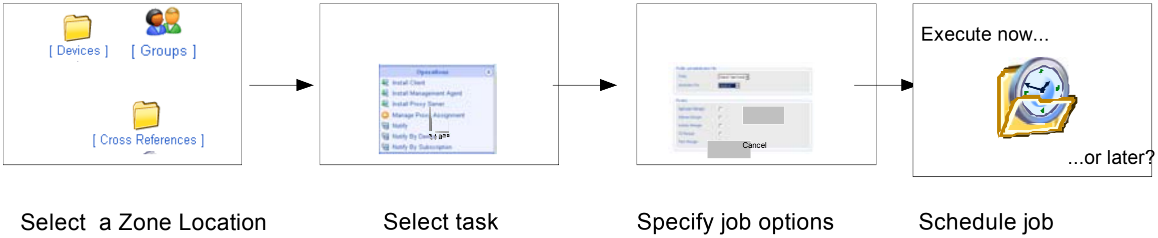
About the Task Lifecycle

Operational tasks are performed on devices and device groups under management by the Portal Zone. These devices and group membership exist in one of three locations:

- Device Container (individually)
- Groups Container (Default Group and created Groups)
- Device Categories Container Groups (groups generated from devices with installed Portal 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 24 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 Device Categories 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 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 CM Proxy Service object under a device object, or a Device Categories container of all CMProxy Servers.

3. **Specify job options.**
   The options vary from task to task. For example, if you perform 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**.
   After you specifythe information for the job, a summary of your selections opens. Aafter you review the summary, submit the job.

Basic Procedures for Operations Tasks

Because every task has the same lifecycle, 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 Portal. When you finish entering the necessary information, a job is created.

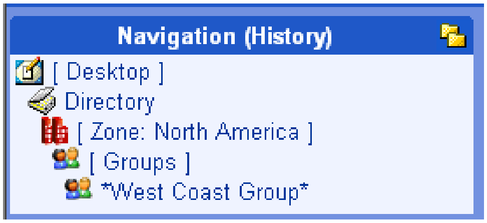
This section covers these basic procedures in detail.

Selecting a Starting Zone, Network, or Directory Location

When you start an operation, select a zone location for performing the task that includes all objects on which you want to perform the task. Review zone containers in About the Zone Containers on page 73. Different zone containers contain different object classes.

- You start most operational tasks from a Zone's Device, Groups, or Device Categories containers—depending on whether you are performing a task on either an individual device or a group of devices. See Establishing Devices and Device Groups on page 140.
- Install operations can also be started from locations in a Zone, Network container or from an LDAP Directory Services location. The Portal will first bring the devices targeted for the install under management before performing the install operation.

- Operations related to other zones in your enterprise are started from the Zone Access Points container.
- See Navigating the Portal Directory and the Zone Containers on page 53.



Navigation (History)

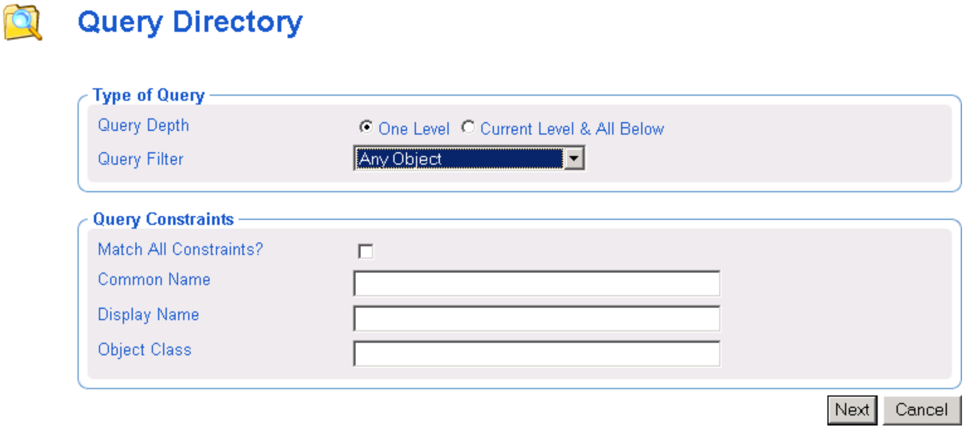
[Desktop]
Directory
[Zone: North America]
[Groups]
West Coast Group

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 25 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:

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, 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.

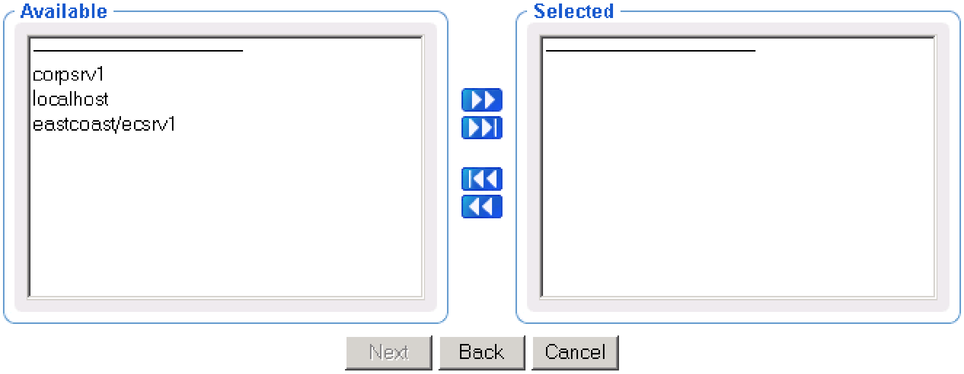
5 Click **Next** to initiate the query and to move to the next step in the task.

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 26 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

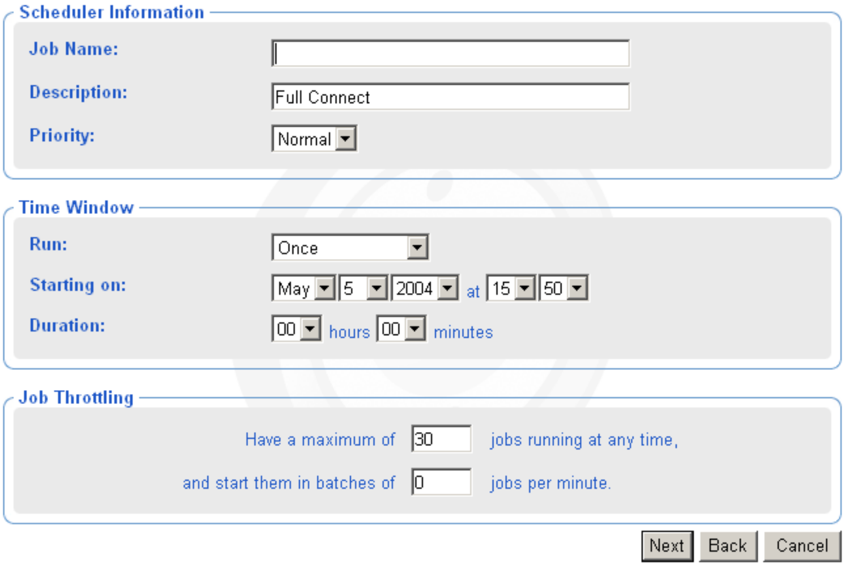
Use the Schedule dialog box to set the scheduling options for the job. By default, a job will begin immediately and run only once. However, you can modify these settings.

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 27 Submit Notify—Schedule dialog box (Windows)



Scheduler Information

Job Name:

Description: Full Connect

Priority: Normal

Time Window

Run: Once

Starting on: May 5 2004 at 15 50

Duration: 00 hours 00 minutes

Job Throttling

Have a maximum of 30 jobs running at any time,

and start them in batches of 0 jobs per minute.

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 If available, 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 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 Portal agents are installed on devices in your zone, you can also use the Notify task from the **Zone** → **Device Categories** 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, Client Automation infrastructure, or Managed Services.

> Use the Notify task from the Device Categories container groups (Hardware, Operating System, IP address Subnet, or Infrastructure) to quickly identify a target audience based on device characteristics.
>
> Use the Notify task from the Device Categories Managed Services container to quickly identify a target audience based on an application currently being Client Automation-managed.

- **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 244 for more information.

Refer to the *HP Client Automation Application Manager and Application Self-service Manager Installation and Configuration Guide (Application Manager and Application Self-service Manager Guide)* for more information about notifying Client Automation agents.

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 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 235 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.

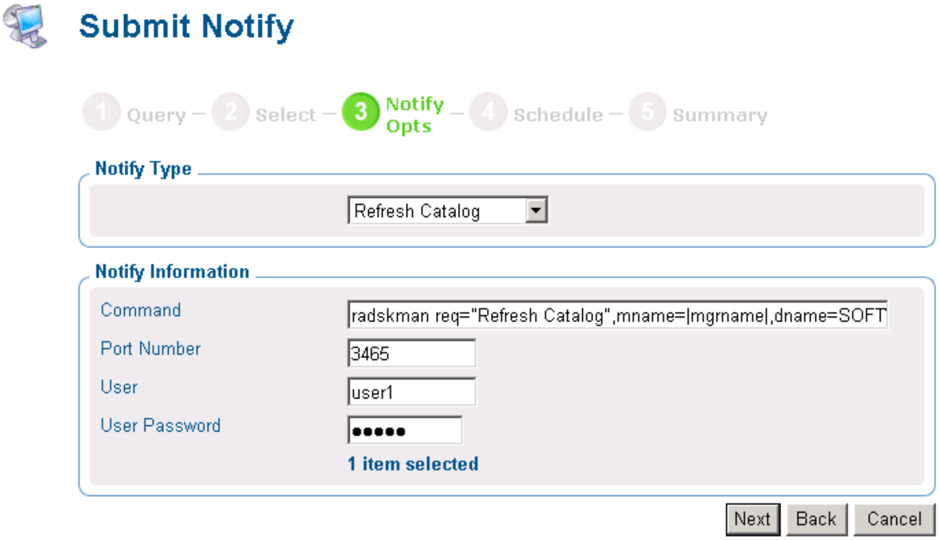
4 Click **Next**.

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 237 for more information.

6 Click **Next**.

The Submit Notify—Notify Opts dialog box opens.



Submit Notify

Notify Type

Refresh Catalog

Notify Information

Command	radskman req="Refresh Catalog",mname=|mgrname|,dname=SOFT
Port Number	3465
User	user1
User Password	●●●●●

1 item selected

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 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 245 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 238.

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 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.

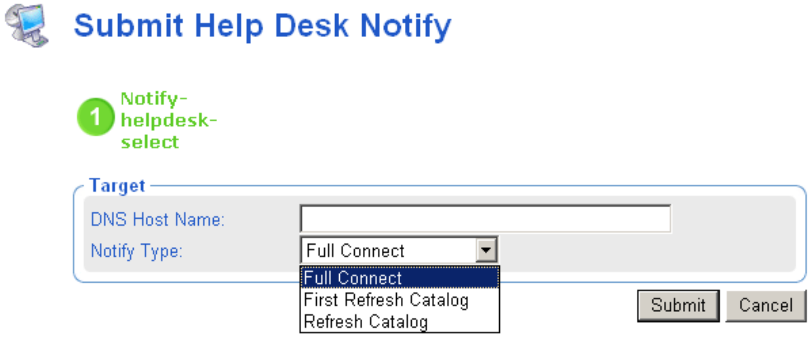
The options and command syntax for the notify task submitted through the Help Desk Notify need to be previously set or customized. For details, refer to one of the following sections:

- Setting Default Options for Notify Commands on page 245.
- Creating Custom Notify Commands on page 248.

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

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 245.

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 a 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**.

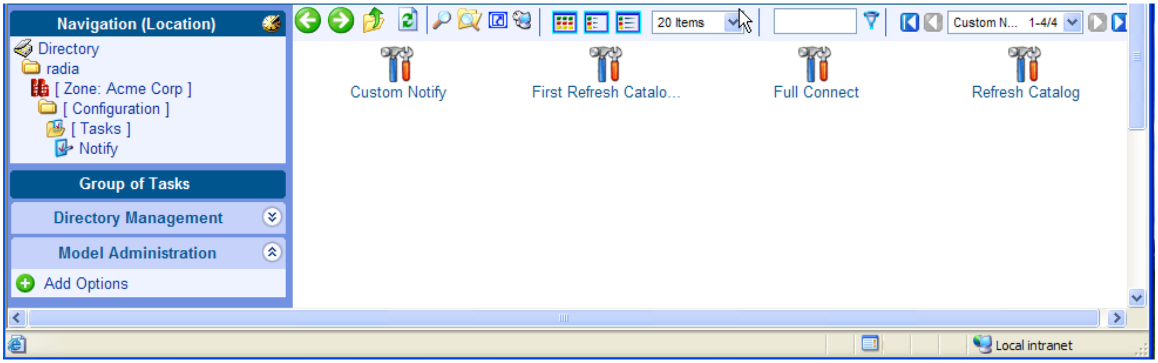
3 In the workspace, locate the notify task that you want to modify, such as **Notify**.

➤ To quickly find the tasks beginning with No, type **`No*`** in the filter area and press **Enter**.

See Paging and Filtering Icons on page 69.

4 Click the **Notify** task to select it.

5 The workspace displays objects that represent the default options for each of the notify operations.

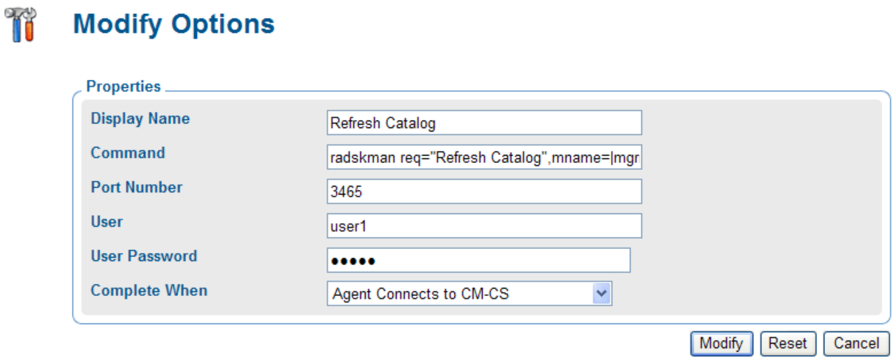


6 In the workspace, click the type of notify operation for which you want to set default options, such as **Refresh Catalog**.

The Options Properties dialog box opens.

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=|mgr
Port Number	3465
User	user1
User Password	•••••
Complete When	Agent Connects to CM-CS

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.

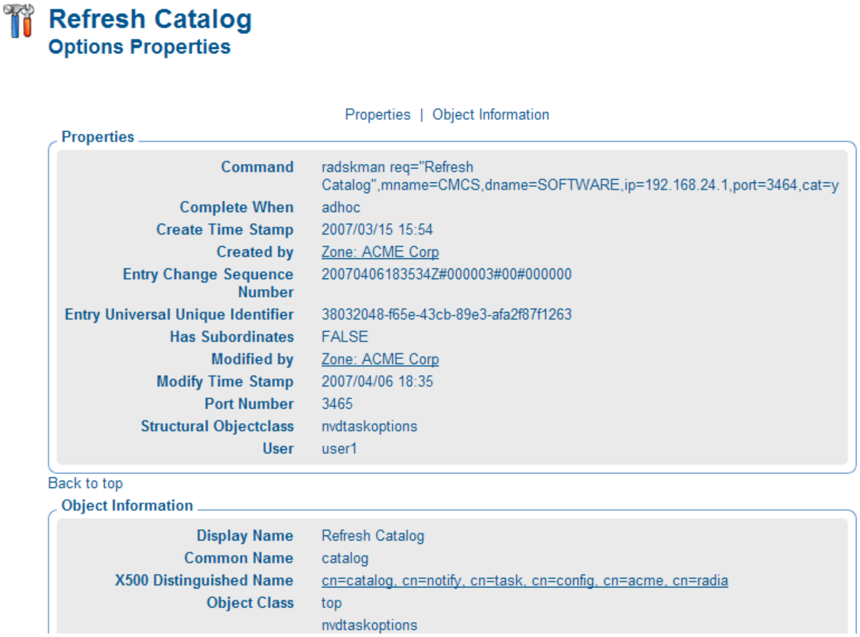
— From the Complete When drop-down list, indicate when the notify is considered completed. See the HP Support web site for detailed information about the Client Automation agent and the Application Event (APPEVENT) object. If you are unsure about which option to select, select **Agent Contacted**.

Complete When Selection:	Complete When Job Property:
Agent Contacted	adhoc
Agent Connects to Configuration Server	radia/catalog
Agent Sends Application Event	radia/service
Agent Processing Finished (Synopsis)	

9 Click **Modify**.

The Options Properties dialog box opens and you can review your changes.

The next figure shows a sample command line.



Refresh Catalog
Options Properties

Properties | Object Information

Properties

Command	radskman req="Refresh Catalog",mname=CMCS,dname=SOFTWARE,ip=192.168.24.1,port=3464,cat=y
Complete When	adhoc
Create Time Stamp	2007/03/15 15:54
Created by	Zone: ACME Corp
Entry Change Sequence Number	20070406183534Z#000003#00#000000
Entry Universal Unique Identifier	38032048-f65e-43cb-89e3-afa2f87f1263
Has Subordinates	FALSE
Modified by	Zone: ACME Corp
Modify Time Stamp	2007/04/06 18:35
Port Number	3465
Structural Objectclass	nvdtaskoptions
User	user1

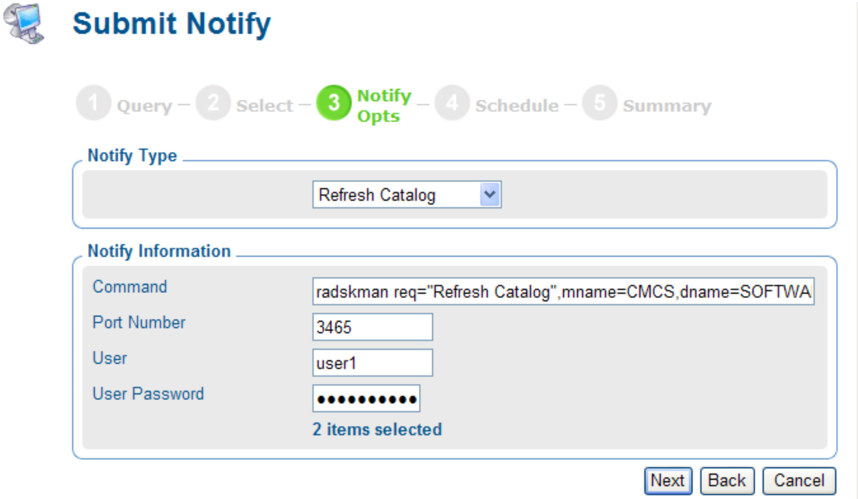
Back to top

Object Information

Display Name	Refresh Catalog
Common Name	catalog
X500 Distinguished Name	cn=catalog, cn=notify, cn=task, cn=config, cn=acme, cn=radia
Object Class	top nvdtaskoptions

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

Notify Type

Refresh Catalog

Notify Information

Command: radskman req="Refresh Catalog",mname=CMCS,dname=SOFTWA

Port Number: 3465

User: user1

User Password: ●●●●●●●●●●

2 items selected

See Notifying an Audience on page 241 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 Options**. The Add Options dialog box opens.
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 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.

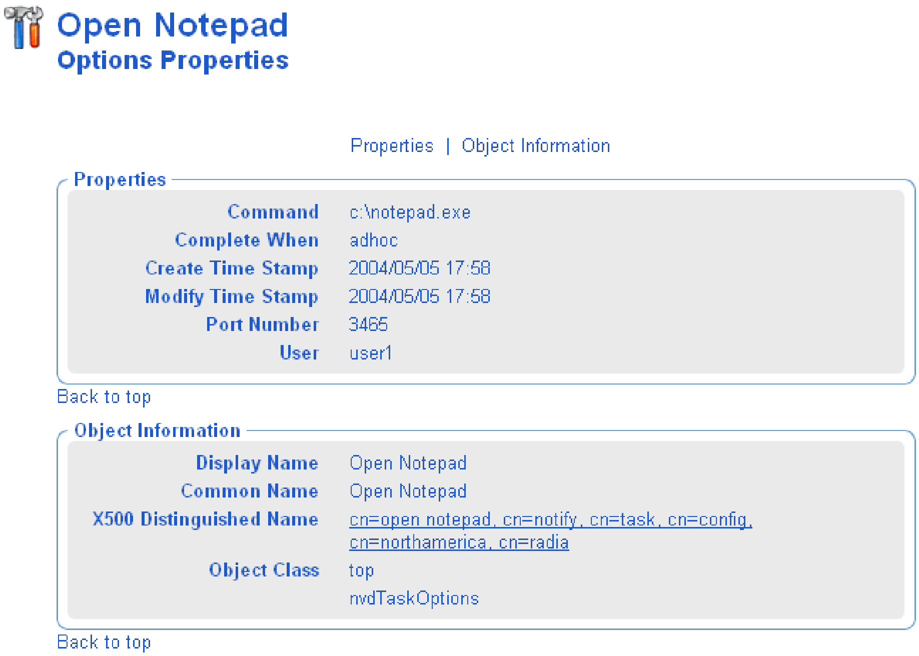
11 In the Complete When drop-down list, select the client action that is to indicate this notify task is complete. The following table shows how your selection is reported on a Task Property or Job Property dialog box.

Table 22 Notify Job Completion Options

"Complete When" Selections	Equivalent Entry on Task Property and Job Reports
Agent Contacted	Adhoc
Agent Connects to Configuration Server	radia/catalog
Agent Sends Application Event	radia/service
Agent Processing Finished (Synopsis)	radia/synopsis

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 241.
- For more information about the Submit Help Desk Notify dialog box, see Using Help Desk Notify on page 244.

Deploying Infrastructure Products and Applications

Use the Portal to install Client Automation infrastructure products and applications to remote devices.

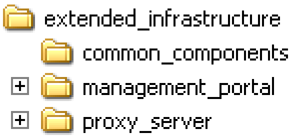
Requirements for Remote Installations

In order to install Client Automation infrastructure products, you must be aware of the following requirements.

- For Windows, the remote computer must be running one of the supported Windows platforms as listed in the accompanying HPCAE 7.20 Release Notes.

- For UNIX, this version of the Portal does not support remote *Infrastructure* installations to UNIX platforms.
- The installation files for the Client Automation product must be stored in the Portal's `\media` directory. The Portal installation program will copy these files automatically. See Installation Procedures on page 30 for more information.

  If you did not use the installation program to copy the files, you must manually copy these files from the appropriate media to the Portal's `\media` directory. The directory structure of the media directory should mirror the media 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 Portal creates the packing list when you launch the remote installation.
- The Management Agents must be able to communicate back to the 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 4 on page 108.

Specific instructions about how to use the Portal to perform each remote install follows.

Prerequisites for Installing Portal Agents onto Linux Devices

When the Portal is installed from a media build, also install the **'Remotely Installable Infrastructure Components"** to place the needed `nvdkit` and `rma.tkd` in the appropriate locations for Steps 1 and 2, below.

1 Verify `nvdkit` is located in this media folder under the Portal installation directory:

  ./media/extended_infrastructure/management_portal/*`<os specific folder>`*/media/nvdkit

  The *`<os specific folder>`* names are:

OS	**Folder Name**
Linux	linux (for Red Hat Linux and Suse Linux)

2 Verify `rma.tkd` is located at this folder where the Portal is installed:

./media/extended_infrastructure/management_portal/<os specific folder>/media/modules/rma.tkd

3 Modify the Portal configuration file, `rmp.cfg,` to include the following line, and then restart the Portal service.

```
USE_SSH    1
```

4 The target Device's Properties requires an OS attribute. The valid OS attribute for Linux devices is: **`linux`**. (Use linux for Red Hat and Suse).

If the device is added using the Portal Interface, modify the Device Properties to add the appropriate OS attribute.

5 The SSH daemon must be running on the target Linux Agent machine.

Installing the Portal Agent

You can use the Portal to perform operational and administrative tasks on the Client Automation infrastructure; however, the Portal cannot always perform these tasks remotely. Therefore, the Portal Agent, which is a thin delegate, is installed on the remote device to perform these tasks on behalf of the Portal. It cannot perform any tasks on its own.

For Windows devices only, when you use the Portal to install CM management services or applications, the Portal Agent is automatically installed on the same device. Use the Install Portal Agent task to install, and optionally re-install, the Portal agent to remote devices. After registering with the Portal, the Portal agent performs the task initiated by the Portal, such as a remote installation.

The Portal agent is installed as a Windows Service on all supported Windows platforms (refer to the HPCAE 7.20 Release Notes for platform support details) and is configured to contact the Portal at regular intervals in order to make its presence known. The Portal agent will notify the Portal when normal operations occur, such as system shut down or restarts.

For Linux, the Portal agent can be installed onto Red Hat and Suse Linux devices that are supported by the Client Automation Agent. Refer to the accompanying Release Notes for the specific Red Hat and Suse platforms supported by the Client Automation Agent.

RMA Registration Throttlingt

An internal throttling feature is built into the Portal to efficiently manage the processing of large numbers of first-time Portal Agent registrations. This throttling feature avoids a potential Portal-processing deadlock situation that can occur when very large numbers of Portal Agents are installed at the same time. The registration throttling feature can be fine tuned, if required, in consultation with customer support.

Portal Agent Registration Schedule and Tasks

The Portal Agent is configured, by default, to contact the 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 Portal Agent port number for Portal Agents using dynamic port assignments, or a different IP address in DHCP environments.

If the Portal Agent has no changes to report from the previous day, it does not contact the Portal.

> Consider using Portal Agents with a static port assignment if you want to eliminate the Portal Agent-registration updates that are generated by Portal Agent s using dynamic port assignments.

The following is a list of some, but not all, of the tasks that the Portal Agent can handle on behalf of the Portal.

- Starting or stopping services.
- Performing remote installations. (Limited to Windows, only).
- Discovering all Client Automation services that are currently running on the device, such as the Notify Daemon, Scheduler Daemon, Configuration Service, and the Integration Service and sub-services.
- Discovering the Client Automation-managed services on the device.
- Discovering hardware and operating system details of the device, including service pack levels, MAC address and IP subnet.

RMA Signal Processing Parameters and Logs

The Portal uses a set of dedicated thread pools to handle the incoming signal processing requests from the Portal Agents. As your Portal Agent workload increases, you may want to adjust the configurable parameters related to Portal Agent signal processing. For more information, refer to Managing Portal Agent Signal Processing on page 318.

Viewing Device Information Discovered by the Portal Agent

For examples of the information collected by the Portal 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 Device Categories container of the zone. These groups are created from the information collected by the Portal Agent.

Choosing a Dynamic or Static Port Assignment for the Portal Agent

For all tasks that install the Portal Agent, you can specify whether the Portal should communicate with the Portal Agent using a dynamically assigned port or a static port.

- Using a dynamic port assignment for the Portal Agent reduces the risk of security attacks on well-known ports.
- Using a static port assignment for the Portal Agent is available to communicate to an agent that is behind a firewall, and to reduce daily registrations from a Portal Agent due to a new port number (which occurs with dynamic port assignments).

Modifying the Portal Agent Re-Install Option

To facilitate the deployment of newer versions, the Install Portal Agent task includes an option to force a re-install of the Portal Agent. This option is turned on by default. To review or turn off this option, access the Modify Install Portal Agent Options dialog box.

To set the Install Portal Agent task options

1. Go to the **Directory** → **Zone** → **Configuration** → **Tasks** container.
2. From the workspace, page forward ▶ or use the filter area □ to locate and then select the **Install Portal Agent** task.
3. Click **Modify** in the Model Administration task group.

   The Modify Install Portal 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.TKD`s will not have the Portal Agents updated using the Install Portal Agent task.

To install the Portal Agent

Be sure to read Requirements for Remote Installations on page 250 before performing this procedure.

To install the Portal Agent onto a Linux device, refer to the prerequisites on page 251

To install the Portal Agent onto a device running Vista using the Domain Admin account, ensure that File and Print Sharing is enabled on the Vista device.

1 Use the navigation aid to select the place in your infrastructure where you want to install the Portal Agent.

> Select devices from any location in your zone, Networks container, or an LDAP directory location, that contains the computers on which you want to install the Portal Agent. If the Portal is not currently managing the targeted Network or LDAP devices, the Portal will bring them under management as part of the install task.

2 From the Operations task group, click **Install Portal Agent**.

> If you selected a single Authority, such as a particular computer or a group of devices, and then selected Install Portal Agent, you 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 Portal Agent — Install Opts dialog box opens.

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 Portal Agent on the same computer as the Portal, delete Administrator from the User text box.

7 Use the Select Portal Port radio buttons to specify whether the Portal should communicate with the Portal 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 Portal Agent 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 Portal Agent—Summary dialog box opens.

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 Portal.

The Portal uses the information discovered by the Portal Agent to add the device to the appropriate groups in the Device Categories container of the Zone.

When the Portal Agent is installed to the remote device and the service is started, a log (`rma.log`) is created in the directory where the Portal Agent is installed. The Portal Agent is installed to `*SystemDrive*:\Program Files\Hewlett-Packard\CM\ManagementAgent`.

Refreshing the Portal Agent

An installed Portal Agent discovers and registers the Integration Server sub-services installed on the remote computer. If additional Integration Server sub-services are installed on the remote computer after the Portal Agent's last discovery, use the Refresh Portal Agent task from the Operations task group to immediately update the registered sub-services on the Portal.

The Refresh Portal Agent task will also remove the registration of services that have been uninstalled since the previous registration. For example, if a Client Automation agent has been removed from a computer since the previous registration, running Refresh Portal Agent will remove the machine's client-related services, such as the Notify Daemon and the Scheduler Daemon, from the Portal registry.

To refresh a Portal Agent's sub-service discovery

1. In the navigation area, navigate to the appropriate device object whose Management Portal Agent service discovery needs to be refreshed.

   You do not need to navigate to the Management Portal Agent, just to the device object.

2. From the Operations task group, click **Refresh Portal Agent**.

Click 🔄 to refresh the workspace area of the Portal. You'll see the current, newly registered Client Automation services and sub-services for the object.

Upgrading the Portal Agent

After migrating or upgrading the Portal to a new version, the Portal Agents on the managed devices also need to be upgraded with the latest `rma.tkd` version. This can be done by running the **Install Portal Agent** task against the devices in your Zone, or, by enabling the Portal Agent self-maintenance feature.

Enabling Self-maintenance for Portal Agents

Portal Agent self-maintenance can be configured to upgrade the Portal Agents on the Windows or Linux devices in your Zone automatically. The maintenance can be applied proactively, or when the Portal Agents register with the Portal. The maintenance can be performed as a critical (high priority) task for the Portal, or only when the Portal is not otherwise busy.

Use the following manual procedures to enable this feature.

To activate self-maintenance for the Portal Agents (or RMAs)

1 Create these folders under your `\ManagementPortal` installation directory for the Portal Agent (RMA) upgrade:

```
\media\extended_infrastructure\management_agent
\media\extended_infrastructure\management_agent\rma
```

2 In the above `\management_agent\rma` folder, copy the latest `rma.tkd` from the Client Automation Portal installation media, or as provided by HP software support.

Note: The `rma.tkd` is *not* OS-specific. To use the latest `rma.tkd` delivered with the Portal on the Client Automation media, copy it from: `\Infrastructure\extended_infrastructure\management_portal\<any OS platform>\media\modules`.

3 You will need the build number of the latest `rma.tkd`. (For Portal 5.10, it was 1305, for Portal 5.11, it was 1405, for Client Automation 7.20, it is 1523 or greater.) To obtain the build number, temporarily place the latest `rma.tkd` in the base `\ManagementPortal` directory that contains nvdkit.exe, and run the command:

```
nvdkit version rma.tkd
```

4 Optionally, you can use the Self-maintenance feature to also upgrade the nvdkit build on the Portal Agents with a critical one provided from HP software support. *The nvdkit executable is OS-specific*. If you don't need to upgrade nvdkit, skip this step.

To use this option, also create these kit subdirectories under your `\ManagementPortal` installation directory with OS-specific subfolders to hold the appropriate nvdkit module for your Portal Agents:

```
\media\extended_infrastructure\management_agent\kit
```

```
\media\extended_infrastructure\management_agent\kit\<OS platform>
```

The supported OS-platforms for Portal Agents include: `linux` and `win32`.

Copy the latest `nvdkit` executable provided by HP software support to the appropriate locations listed above.

Note: The latest nvdkit build supplied with Client Automation 7.20 media is build 460 or above.

5 Create a text file named **`selfmaintenance`** (with no file extension). The content of **`selfmaintenance`** needs to define these case-sensitive parameters and values.

```
criticalKitBuildNum   <Critical nvdkit build number>

criticalRMABuildNum   <Critical RMA build number>

expectedRMABuildNum   <Expected RMA build number>

proactiveupgrade  <0|1>
```

Note: Use spaces to separate the parameters and values; do not use the tab character.

Table 23 RMA self-maintenance parameters

Parameter	Explanation
`criticalKitBuildNum`	This parameter was added as of Portal v 5.11. Optional. Use this to apply a critical nvdkit upgrade, such as one provided to you from HP support. Specify the minimum nvdkit build number that must be on the RMA device. If the specified number is greater than the build number of the nvdkit on the RMA machine, then the nvdkit will be upgraded.
`criticalRMABuildNum`	Specifies the minimum RMA build number that **must** be on a device. If a device has a lower RMA build number, its RMA will be upgraded on a **priority basis**. This will be done even if the Portal is busy. If you want to disable the processing of priority-basis RMA upgrades, set this value to 1. **Note:** For selfmaintenance to be applied, the build number of the `rma.tkd` in the `\media\extended_infrastructure\management_agent\rma` folder must be greater than or equal to this value.

Parameter	Explanation
expectedRMABuildNum	Specifies the minimum RMA build number that is expected on the devices. If a device has an earlier RMA build number, the RMA on that device will be upgraded on a **non-priority basis**. The RMAs will be upgraded when the Portal is not busy. To disable non-priority basis RMA upgrades, set this value to 0. **Note:** For selfmaintenance to be applied, the build number of the rma.tkd in the \media\extended_infrastructure\management_agent\rma folder must be greater than or equal to this value.
proactiveupgrade	Specifies a flag value of 0 or 1. If set to 1, the Portal proactively upgrades existing RMAs without waiting for register signals. If set to 0, the Portal upgrades older RMAs whenever a register signal is received from that device. Setting this flag to 1 can make the Portal busy as it attempts to upgrade RMAs proactively.

6 Place selfmaintenance in this folder:

```
\media\extended_infrastructure\management_agent
```

As soon as the selfmaintenance file is placed in this folder, the Portal begins executing the RMAAutoUpgrade job to perform RMA self-maintenance; the Portal service does not require a restart.

Self-maintenance Examples

For all examples below, rma.tkd for Build 1523, or above, is placed in the folder:

\media\extended_infrastructure\management_agent\rma

Example 1: These entries proactively upgrade the RMAs in the Portal Zone. It upgrades RMAs with Builds less than 1405, on a priority basis, and upgrades RMAs with Builds less than 1523 on a non-priority basis (when the Portal is not busy).

```
criticalRMABuildNum    1405
expectedRMABuildNum    1523
proactiveupgrade       1
```

Example 2: These entries upgrade RMAs with Builds less than 1405, on a priority basis, whenever the RMAs contact the Portal.

```
criticalRMABuildNum    1405
expectedRMABuildNum    0
proactiveupgrade       0
```

Example 3: These entries upgrade the RMAs with Builds less than 1405 if the Portal is not busy with other tasks when the RMAs contact the Portal.

```
criticalRMABuildNum    0
expectedRMABuildNum    1405
proactiveupgrade       0
```

To verify a device has the latest RMA

From the Portal, navigate to a device and select the **HPCA Management Agent**. Click the Properties icon from the toolbar to display the service properties page, which includes the **RMA Build** number.

Troubleshooting:

- Verify that the `selfmaintenance` file does *not* include a tab character or have a .txt extension; remove any tab characters or file extension.
- If the Portal detects the `selfmaintenance` file with valid entries, it executes the “RMAAutoUpgrade” job; verify the Portal log file include messages with the string "RMAAutoUpgrade".
- After the RMAAutoUpgrade job runs, the \management_agent\rma folder will contain files named `Packing.list` and `Package.info`.
- To verify the Portal is receiving registration signals from the RMA devices, review the `RMA-signals.log` file, located in the Portal’s `\logs` directory.

To disable the Portal Agent (RMA) self-maintenance feature

To turn off RMA self-maintenance, either rename or delete the `selfmaintenance` file from the `\management_agent` folder, or, set the `criticalRMABuildNum` and `expectedRMABuildNum` values to low build numbers, or 0.

Installing the Client Automation Agent

Use the Install Client Automation Agent task to install the Client Automation agents to remote devices. The Client Automation agent installation program uses the Microsoft MSI format for Windows Installer. The program consists of one MSI package, with five feature sets, one for each agent— Application Manager, Application Self-service Manager, Inventory Manager, OS Manager, and Patch Manager.

Use the Assign Proxy Assignment task prior to the Install Client Automation Agent task if you want to deploy a set of Client Automation agents from pre-assigned Proxy Servers, instead of directly from the Portal. This option allows for existing Proxy Servers in your infrastructure to handle some or all of the client deployment workload, instead of requiring the Portal to do all the work. For details, see Assigning Proxy Servers on page 269.

The Portal supports multiple client profiles. For details, see Supporting Remote Installs Using Multiple Profiles on page 266.

To install the HPCA Agents with the Portal

Be sure to read Requirements for Remote Installations on page 250 before performing this procedure.

For detailed information, such as system requirements and customization options, refer to the *Application Manager Guide and Application Self-service Manager Guide*.

1 Use the navigation aid to select the device or group of devices on which you want to install the Client Automation agents.

   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 Client Automation agents. If the Portal is not currently managing the targeted Network or LDAP devices, the Portal will bring them under management as part of the Install Client Automation Agent task.

2 From the Operations task group, click **Install Client Automation Agent**.

> 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 235 for more information.

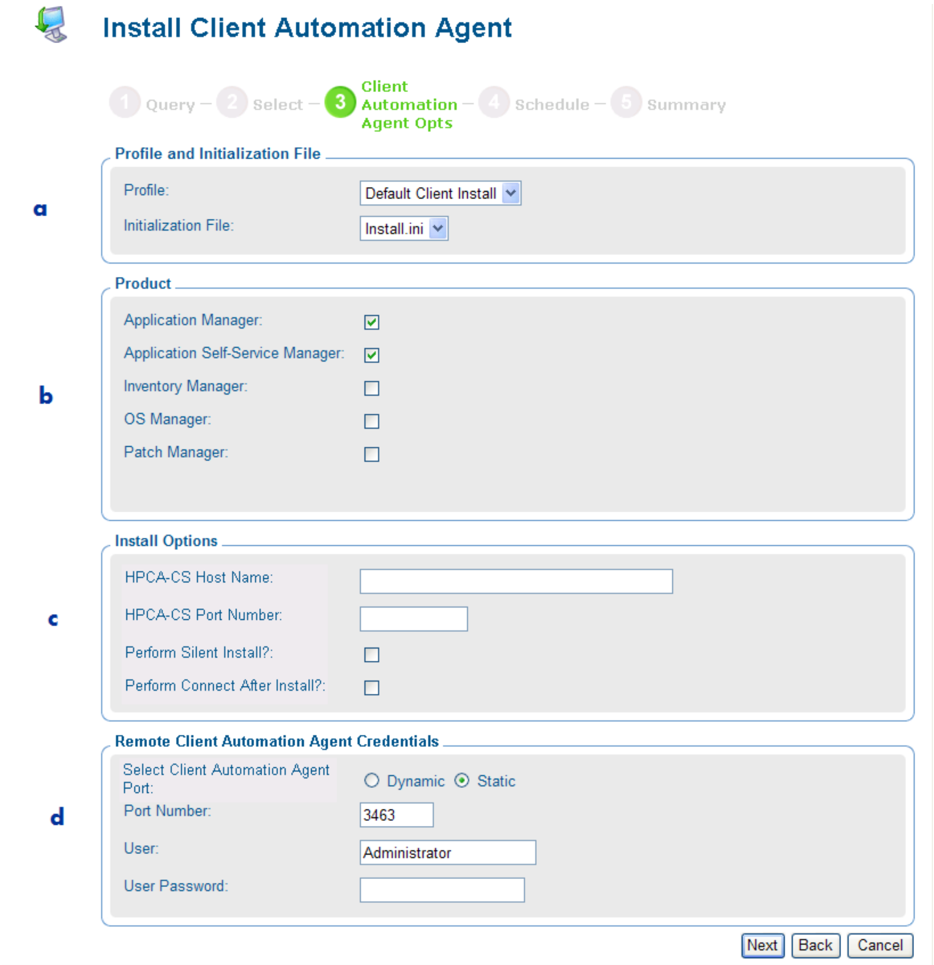
4 Click **Next**.

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 237 for more information.

6 Click **Next**.

The Client Automation Agent Opts dialog box opens.



Install Client Automation Agent

Profile and Initialization File

Profile: Default Client Install

Initialization File: Install.ini

Product

Application Manager: ☑

Application Self-Service Manager: ☑

Inventory Manager: □

OS Manager: □

Patch Manager: □

Install Options

HPCA-CS Host Name:

HPCA-CS Port Number:

Perform Silent Install?: □

Perform Connect After Install?: □

Remote Client Automation Agent Credentials

Select Client Automation Agent Port: ○ Dynamic ● Static

Port Number: 3463

User: Administrator

User Password:

Legend

a Select the Agent Install Profile.

b Select the Client Automation agents to install.

c Specify the Configuration Server parameters.

d Specify the Agent port and logon credentials for the target device.

7 From the Profile drop-down list, select a profile to use for the installation. For details on creating Agent Profiles, see Adding, Modifying, and Deleting Install Profiles on page 266.

8 In the Initialization File area, select the appropriate installation INI file from the drop-down list. This file contains parameters necessary for the

Client Automation agent to run, such as the IP address of the Configuration Server.

The Portal will honor settings placed in a customized `*.INI` file when it installs the agent.

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 **HPCA-CS Host Name** text box, type the IP address or host name that the HPCA agent will use to access the Configuration Server.

11 In the **HPCA-CS Port number** text box, type the port number that the HPCA agent will use to access the Configuration Server.

12 Select the **Perform Silent Install?** check box if you want to install an agent 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 *HPCA Application Manager and Application Self-service Manager Guide* for more information.

When the agent computer connects to the Configuration Server, the Portal also captures information about your users and stores it in the Portal Directory. See Discovering User Information on page 271 for more information.

14 Using the **Select Client Automation Agent Port** radio buttons, select whether to communicate with the Portal Agent on the agent 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 an Agent Port type of static, a Port Number text box appears.

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 238.

20 Click **Next**.

The Install Client Automation Agent—Summary dialog box opens.

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 Client Automation agents from the Portal. For example, you may want to install all agents on some computers, but only select agents on others. Or, you may want to minimize the size of the agent media package being installed, and create an agent 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 Automation Agent installation. The profile points to a code source for the product that is different from the default code source provided by Portal.

Topics in this section identify where to place the source code for Agent installation profiles, and procedures for adding, modifying, and deleting them.

Client Automation Agent Install Profiles –Source Code Required Locations

The code source needs to be placed at the following location:

`Agent Installs:` *`ManagementPortal`*`\media\client\`*`profile`*`\`*`OS`*

Where:

`ManagementPortal` is the Portal installation location

`profile` is your folder name for the install profile

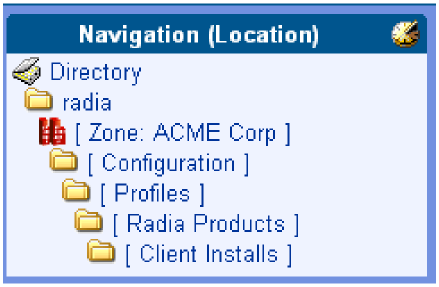
`OS` is the operating system folder name.

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 Automation Agent Install Profile

1 Navigate to the following location in the Portal.



2 Click **Add Install Profile** from the Model Administration task group.

The Add Install Profile window opens.

3 Complete the Properties for the Add Install Profile, as follows:

`Common Name` A unique name for the Install Profile object in the Portal.

`Display Name` The display name for this Install Profile in the Portal.

`Description` A full description of the source code installed by this profile.

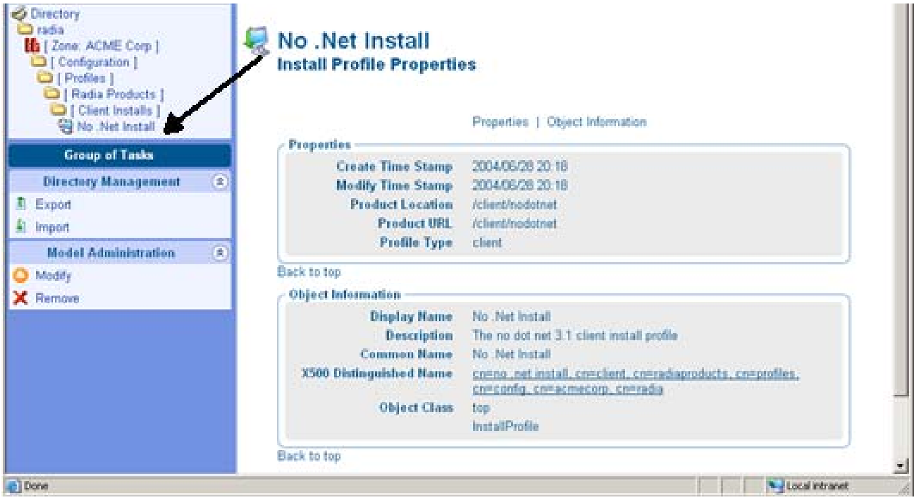
`Product Location` The directory in the base- Portal `/media/client` directory that contains the code source. Use forward slashes.

For example: `/client/nodotnet`

Below the folder specified in the Product Location must be subdirectories for each supported operating system, such as `win32`. The agent source code is located in these operating system-level folders.

4 Click **Add**.

The Properties page for the Install Profile opens. The navigation area includes the new entry for this Install profile.



No .Net Install

Install Profile Properties

Properties

Create Time Stamp	2004/06/28 20:18
Modify Time Stamp	2004/06/28 20:18
Product Location	/client/nodotnet
Product URL	/client/nodotnet
Profile Type	client

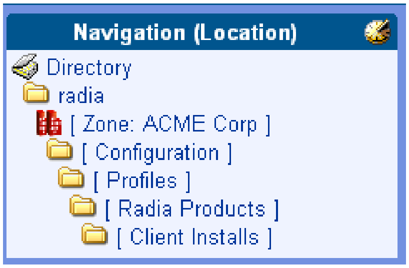
Object Information

Display Name	No .Net Install
Description	The no dot net 3.1 client install profile
Common Name	No .Net Install
X500 Distinguished Name	cn=no .net install, cn=client, cn=radiaproducts, cn=profiles, cn=config, cn=acmecorp, cn=radia
Object Class	top InstallProfile

5 Portal users will now be able to select this profile from the Options page when using the **Install** Client Automation **Agent** task.

To modify a Client Automation Agent Install Profile

1 Navigate to the where the profiles for Client Automation Agent 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**.
5. The Properties page opens, showing your modifications.

To delete a Client Automation Agent Install Profile

Deleting an install profile deletes the Portal user's ability to select this profile during the Install Client Automation Agent 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 266 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 Client Automation Agent task to schedule the installation of the agents. If a device that is scheduled for an agent installation has been assigned to a Proxy Server, the Portal will first synchronize with the Proxy Server, and then the Proxy Server will install the agent 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.

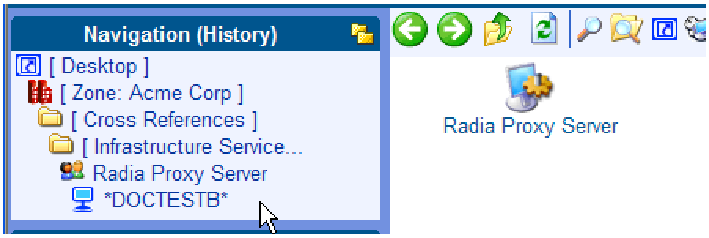
Requirements for Managing Proxy Assignments

- One or more previously installed Proxy Servers.
- For each Proxy Server, an installed Portal Agent that has also successfully discovered the Proxy Server service.

If these requirements have been met, when you navigate to a device containing the Portal Agent-discovered Proxy Server, the Proxy Server icon will display in the workspace of the Portal.

For example, the next figure shows the Proxy Server installed and discovered by the Portal Agent on the computer DOCTESTB. If you had multiple devices in your Portal zone with a Proxy Server, all would be listed in the Device Categories container. Go to the Infrastructure Services group and click on the Proxy Server container. All devices that have Portal Agents and Proxy Servers on them are automatically added to Device Categories.

Figure 28 Proxy Server discovered by the Portal 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 266.
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.
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.

6. Click **Submit** to save the proxy assignment of nodes to the selected server.
7. After completing all proxy assignments, run the **Install Client Automation Agent** task from the Operations task group of the Portal; this is discussed in the topic Installing the Client Automation Agent on page 262. If a proxy-assigned node is selected for the Client Automation agent install, the Proxy Server performs the Client Automation agent script deployment, as opposed to the Portal.

Discovering User Information using Managed Services

The Portal can be enabled to capture information about your users and store it in the Portal directory. In the Device Categories container, there is a group named Managed Services. The information about users is used to create automatic groups for each service being managed by Client Automation Software for your users.

HPCA Services will appear in the Device Categories container as long as:

- Agent reported objects have been enabled for posting to the Portal. For more information, see Posting Agent Objects to the Portal on page 37.
- Application Event reporting is turned on for the services being installed.
- An agent has installed at least one service.

When the Client Automation agent computers connect to the Configuration Server, information is captured from the agent reporting objects, and then the Messaging Server routes the appropriate agent objects, such as APPEVENT, to the Portal. Refer to the *HP Client Automation Enterprise Messaging Server Installation and Configuration Guide* for more information on how to install and configure the Messaging Service to route messages to the Portal.

To view Client Automation-Managed Services information

1. Navigate to the **Zone** → **Device Categories** container.
2. Select **Managed Services**.

   The Managed Services container includes groups of devices for which the Configuration Server has reported Client Automation-managed applications.

3 In the workspace, you will see one or more groups, each representing the name of a service being managed by Client Automation on devices in this Portal Zone.

4 Click on a group in the Managed Services container to see all Zone devices for which Client Automation is managing that service.

Installing the Proxy Server

Use the **Install Proxy Server** task to install the 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 *HP* Client Automation *Proxy Server Installation and Configuration Guide* for more information.

See Preparing and Locating Configuration Files for Proxy Server Installs on page 275 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 250 before performing this procedure.
>
> You may also want to check the HP Support 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.

> You can select one or more devices from a location in your Zone, a Networks container, or an LDAP directory. If the Portal is not currently managing the targeted Network or LDAP devices, the 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 235 for more information.

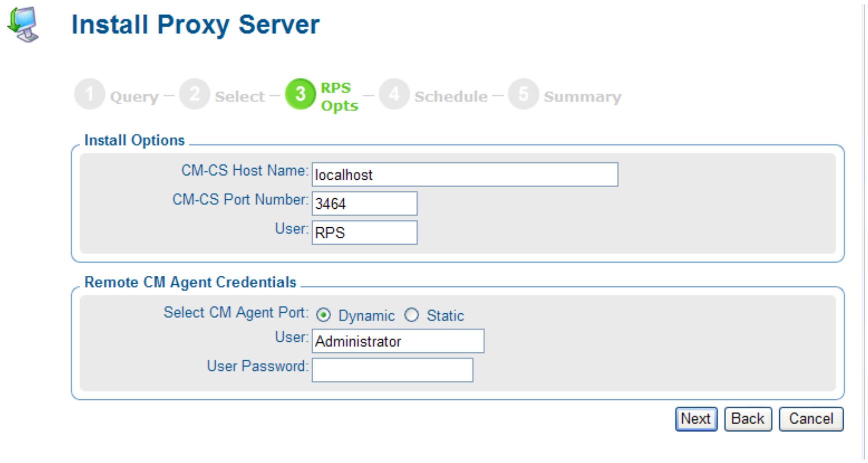
4 Click **Next**.

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 237 for more information.

6 Click **Next**.

The Install Proxy Server—RPS Options dialog box opens.



Install Proxy Server

Install Options

CM-CS Host Name: localhost

CM-CS Port Number: 3464

User: RPS

Remote CM Agent Credentials

Select CM Agent Port: ● Dynamic ○ Static

User: Administrator

User Password:

7 In the Configuration Server Host Name text box, type the name or IP address for the Configuration Server.

8 In the Configuration Server Port Number, type the port number for the Configuration Server.

9 In the User text box for Install Options, type the user ID to use to connect to the Configuration Server.

10 If available, select which Proxy Server 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 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 275.

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.

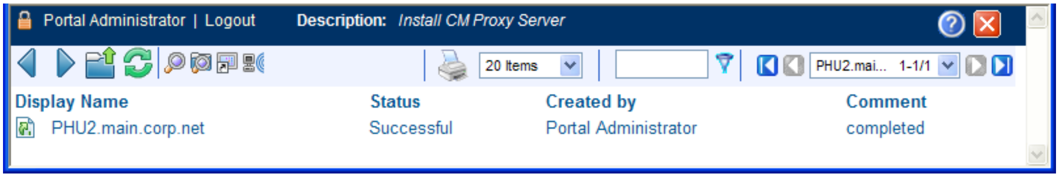
14 In the Schedule dialog box, specify when you want this job to run. For more information, see Scheduling Jobs on page 238.

15 Click **Next**.

   The Install Proxy Server—Summary dialog box opens.

   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.



Portal Administrator | Logout   **Description:** *Install CM Proxy Server*

20 Items   PHU2.mai... 1-1/1

Display Name	Status	Created by	Comment
PHU2.main.corp.net	Successful	Portal Administrator	completed

— 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.

12 When you are done viewing the job status, click ☒ to close the Job Status page, and return to the 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 Portal to use them. When you run the Install Proxy Server task from the 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 Portal media directory.

The appropriate location of a configured rps.cfg file will indicate Win32; the platform on which you are installing the Proxy Server. For example, the location for a Windows Proxy Server installation is similar to this:

```
C:\Program Files\Hewlett-Packard\
CM\ManagementPortal\media\extended_infrastructure\
proxy_server\win32\media\etc
```

a Go to the directory where the Portal is installed.

The default is

```
SystemDrive:\Program Files\Hewlett-Packard\
CM\ManagementPortal
```

b Go to the following folder location in the Portal directory:

```
\media\extended_infrastructure\proxy_server\<platform>\m
edia
```

where *<platform>* is win32 for a Windows platform.

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 Portal is installed on C:\Program

`Files\Hewlett-Packard\CM\ManagementPortal`, and the Proxy Server will be installed on a Windows platform, then place the `rps.cfg` file in the following location: `C:\Program Files\Hewlett-Packard\CM\ManagementPortal\media\extended_infrastructure\proxy_server\win32\media\etc`

3 Run the Install Proxy Server task from the 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 Portal Agent installed, the rps service is automatically discovered.
- For devices that do not have a Portal Agent installed, you can manually add a service for the Proxy Server to enable the task. For details, refer to Adding Services on page 170.

See the *HP Client Automation Enterprise 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 Servers 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 Portal Agents in a Zone at once, navigate to the Proxy Server group in the **Zone → Device Categories→ 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 238.

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 222 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.

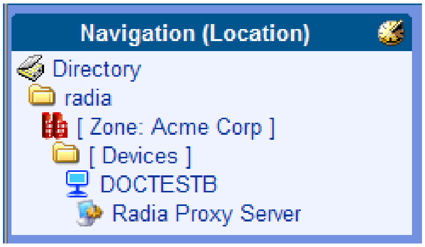
- For devices that have a Portal Agent installed, a Proxy Server service is automatically discovered. Once discovered, it will be listed in the Zone's Device Categories Container within the Infrastructure Services group for Proxy Servers.
- For devices that do not have a Portal Agent installed, you can manually add a service for the Proxy Server to enable the task. For details, refer to Adding Services on page 170.

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.

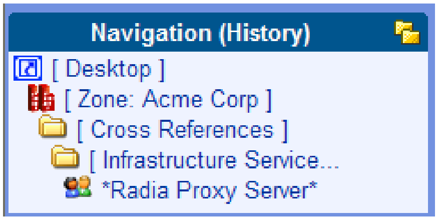
— To purge the dynamic cache of an individual Proxy Server, navigate to the device's properties from a Group or Device container, and select the service for the Proxy Server. The following figure shows a sample location of a Proxy Server on a single device:



Navigation (Location)

- Directory
  - radia
    - [Zone: Acme Corp]
      - [Devices]
        - DOCTESTB
          - Radia Proxy Server

— To purge the dynamic cache of all Proxy Servers identified by the Portal Agents in a zone at once, navigate to the Proxy Server group. This group is located in the **Zone** → **Device Categories**→ **Infrastructure Services** container, as shown in the following figure.



Navigation (History)

- [Desktop]
  - [Zone: Acme Corp]
    - [Cross References]
      - [Infrastructure Service...
        - *Radia Proxy Server*

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 238.

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 222 for more information.

Managing Services

Use the 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 Device Categories → Infrastructure Services container.

Selecting the Device, then select the Service.

2 In the Operations task group, click the appropriate action.

— Click **Pause** to temporarily stop 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 Portal 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 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.

2 In the Operations task group, click **Add Task Template**.

The Add Task Template options page opens.

3 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.

4 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 do not 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*".

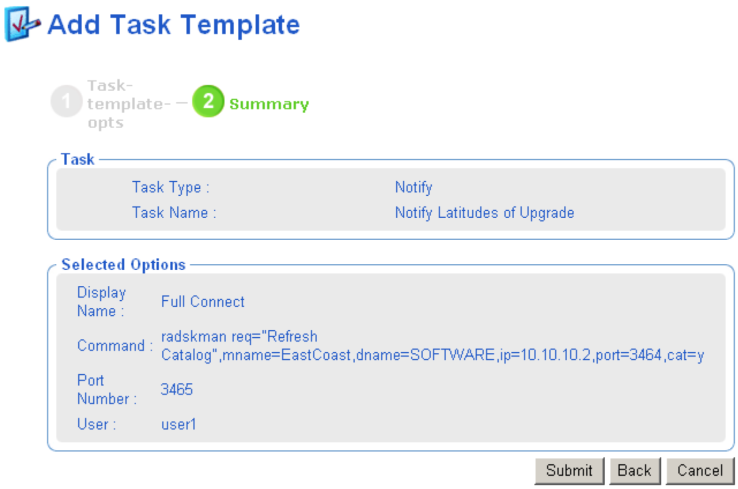
5 Complete the options for the task you selected. For details, refer to the appropriate topics:

— To complete notify tasks, see Using the Notify Tasks on page 240.

— To complete Install Proxy tasks, see Installing the Proxy Server on page 272.

6 Click **Next**.

The Add Task Template Summary page opens.



Add Task Template

Task

Task Type : Notify

Task Name : Notify Latitudes of Upgrade

Selected Options

Display Name : Full Connect

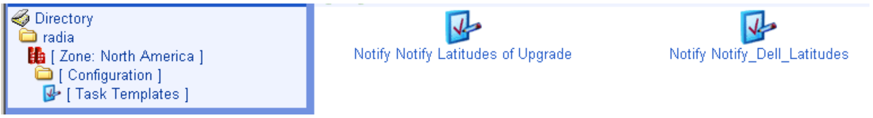
Command : radskman req="Refresh Catalog",mname=EastCoast,dname=SOFTWARE,ip=10.10.10.2,port=3464,cat=y

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.

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.

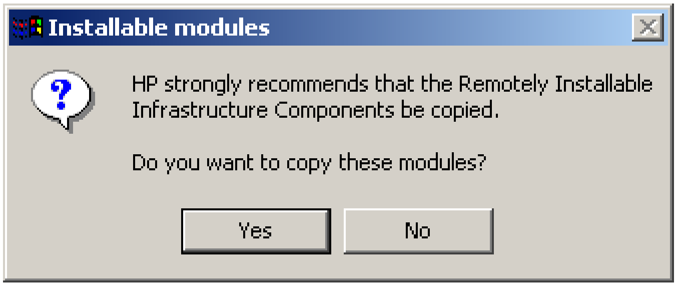
The task template and its options are removed from the Portal Directory.

Installing Additional Portal Zones (Subordinate Zones)

Once your initial Portal zone is installed, you can use the Portal to remotely install additional Portal zones in your enterprise. These zones are called subordinate zones.

Prerequisite for Install Portal task

- The media that is needed to run the Install Portal task must be stored in the Portal's `\media` directory, in a structure that mirrors the original Portal installation media.
- The Portal installation program, `setup.exe`, automatically copies the needed files to the appropriate locations when you select **Yes** to the following prompt:



Installable modules

HP strongly recommends that the Remotely Installable Infrastructure Components be copied.

Do you want to copy these modules?

- To verify that your Portal includes the needed install media, you can check that the following directory structure exists:

```
<<CM_Portal_install_directory>>\media\extended_infrastructure\
management_portal\<platform>\
```

- Below each `<platform>` directory will be subdirectories for `\media\modules`. A copy of your `license.nvd` file must exist in the `<platform>\media\modules` directory.

If the needed directory structure and files are missing, just rerun the `setup.exe` program and elect to update the installable components. When prompted to copy the Remotely Installable Infrastructure Components, choose **Yes**. See Installation Procedures on page 30 for more information.

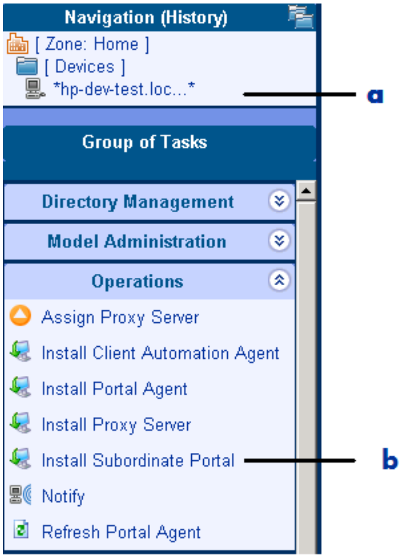
To install a Portal Zone from the Master Zone

1 Login to the Master Zone Portal as **`Admin`**.

2 The device on which you are installing the 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 156.) After adding the device, navigate to and display the Device Properties.



Legend

a Locate device.

b Select Install Subordinate Portal.

3 Click **Install Subordinate Portal** in the Operations task group to install a subordinate zone onto the selected device.

The RMP – Opts panel of the Install Subordinate Portal page opens (Step 3 of 5). Complete the Zone Options and Remote Client Automation Agent Credentials using the following information.

Table 24 Zone Options for the Install Subordinate Portal task

Field	Example	Description
Zone Name	Chicago	Zone name becomes the high-level qualifier for all nodes in this Portal 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 Portal. **Note:** Use onlyASCII characters in this field.
RIS Port	3466	The port number of the Subordinate Zone - Portal service. Select an available port on the target device for the Portal. Default is 3466.
RIS Install Directory	`C:/Program Files/Hewlett-Packard/CM/ManagementPortal`	The base directory for the Portal on the remote device. Important: Use *forward* slashes for both Windows and UNIX path syntax.

RIS Service Name Suffix	Chi	Optional entry. If used, this suffix is appended to the Portal Service name, `httpd-managementportal`, to allow for a distinct entry.
		If a suffix is entered, the 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 Portal service with this suffix, the Portal install only continues if the above /ManagementPortal directory is empty.
		Note: If you enter a suffix, then append this suffix to the `httpd-managementportal` entry when you start or stop the Portal from a command line. For example:
		`nvdkit start httpd-managementportalChi.tkd`
		`nvdkit stop  httpd-managementportalChi.tkd`

Zone Port	3474	Listening Port for the Subordinate Zone OpenLDAP directory. Default is 3474.
Zone Backup Port	3475	When backup is enabled, this is the required listening port for the backup of the Subordinate Zone OpenLDAP directory. Default is 3475.

Field	Example	Description
Enable Backup	1	Set to 1 to enable the Portal Backup Directory task and the resources it needs to create a backup of the OpenLDAP Database. The Backup Directory task uses the Listening Port for OpenLDAP Backup. Default is 1. or Set to 0 disable the Portal Backup Directory task. This option is not recommended unless alternate database replication or backup processes are being used in your environment.

Table 25 Remote HPCA Agent Credentials for the Install Subordinate Portal task

Field	Example	Description
Select Client Automation Agent Port	Select Dynamic or Select Static	Port for the Portal Agent on the Subordinate Portal. 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 Automation Agent Port is set to Static, a Port Number field allows you to specify the Client Automation Agent Port number to use.
User	Administrator	A 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**.

The Schedule panel (Step 4 of 5) of the Install Subordinate Portal page opens. The default schedule is to run the 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 Subordinate Portal page opens, as shown in the following figure.

6. Review all entries are as desired, and then click **Submit**.

   A job summary window opens for the Install Subordinate Portal 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 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.

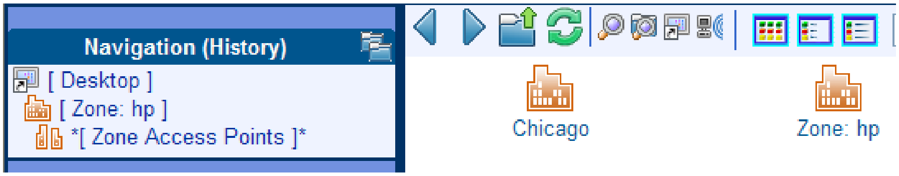
Updating Subordinate Portal Zones

After you install an update to the Master Portal for a service pack or release, use the Update Subordinate 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 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 Subordinate 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 Portal Zones at once, click **Update Subordinate Portal** from the Operations task group.

or

To update a single zone, select the individual Zone object and click **Update Subordinate 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 Portal 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 Portal Agent on page 252 for more information.

Scheduling Zone Operations

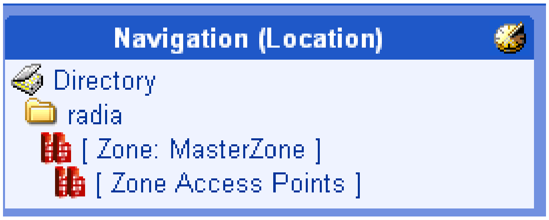
Scheduling Zone Operations using the ZoneJob task requires you to have the following objects in your zone directory:

- Zones in the Zones Access Points container. When you use the Install Subordinate 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 73.
- Task Templates for the job being scheduled. For details, see Managing Task Templates on page 279.
- 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 Device Categories 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 Device Categories container, make sure the devices in your zones have the Portal 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.



Navigation (Location)

Directory

radia

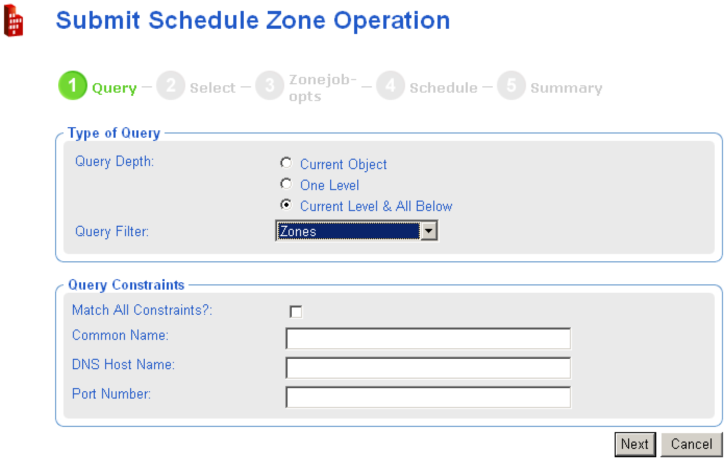
[Zone: MasterZone]

[Zone Access Points]

You may want to add the Zone Access Points container to your desktop. To do this, navigate to the Zone Access Points container and click the Add Shortcut icon 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: Zones

Query Constraints

Match All Constraints?: □

Common Name:

DNS Host Name:

Port Number:

3 To view and then select from all available zones, click **Next**.

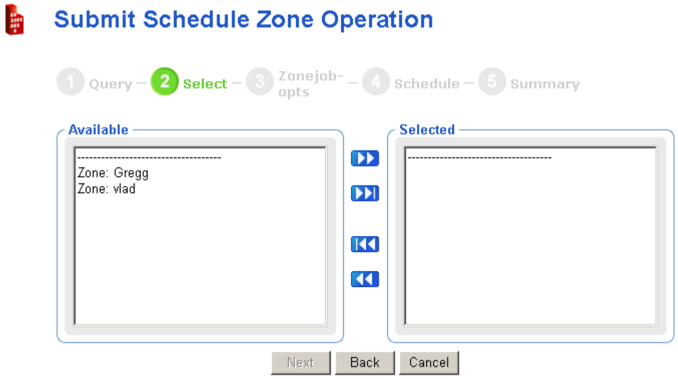
or

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**.

If there is only one zone meeting your Query constraints, skip to Step 6.

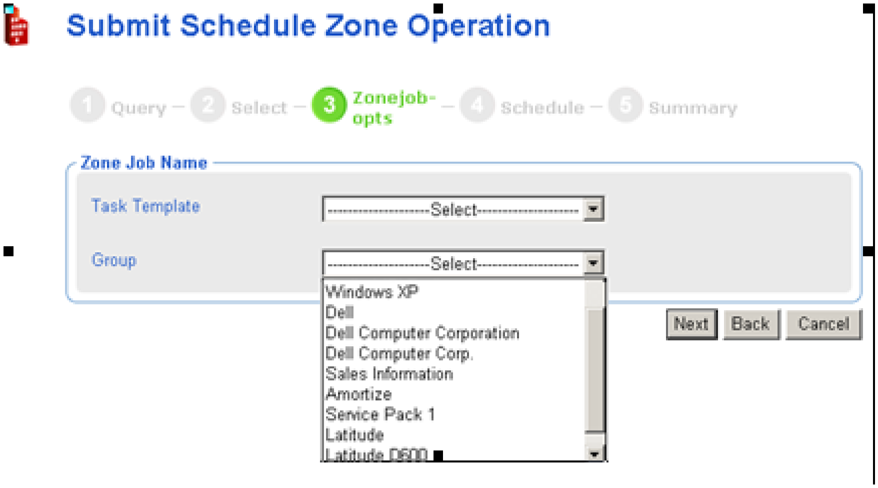
If there is more than one zone meeting your Query constraints, the Submit Schedule Zone Operation – Select window opens. The Zones meeting your query constraints are listed in the Available column.

4 Move the zones for the job to be scheduled to the Selected column using the Arrow icons, or, by double-clicking on an entry.



5 Click **Next** to schedule the job against the zones listed in the Selected column.

The Submit Schedule Zone Operation – ZoneJob opts window opens.



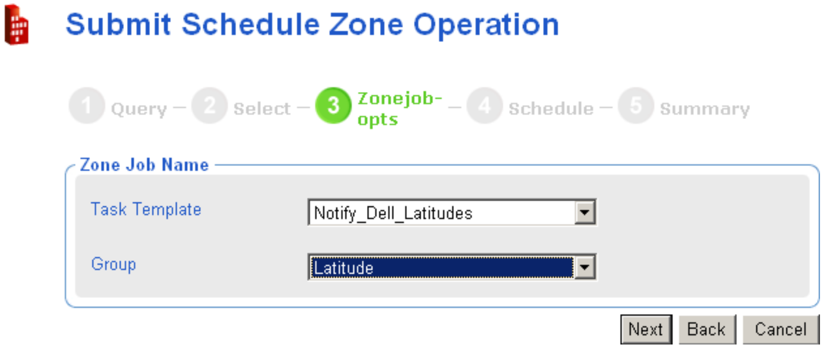
6 Use the Zone Job Name group fields to select the task template and the Group of Devices for the scheduled zone jobs. The task template defines the job type and options to be scheduled (the WHAT). The group represents the group of devices to which the job is to apply (WHICH objects in the selected zones).

- Select a task template from the drop-down list. The list represents the task templates that have been entered in the Task Template container at the Directory level of the Portal.
- Click the **Group** drop-down list to select one of the groups of devices. The list represents the self-managed groups in the Device Categories container as well as the groups created in the Zone Groups container.

  The Device Categories 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 Device Categories groups.



Submit Schedule Zone Operation

Zone Job Name

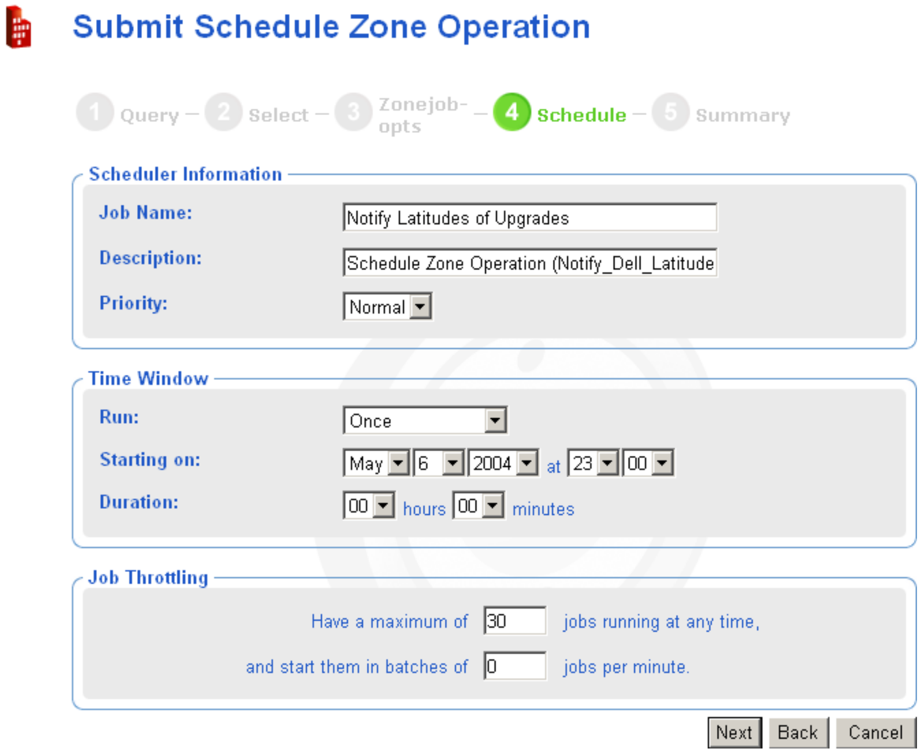
Task Template: Notify_Dell_Latitudes

Group: Latitude

1 Query – 2 Select – 3 Zonejob-opts – 4 Schedule – 5 Summary
Next
Back
Cancel

7 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: Notify Latitudes of Upgrades

Description: Schedule Zone Operation (Notify_Dell_Latitude

Priority: Normal

Time Window

Run: Once

Starting on: May 6 2004 at 23 00

Duration: 00 hours 00 minutes

Job Throttling

Have a maximum of 30 jobs running at any time,

and start them in batches of 0 jobs per minute.

8 In the Scheduler Information area, enter a Job Name, such as `Notify Latitudes of Upgrades`. If desired, modify the Description and Priority.

9 In the Time Window area, use the Run drop-down box to select a frequency for the zone operation job. Complete the schedule options the same as for any other job.

> You can select **Do Not Schedule** to save the Job and select the Job for use in the Sequence Tasks operation.

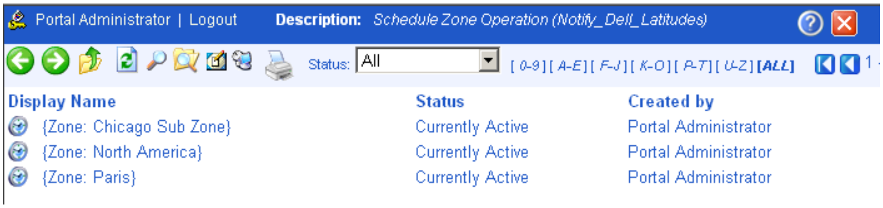
10 In the Job Throttling area, enter the maximum jobs to run at any time, and how many can run per minute. The throttling options apply to each zone from which the jobs will run.

11 Click **Next** to review the summary and submit the job.

The Submit Schedule Zone Operation – Summary window opens.

12 Click **Submit** to submit the job for the selected zones.

13 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.



Portal Administrator | Logout **Description:** *Schedule Zone Operation (Notify_Dell_Latitudes)*

Status: All [0-9] [A-E] [F-J] [K-O] [P-T] [U-Z] **[ALL]** 1

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

14 To View Job Properties for any of these zone jobs, click on the job listing, then click on the View Properties toolbar icon 🔍.

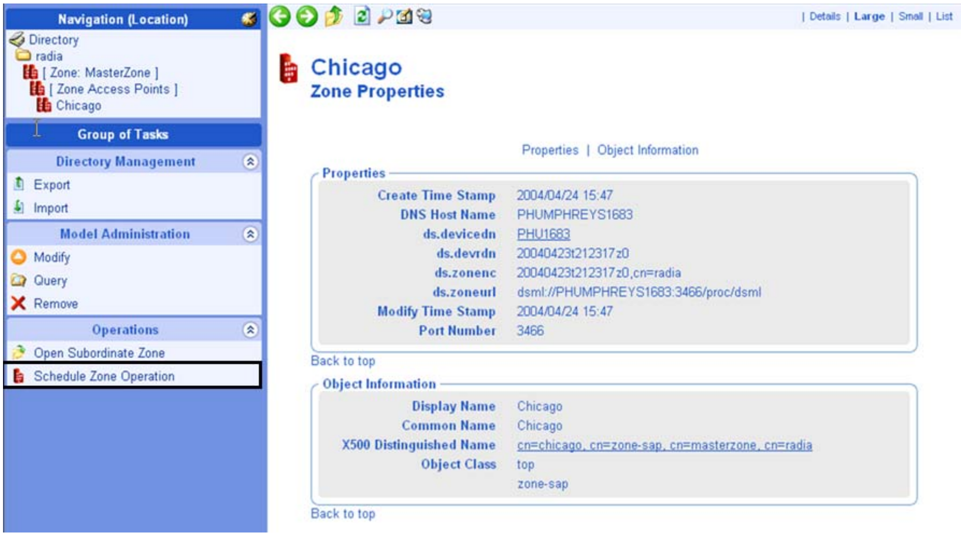
What happens with jobs scheduled from Remote Zone Operations?

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.



Chicago
Zone Properties

Properties

Create Time Stamp	2004/04/24 15:47
DNS Host Name	PHUMPHREYS1683
ds.devicedn	PHU1683
ds.devrdn	20040423t212317z0
ds.zonenc	20040423t212317z0,cn=radia
ds.zoneurl	dsml://PHUMPHREYS1683:3466/proc/dsml
Modify Time Stamp	2004/04/24 15:47
Port Number	3466

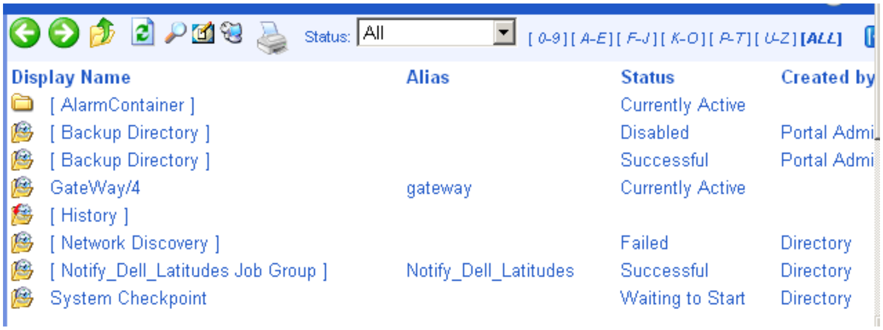
Object Information

Display Name	Chicago
Common Name	Chicago
X500 Distinguished Name	cn=chicago, cn=zone-sap, cn=masterzone, cn=radia
Object Class	top zone-sap

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.

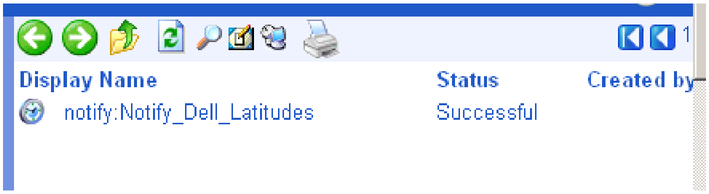
Navigate to the **Zone** → **Jobs** container to see jobs launched from another Portal.

In the following sample figures, the Job Name Scheduled for Zone Operations is Notify Dell Latitudes. The zone audience included the Zone of Chicago.



Display Name	Alias	Status	Created by
[AlarmContainer]		Currently Active	
[Backup Directory]		Disabled	Portal Admi
[Backup Directory]		Successful	Portal Admi
GateWay/4	gateway	Currently Active	
[History]			
[Network Discovery]		Failed	Directory
[Notify_Dell_Latitudes Job Group]	Notify_Dell_Latitudes	Successful	Directory
System Checkpoint		Waiting to Start	Directory

Select the [**Notify Dell Latitudes Job Group**] to see the Job details.

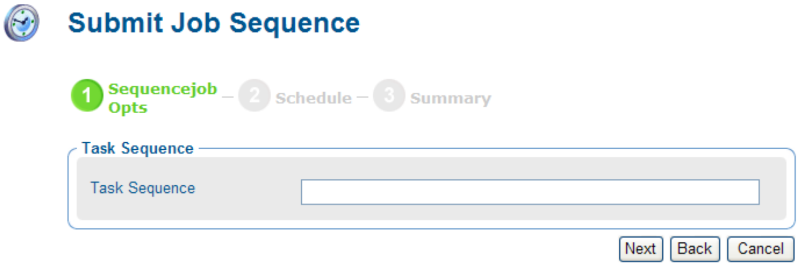


Display Name	Status	Created by
notify:Notify_Dell_Latitudes	Successful	

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:

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}* Agent 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 Agents Only)

Use Remote Control to manage Client Automation agents running on a supported Windows platform with TightVNC: Enhanced VNC Distribution through the Portal. TightVNC: Enhanced VNC Distribution is a freely re-distributable solution that allows you to control Client Automation agents 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 2000 or above.
- The Portal Agent must be installed on the remote device.
- A Web browser that supports and has Java applets installed.

Prerequisites

- Ability to use the CSDB Editor.
- Ability to distribute applications (with the Client Automation agent or using a notify operation).
- In the ZSERVICE class of the Configuration Server DB, 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 CM. Some examples of ways to do this are to use the Client Automation agent or the Notify task in the Portal.

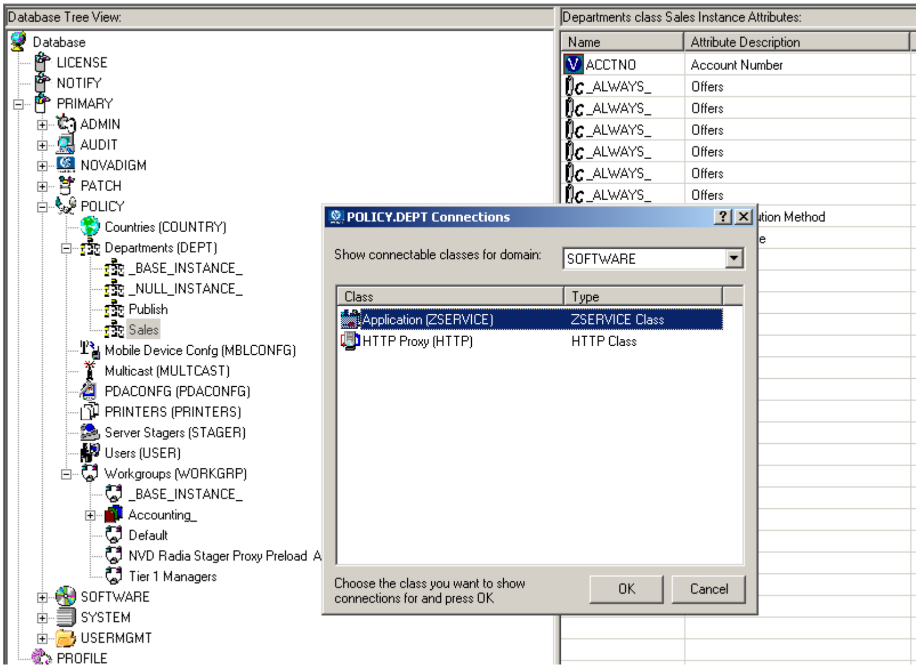
Connecting the Remote Control Service to Users

Use the CSDB Editor to connect the Remote Control Service to the appropriate users, servers, or groups, representing the devices to be managed by CM. 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 CSDB Editor to the PRIMARY.POLICY Domain.
2. Navigate to the appropriate DEPT, USER, or WORKGRP 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.



Database Tree View:

- Database
  - LICENSE
  - NOTIFY
  - PRIMARY
    - ADMIN
    - AUDIT
    - NOVADIGM
    - PATCH
    - POLICY
      - Countries (COUNTRY)
      - Departments (DEPT)
        - _BASE_INSTANCE_
        - _NULL_INSTANCE_
        - Publish
        - Sales
      - Mobile Device Confg (MBLCONFG)
      - Multicast (MULTCAST)
      - PDACONFG (PDACONFG)
      - PRINTERS (PRINTERS)
      - Server Stagers (STAGER)
      - Users (USER)
      - Workgroups (WORKGRP)
        - _BASE_INSTANCE_
        - Accounting_
        - Default
        - NVD Radia Stager Proxy Preload A
        - Tier 1 Managers
    - SOFTWARE
    - SYSTEM
    - USERMGMT
  - PROFILE

Departments class Sales Instance Attributes:

Name	Attribute Description
ACCTNO	Account Number
ALWAYS	Offers
ALWAYS	Offers
ALWAYS	Offers
ALWAYS	Offers
ALWAYS	Offers
ALWAYS	Offers
	tion Method
	e

POLICY.DEPT Connections

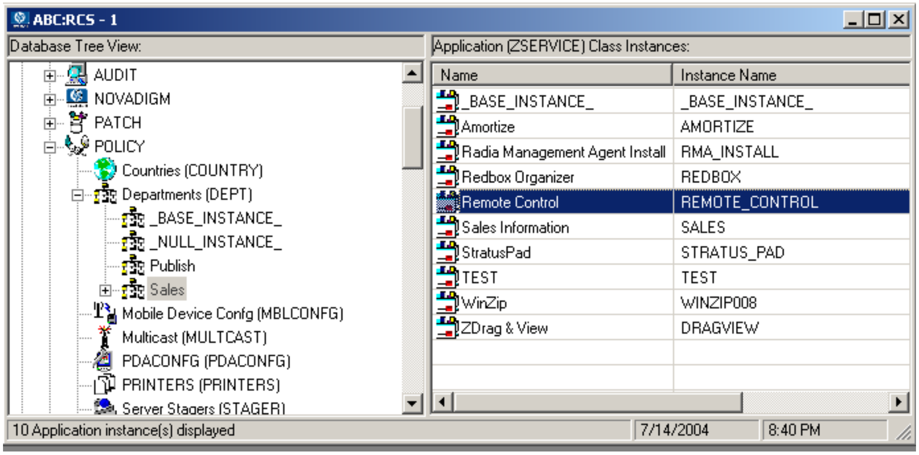
Show connectable classes for domain: SOFTWARE

Class	Type
Application (ZSERVICE)	ZSERVICE Class
HTTP Proxy (HTTP)	HTTP Class

Choose the class you want to show connections for and press OK

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.



ABC:RCS - 1

Database Tree View:

- AUDIT
- NOVADIGM
- PATCH
- POLICY
  - Countries (COUNTRY)
  - Departments (DEPT)
    - _BASE_INSTANCE_
    - _NULL_INSTANCE_
    - Publish
    - Sales
  - Mobile Device Confg (MBLCONFG)
  - Multicast (MULTCAST)
  - PDACONFG (PDACONFG)
  - PRINTERS (PRINTERS)
  - Server Stagers (STAGER)

Application (ZSERVICE) Class Instances:

Name	Instance Name
_BASE_INSTANCE_	_BASE_INSTANCE_
Amortize	AMORTIZE
Radia Management Agent Install	RMA_INSTALL
Redbox Organizer	REDBOX
Remote Control	REMOTE_CONTROL
Sales Information	SALES
StratusPad	STRATUS_PAD
TEST	TEST
WinZip	WINZIP008
ZDrag & View	DRAGVIEW

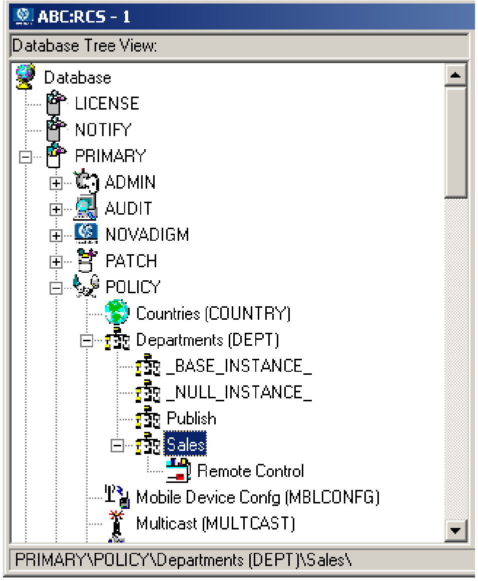
10 Application instance(s) displayed | 7/14/2004 | 8:40 PM

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 Client Automation agent or the Notify task.

Using Remote Control (*Windows Clients Only*)

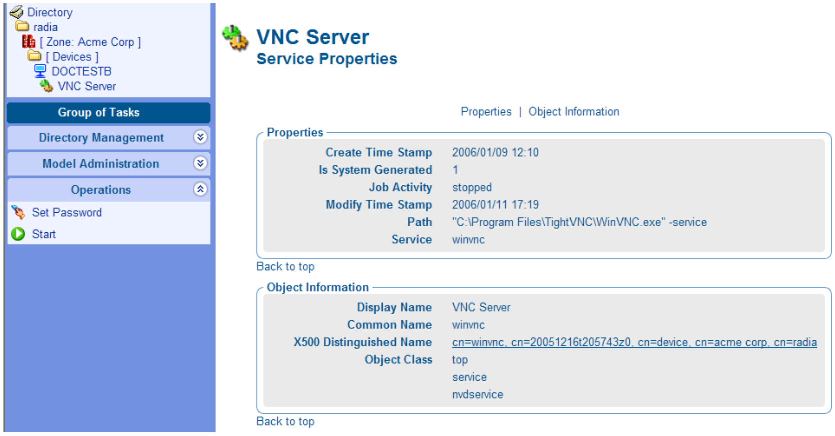
After using the Client Automation agent or the Notify task to distribute the Remote Control service to the remote device, you can use Remote Control to manage the Client Automation agents using TightVNC.

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.



VNC Server
Service Properties

Properties | Object Information

Properties

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
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

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.

4 In the User Password text box, type the password for the VNC session.

5 Click **Submit**.

The VNC Properties Service dialog box opens.

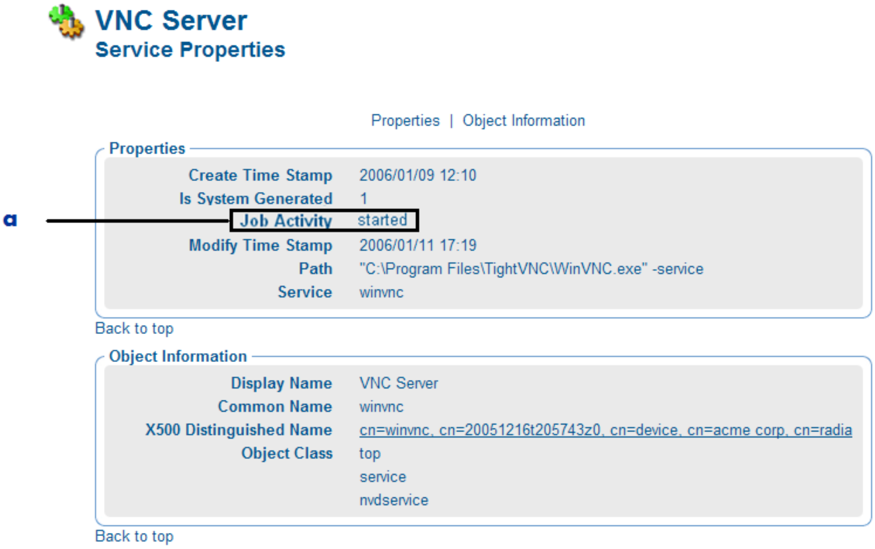
6 In the Operations task list, click **Start** to start the VNC server.

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 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.

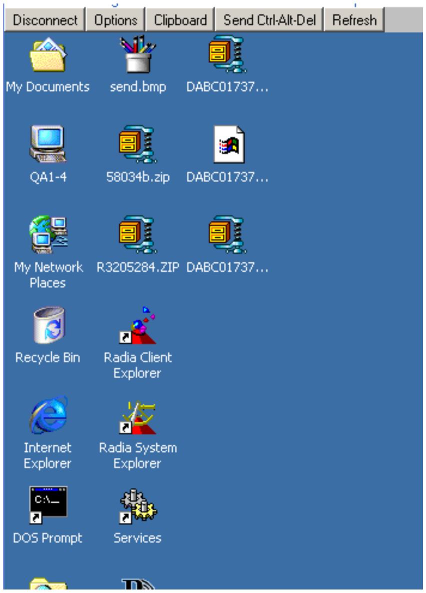
> If your web browser does not support Java applets, you may see this message "Refresh this Page for Remote Authentication Prompt". Be sure to install the Java component.

9 In the Password text box, type the password for the VNC session.

10 Click **OK**.

Now, you can control the Client Automation agent 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 Portal. For details, see the topic Customizing the Start Viewer Task Properties on page 300.



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 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

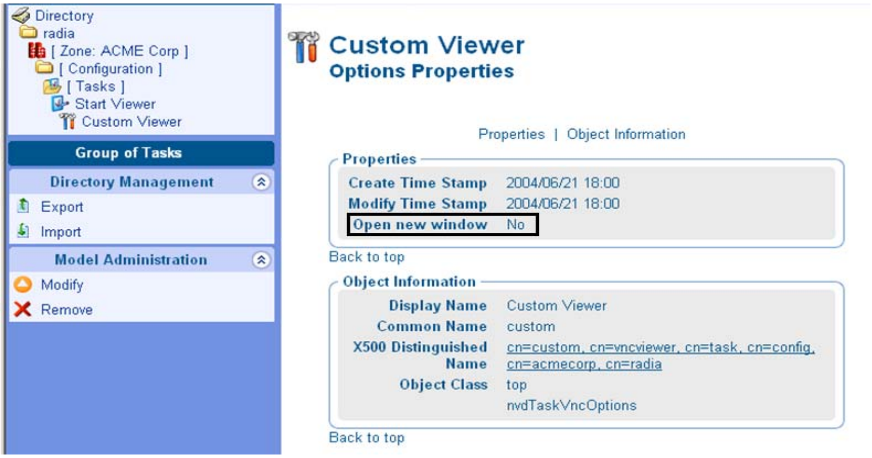
You can customize the Start Viewer task of the Portal to display the remote session in a new window, as opposed to displaying the remote session within the Portal workspace area (the default). To do this you will modify the Start Viewer task from the Portal before you begin the VNC session.

To customize the Start Viewer Task from the 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.



Custom Viewer

Options Properties

Properties

Create Time Stamp	2004/06/21 18:00
Modify Time Stamp	2004/06/21 18:00
Open new window	No

Back to top

Object Information

Display Name	Custom Viewer
Common Name	custom
X500 Distinguished Name	cn=custom, cn=vncviewer, cn=task, cn=config, cn=acmecorp, cn=radia
Object Class	top nvdTaskVncOptions

Back to top

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 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.

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 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 Configuration Server DB Editor.

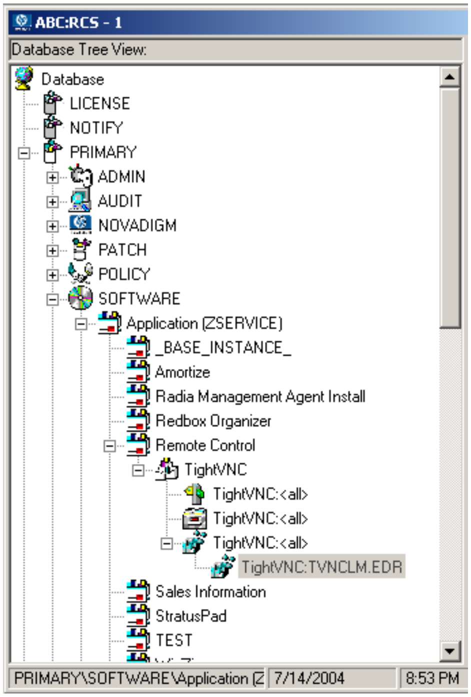
To configure remote control parameters

1 Go to **Start** → **Programs** → **HP Client Automation Administrator** → **Client Automation Admin CSDB Editor**.

2 In the 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).



ABC:RCS - 1

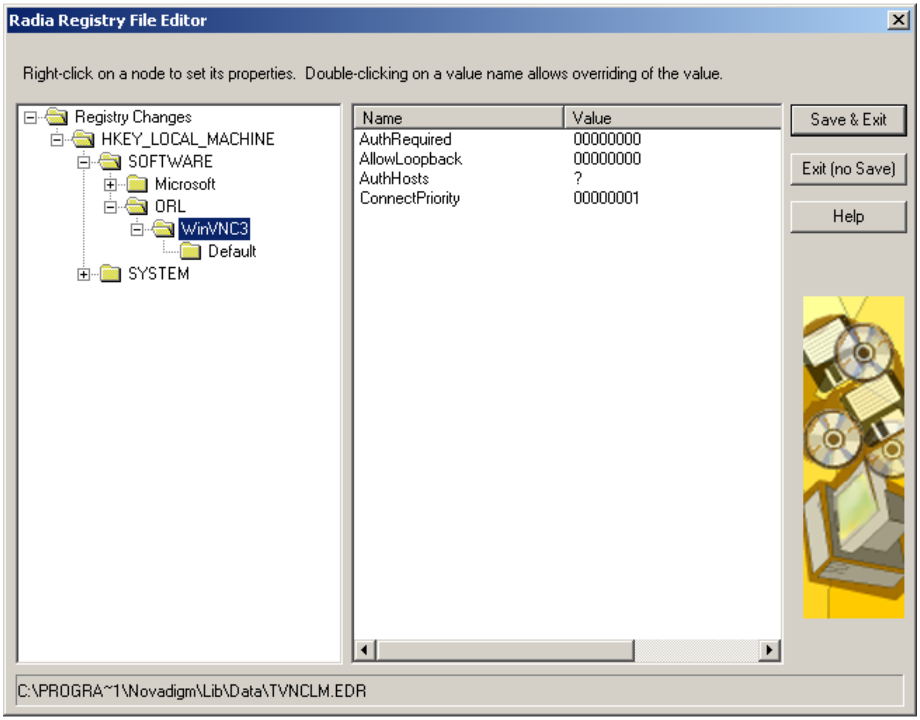
Database Tree View:

- Database
  - LICENSE
  - NOTIFY
  - PRIMARY
    - ADMIN
    - AUDIT
    - NOVADIGM
    - PATCH
    - POLICY
    - SOFTWARE
      - Application (ZSERVICE)
        - _BASE_INSTANCE_
        - Amortize
        - Radia Management Agent Install
        - Redbox Organizer
        - Remote Control
          - TightVNC
            - TightVNC:<all>
            - TightVNC:<all>
            - TightVNC:<all>
              - TightVNC:TVNCLM.EDR
        - Sales Information
        - StratusPad
        - TEST

PRIMARY\SOFTWARE\Application (Z | 7/14/2004 | 8:53 PM

5 Right-click **TightVNC:TVNCLM.EDR** and select **Edit Registry Resource**.

6 Navigate to WinVNC3 to view the local machine-specific settings.



Radia Registry File Editor
Right-click on a node to set its properties. Double-clicking on a value name allows overriding of the value.
Registry Changes
HKEY_LOCAL_MACHINE
SOFTWARE
Microsoft
ORL
WinVNC3
Default
SYSTEM
Save & Exit
Exit (no Save)
Help
C:\PROGRA~1\Novadigm\Lib\Data\TVNCLM.EDR

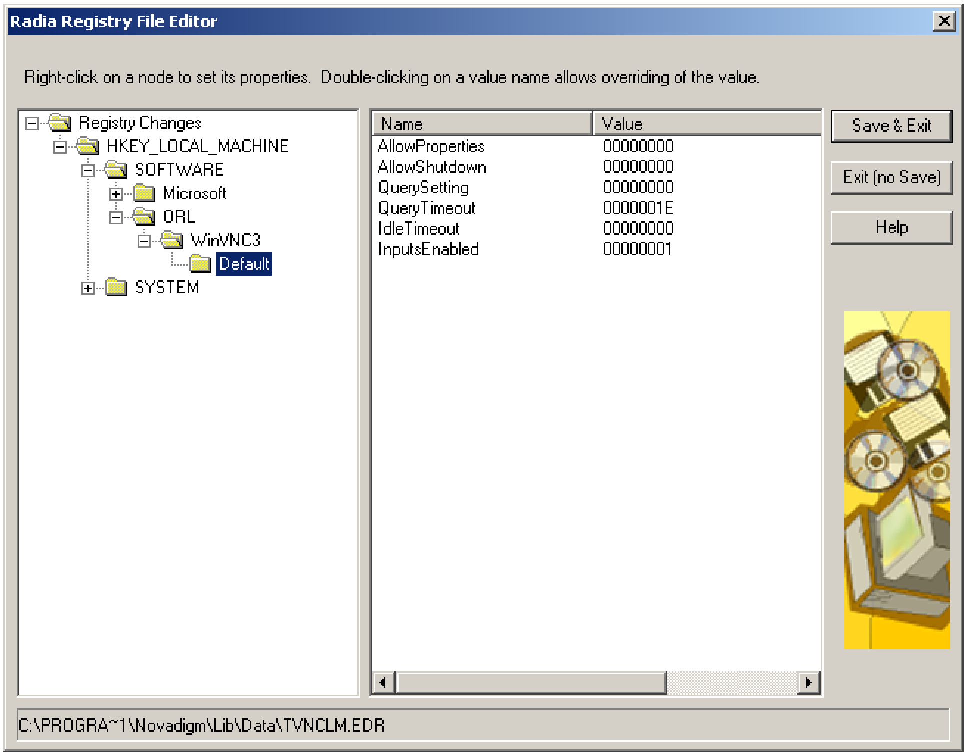
Name	Value
AuthRequired	00000000
AllowLoopback	00000000
AuthHosts	?
ConnectPriority	00000001

Table 26 Local Machine-Specific Settings for TightVNC Service

Field	Description
AuthRequired	Set AuthRequired = 1 (default) to ensure that a password is set when you start the service. Set AuthRequired = 0 to disable null password checking by WinVNC. Use DWorD format.
AllowLoopback	Set AllowLoopback = 0 to disable the ability to remote control the local machine. Set AllowLoopback = 1 to allow the ability to remote control the local machine. Use DWorD format.

Field	Description
AuthHosts	Specifies a set of IP address templates that incoming connections must match in order to be accepted. By default, the template is empty and connections from all hosts are accepted. Three settings are available: - IP address – Specifies a range of IP addresses that are not authorized to connect ? IP address – Specifies a range of IP addresses that you want to be prompted for + IP address – Specifies a range of IP addresses that are authorized to connect Example: +192.10,-192.10.12 This parameter is used in conjunction with the QuerySettings parameter. Use STRING format.
ConnectPriority	By default, the TightVNC server disconnects existing connections when a non-shared connection authenticates. You can change this behavior by setting this value to: 0 - to disconnect all existing connections 1 - to continue all existing connections. 2 - to refuse any new connections. Use DWorD format.

7 Click **Default** to see the local default user properties that you can set.



Right-click on a node to set its properties. Double-clicking on a value name allows overriding of the value.

```
Registry Changes
  HKEY_LOCAL_MACHINE
    SOFTWARE
      Microsoft
      ORL
        WinVNC3
          Default
    SYSTEM
```

Name	Value
AllowProperties	00000000
AllowShutdown	00000000
QuerySetting	00000000
QueryTimeout	0000001E
IdleTimeout	00000000
InputsEnabled	00000001

C:\PROGRA~1\Novadigm\Lib\Data\TVNCLM.EDR

Table 27 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	Sets whether you want to prompt the user about an incoming connection. This setting must be used in conjunction with AuthHosts. Set this value to: 0 or 1 – Does not prompt on incoming connection. 2 – Prompts on incoming connection (default). Use DWorD format.
QueryTimeout	Specifies how long (in seconds) the prompt panel appears to the user when you begin a remote control session. This panel prompts the user to accept the session. Use DWorD format.
IdleTimeout	Indicates how long (in seconds) a VNC client can remain idle for before being disconnected. If this is blank or set to 0, a timeout is not enforced. Use DWorD format.
InputsEnabled	Allows incoming connections to send input. If InputsEnabled = 1 you can interact with the remote computer. If InputsEnabled = 0 you can view the remote computer, but cannot interact with it. Use DWorD format.

Summary

- Bring computers in your network under control of the Portal using the Manage Computer task.
- The starting location of a task determines the audience for the task. Typical starting locations are groups in the Groups container and Device Categories Containers.
- 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 Portal media directory.
- Use the Install Portal Agent task to deploy the Portal Agent on remote devices.
- Use the Install Client Automation Agent task to deploy the Client Automation agents 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 Subordinate 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 Portal task to apply the code delivered in a new build of the Portal to the remote Portal Zones in your enterprise.
- Use like-named Groups or Device Categories Groups to schedule jobs to run on multiple zones in your enterprise.
- You can use Remote Control to manage Client Automation agents with TightVNC from a remote location.

6 Troubleshooting

At the end of this chapter, you will:

- Be familiar with the 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 backup utilities.
- Be familiar with the options available for troubleshooting and logging the Portal Directory services (slapd, slurpd).
- Be familiar with Portal Agent signal processing parameters that can be tuned to enhance performance.

About the Log Files

⚠ If your environment uses Core and Satellite servers, first read the *Core and Satellite Servers Getting Started Guide* as the configuration, installation and troubleshooting information in that guide may override the information in this guide.

The Portal writes several logs, which can be used to track progress and diagnose problems. The log files are stored by default in `SystemDrive:\Program Files\Hewlett-Packard\CM\Management Portal\logs` for the Portal for Windows.

The log files are:

- `httpd-managmentportal-port.log`
  This is the main log for the Portal. It contains information about the actions that you perform in the Portal, operational statistics, as well as the version and build number of the Portal.

  Replace *`port`* with your port number, for example, `httpd-managementportal-3471.log`.

  Each time you start the web server a new log is written. The old log is saved as `httpd-managementportal-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-port.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 312 for more information.

To change the trace level for the logs

1 Open the file `SystemDrive:\Program Files\Hewlett-Packard\CM\ManagementPortal\etc\httpd-managementportal.rc` for

Windows, which is located on the computer that is running the Portal. The following is an excerpt from this file.

```
# Config Array
# Element Default
# ======= =======
# HOST           [info hostname]
# PORT           3471
# HTTPS_HOST     [info hostname]
# HTTPS_PorT     443
# DEBUG          0
# DOCROOT        [file join $home htdocs]
# IPADDR         {}
# HTTPS_IPADDR   {}
# WEBMASTER      support@hp.com
# UID            50
# GID            100
# NAME           $tcl_service
# LOG_LEVEL      3
# LOG_LIMIT      7
#
Overrides Config {
    PORT         3471
    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 28 Trace Levels

Trace Level	Description
0	No logging.
1	Logs errors only.
2	Logs warnings and errors.
3	Logs informational messages, warnings, and errors. *Recommended trace level setting for customers.*

Trace Level	Description
4	Logs all debug information. *Recommended for experienced customers only.*
5 - 9	Full trace *Not recommended for customer use.*

3 Save the file changes and restart the Portal service.

Common Message Types

Table 29 below contains common message types found in the main Portal log (`httpd-port.log`).

Table 29 Common Message Types

Message Type	Description/Example

Info	Provides general information. For example:
	`20010913 12:37:55 Info: LdifImport/4: BEGIN`
	Indicates that a job to import an LDIF has begun.
	`20010913 12:37:55 Info: RMP: Starting Scheduler...`
	Indicates that the Portal's Scheduler service is started.
	`20010913 12:37:55 Info: RMP: Management Portal ready`
	Indicates that the Portal is up and running.

Audit/success	Indicates a successful change to an object in your Portal directory. For example: `20010913 12:46:43 Audit/success: RMP: (who/admin) add: uid=jbanks, cn=opsys,ou=who` Indicates that a new user was added.

Message Type	Description/Example
Audit/failure	Indicates an unsuccessful change to an object in your Portal directory. For example: `20010913 16:26:31 Audit/failure: RMP: (who/admin) add: uid=Guest, ou=who, object "uid=guest,ou=who" already exists` Indicates that you were not able to add a user with the ID Guest to the organizational unit "who" because it already exists.
Error	Indicates a critical problem.
Warning	Indicates a non-critical problem. `20010913 16:20:42 Warning: to: output to 1 job-create-reply 2 resume: no gate`

Collecting Information for HP Technical Support

If you need to contact HP Technical Support for assistance, be sure to collect the following information:

1. The log directory, stored by default in the following locations:

   For Windows, *SystemDrive*:\Program Files\Hewlett-Packard\CM\ManagementPortal\logs

2. Version information for nvdkit.exe. See Viewing and Logging Version Information, below.

3. The etc directory files, stored by default in the following location:

   ```
   SystemDrive:\Program Files\Hewlett-Packard\
   CM\ManagementPortal\etc
   ```

Viewing and Logging Version Information

After logging into the Portal, click the Information button ? on the banner area to open the Version Information Window. This window displays the installed Module, Version, and Build levels for the Portal, including component modules NVDKIT.EXE, HTTPD.TKD, NVDCRT.TKD and RMP.TKD. Whenever this window is displayed, the version and build levels for each module are also written to the Portal log (httpd-mangementportal-*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 Portal session.

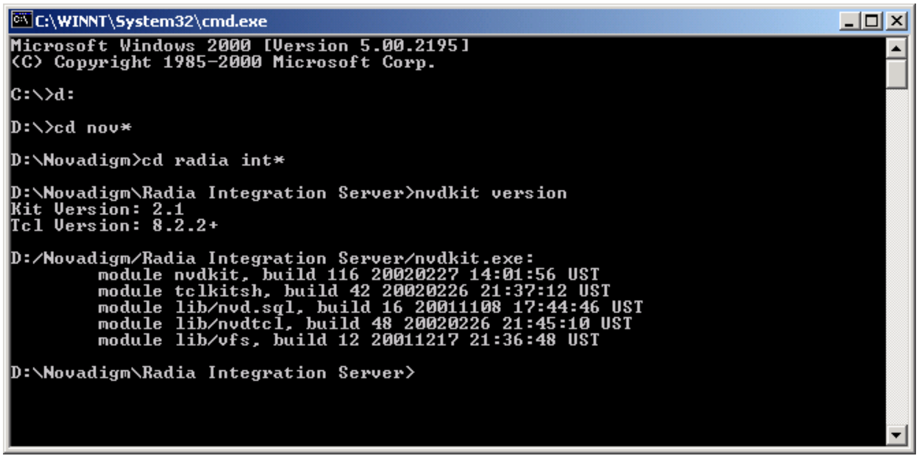
To gather the version information for NVDKIT.EXE

1 Open a command prompt.

2 Navigate to the location of nvdkit.exe (by default, *SystemDrive*:\Program Files\Hewlett-Packard\CM\ManagementPortal)

3 Type **nvdkit version**, and press **Enter**.

Below is an example of the version information.



```
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/nvdtcl, 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

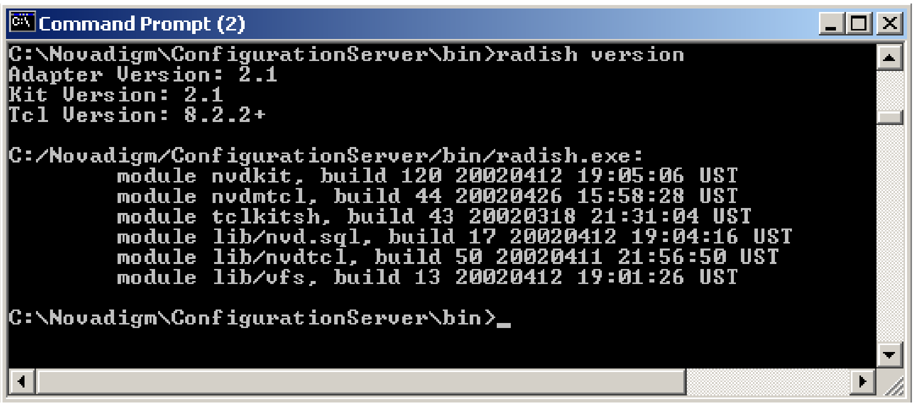
1 Locate the directory of your radish.exe on the machine running the Configuration Server. The default for Windows is:

`*SystemDrive*:\Program Files\Hewlett-Packard\CM\ConfigurationServer\bin`

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

The Portal Directory loads all configuration and entitlement information for the Portal as well as devices, groups, managed infrastructure, job status, network and mounted services information.

For performance reasons, HP recommends limiting the number of devices managed by a single zone to the following:

- Recommended maximum: 50,000 devices

To create additional zones in your enterprise, see Installing Additional Portal Zones (Subordinate Zones) on page 282.

Portal Directory Troubleshooting

The following two options can be configured if you are having difficulties with the Portal Directory's Slapd service.

To adjust the OVCMLDAP Heartbeat Detection Interval

By default, the "heartbeat" of the Master Slapd service for the Portal Directory is checked every 20 seconds. If the service is stopped, it is automatically restarted at this point to ensure continued support. You can change this heartbeat detection interval, if desired, by adding the following line to the `rmp.cfg` file:

```
OVCMLDAP_HEARTBEAT_INTERVAL     xx
```

Where: *xx* represents the interval value in seconds. For example, to set a heartbeat detection interval of 10 seconds, enter:

```
OVCMLDAP_HEARTBEAT_INTERVAL     10
```

Restart the Portal service to activate the new heartbeat interval.

To enable logging of the Slapd, Backupslapd, and Slurpd Services

If the Portal Directory's Slapd service requires troubleshooting, CM customer support may ask you to turn on logging for the slapd, backup slapd, and slurpd services.

To create a `slapd.log`, `backupslapd.log`, and `slurpd.log` in the Portal `\openldap` directory, add these parameters to `rmp.cfg`:

```
SLAPD_DEBUG_LEVEL         256
BACKUP_SLAPD_DEBUG_LEVEL  256
SLURPD_DEBUG_LEVEL        256
```

Where: *256* represents a sample debug level. Replace 256 with the desired debug level from Table 30, below. If no value is entered, the default is 0, which turns logging off.

Table 30 Debug levels for slapd, backupslapd, and slurpd logs

Debug level	Description
-1	Enable all debugging **Warning:** Logs ferocious amounts of data. Not recommended.
0 (default)	Turn off logging
1	Trace function calls
2	Debug packet handling
4	Heavy trace debugging
8	Connection management
16	Print out packets sent and received
32	Search filter processing
64	Configuration file processing
128	Access control list processing
256	Stats log connections/operations/results
512	Stats log entries sent
1024	Print communication with shell backends
2048	Print entry parsing debugging

Restart the Portal Service to begin logging the slapd, backupslapd, and slurpd services.

To turn off logging for the Slapd, Backupslapd, and Slurpd services

1 Reset the value of all *DEBUG_VALUE parameters in `rmp.cfg` to 0, or delete the values.

2 Restart the Portal Service.

Managing Portal Agent Signal Processing

RMA Signal Processing Parameters

The Portal uses three types of dedicated thread pools to handle the incoming requests from Portal Agents (RMAs). You can adjust the number of threads assigned to each pool by adding or updating these parameters in rmp.cfg.

You can also adjust the maximum number of RMA signals the Portal will process at a time.

The parameter changes you make in the `rmp.cfg` file will take affect when the Portal is restarted.

- The Portal limits the number of RMA signals it will accept for concurrent processing. This is defined in the `OPEN_RMA_SIGNAL_SOCKETS_MAX` parameter.
- All incoming RMA requests are handled initially by the `RMA_SIGNAL_RECEIVER_THREADS` pool. These lightweight threads handle only the simplest tasks, such as RMA status checks when the device DN is known.
- RMA requests requiring a database update for a known DN are passed to the `RMA_SIGNAL_PROCESSOR_THREADS` pool.
- RMA requests requiring any RMA registration look-up or creation work (that is, the device DN is not known) are passed to the `RMP_REGISTRATION_THREADS` pool. These threads perform the heaviest work.

Table 31 below summarizes the default and valid values for each parameter related to RMA signal processing.

Table 31 RMA Signal Processing Parameters (rmp.cfg)

Parameter, Default, Valid Values	Definition
`OPEN_RMA_SIGNAL_SOCKETS_MAX` Default: 1024 Valid Values: 256 or greater	Maximum number of RMA signals concurrently being processed by the Portal. After reaching this maximum, the Portal will reject additional incoming signals.

Parameter, Default, Valid Values	Definition
RMA_SIGNAL_RECEIVER_THREADS Default: 20 Valid values: positive number	Number of lightweight threads to use to accept incoming RMA requests. These threads handle RMA status checks when the DN is known, or pass requests to appropriate RMA Signal Processor or RMA Registration pool.
RMA_SIGNAL_PROCESSOR_THREADS Default: 3 Valid Values: positive number	Number of threads to process database updates when the RMA device DN is known.
RMP_REGISTRATION_THREADS Default: 1 Valid Values: positive number	Number of threads to process RMA registration look-up or creation work when the DN is not known. If these threads have no work, they will automatically assist with any RMA signal processor work.

Signal Processing Logs

All messages related to RMA signal processing will be handled by a separate thread and written to a separate log file, RMP-Signal.log, located in the \logs folder. Older logs are renamed RMP-Signal.log.1.log, for example, just like the Portal logs.

Summary

- The `httpd-managementportal-`*`port`*`.log` is the main log for the 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 Portal banner area after logging on. Alternatively, from a command prompt you can run "nvdkit version" on the agent side, and "radish version" on the Configuration Server side.
- Adjust the values for the RMA thread pool parameters to meet the needs of your current Portal requirements.

Index