Radia Client Automation Enterprise Portal

For the Windows® operating system

Software Version: 9.00

Reference Guide

Document Release Date: April 2013

Software Release Date: June 2013

Legal Notices

Warranty

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

Restricted Rights Legend

Copyright Notice

Trademark Notices

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

Acknowledgements

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

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

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

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

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

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

Documentation Updates

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

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

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

http://support.persistentsys.com/

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

For more details, contact your Persistent sales representative.

Support

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

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

To access the Self-solve knowledge base, visit the Persistent Support home page.

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

To register for a Persistent Support ID, go to: Persistent Support Registration.

Contents

Reference Guide 1

Contents 5

Introduction 7

- Benefits 7
- About the Portal Capabilities 7
- About the Product Architecture 8
- Portal Zones Overview 8
  - What is a Zone? 8
  - The Zone Directory Structure 9
  - About Object Names in a Zone 9
- Terminology 10
- Abbreviations and Variables 11
- Summary 11

Portal Zone Containers 13

- About the Zone Containers 13
- Summary 15

Administrative Functions 17

- Configuring a Portal Zone 17
- Setting Additional Configuration Parameters 17
- Configuring Directory Services 19
  - Directory Service Connection Status upon Portal Restart 20
    - Startup Property Set to Auto or Disabled 20
    - Startup Directory Service Property - Set to Manual 20
- Configuring for a Custom LDAP Policy Extension Prefix 21
- Customizing Domain Filters (DNAMEs) for Policy Resolution 22
- Managing the Portal Zone Directory 23
  - Terms for Database Recovery 23

Restore Procedures 23
Managing Management Agent Signal Processing 23
Managing the Portal Web Services Token 25
Routing Messages to Portal 25
We appreciate your feedback! 27

Chapter 1

Introduction

Use this reference guide as an extension to the *Radia Client Automation Enterprise User Guide*. The main goals of this guide are:

- To provide you with a better understanding of the concepts behind Portal management
- To allow you to perform more advanced administrative functions not covered in the *Radia Client Automation Enterprise User Guide*.

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

Benefits

The Portal is a backend component of any Radia Client Automation environment that provides an engine, Web Services, and an OpenLDAP database for the devices being managed in your environment.

The Portal provides the following benefits:

- **Security**
  Administrators are authenticated against the Portal Directory.
- **Extensibility**
  Administrators can access any Configuration Server, Configuration Server DB, Active Directory, or other LDAP Directory in your enterprise from within the Portal and administer policy, services, users, and machines directly by using the RCA Console.

About the Portal Capabilities

The Portal allows you to perform administrative and operational tasks from the RCA Console on any piece of your Client Automation infrastructure. The capabilities of the Portal include:

- **Network Discovery**
  The Portal engine automatically discovers the objects in your networks.
- **Authentication**
  Entries in the Portal Directory to authenticate administrators. These are entered from the RCA Console.
- **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.

- **OpenLDAP Directory for Device and Group Tasks**
  From the RCA Console, many activities, such as Notify, are performed on the target device groups that you select. The Portal provides the OpenLDAP directory hosting the device and device groups. The RCA Portal OpenLDAP directory is referred to and managed by the Core as the Radia Client Automation Directory Service.

About the Product Architecture

Although you will work with the Portal in the RCA Console, you may want to be familiar with its base architecture.

The Portal contains the following:

- The **Portal Run-time** contains the HPCA Portal service (HPCA-RMP) and the `RMP.TKD` module (located in the `\modules` directory).
- The **Portal Zone Directory**, is an OpenLDAP directory service in the `HPCA\DirectoryService` 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
  - Managed Services Catalog
  - Directory Services Definition
  - 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 Core Servers in your enterprise, all zones load the same-named set of containers at startup.
- The **Management Agent**, installed on the remote devices when the RCA Agents are installed, performs tasks on behalf of the Portal.

Portal Zones Overview

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 through the RCA Console.

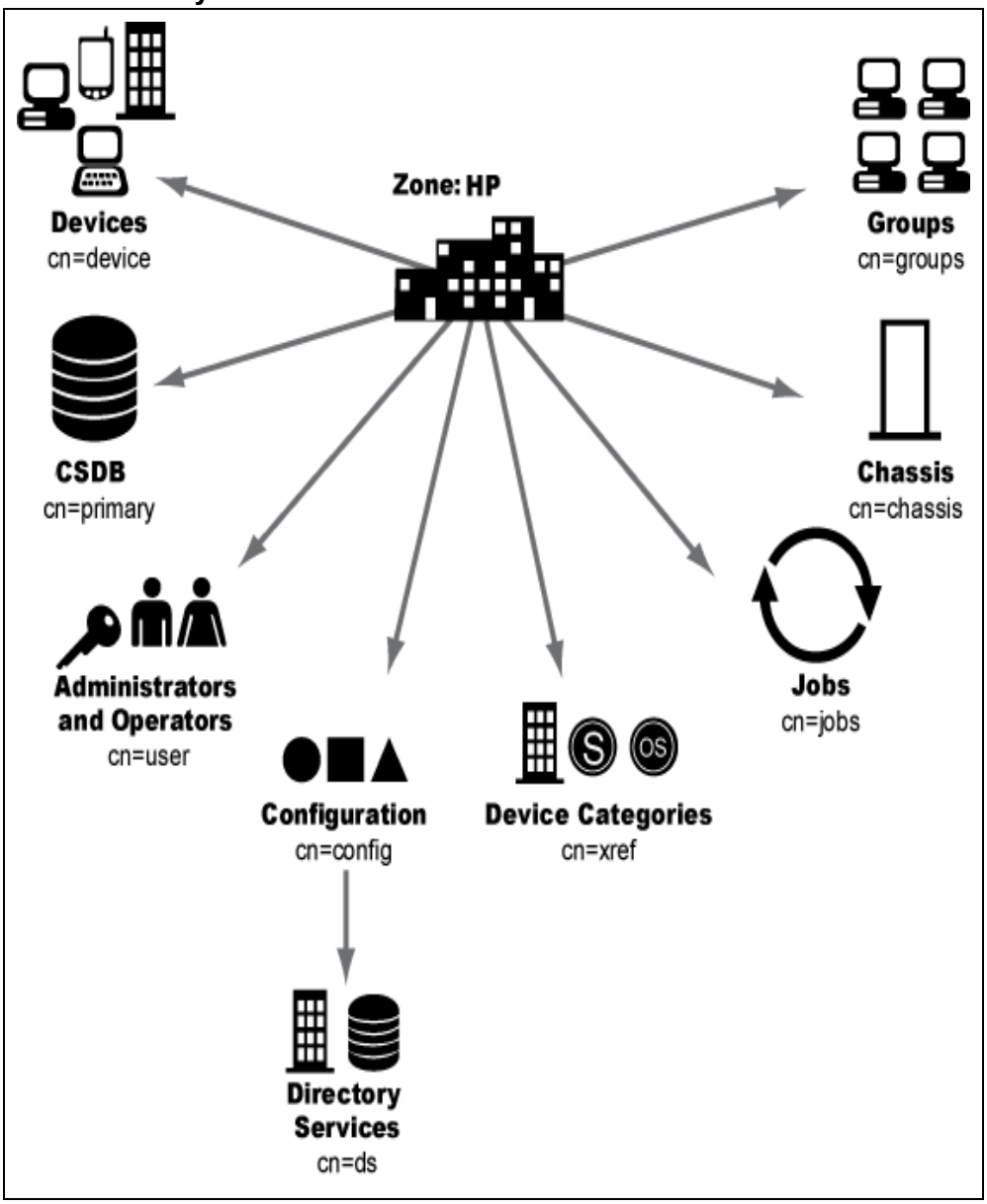
A zone is created whenever the Portal is installed (as part of the RCA Enterprise installation), and all objects in the zone include the high-level qualifier of the zone name. The properties for the zone object, itself, include the URL information needed to access the zone.

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

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=HP,cn=radia` and the location of the PRIMARY File on the Configuration Server is `cn=Primary, cn=HP,cn=radia`.

Terminology

The following terms are used frequently throughout this guide. You should become familiar with them before using 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 and the Configuration Server Database.

RCA Core Console user can connect to the LDAP Directory Services for which they are configured (given proper authority). These configurations are stored in the directory services container of the Portal OpenLDAP directory.

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.

rack

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

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.

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 through the RCA Console.

A zone is created whenever the Portal is installed as part of the RCA Core Server installation, and all objects in the zone include the high-level qualifier of the zone name.

Abbreviations and Variables

Abbreviations Used in this Guide

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

Variables Used in this Guide

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

Summary

- The Portal is an engine, a set of Web-services, and host to the OpenLDAP Zone directory for managed devices. The Portal components are required to support all RCA Client Automation environments.
- The Portal consists of the Portal Run-time, the Portal Zone Directory, and the Management Agent embedded in the RCA Agents. 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. Each zone directory contains the same set of containers.
- A single cn=hp,cn=radia zone is configured when a Core Server is installed.

Chapter 2

Portal Zone Containers

At the end of this chapter, you will be familiar with the zone containers that exist at the highest level of the directory.

About the Zone Containers

Portal zone containers 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)
- 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.

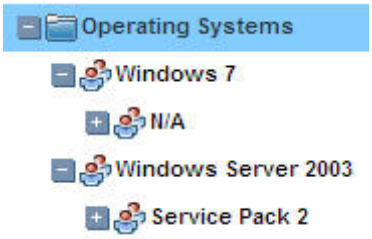
The portal zone containers and their objects are the following:

- **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 two groups:
  - Blade Enclosures
  - Racks Containing 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:
  - Device Discovery Types – Container for objects needed to discover LDAP Devices, NT Domains and RCA Reporting Servers.
  - Directory Services (cn=ds, cn=config) – Container of available directory services. See below for more information.
- **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 Management 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 Management Agent to the Portal for all devices under a zone's management:
  - **Device Architecture** - For example, HP Itanium Architecture, PC Architecture, and PowerPC IBM 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, Management Agent, and Configuration Server device groups.
  - **Managed Services** – For example, groups for each service being managed on devices through the RCA Application Manager or RCA Application Self-service Manager.

    Note: 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.
  - **Operating Systems** – For example, Windows Server 2003. Within a specific operating system group are sub-groups for service pack levels, as shown in the following figure:

  - **OS Management** - For example, Invalid OS, No Resolved OS, Pending Hardware Configuration, Pending OS Selection and Un-Managed OS.
  - **Service Acess Points** – For example, CONFIG, DATA, ROMS.
  - **Subnets** – For example, Subnet 16 groups all devices whose IP addresses are on that subnet.

    Note: 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.
- **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.

Summary

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.

Chapter 3

Administrative Functions

Configuring a Portal Zone

Following installation of the RCA Core Server, you need to add the following objects to a zone's infrastructure in order to use various new features. Most of these are added by using the RCA Core Console 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.
- **Device Categories Container**
  The groups in the Device Categories container are self-managed. They are automatically created after the Management Agent is installed on devices in the Device container, and dynamically maintained.

Setting Additional Configuration Parameters

Separate topics discuss how to modify the `rmp.cfg` file for:

- Customizing Domain Filters for Policy Resolution (see page "Customizing Domain Filters (DNAMEs) for Policy Resolution" on page 22).
- Managing Management Agent Signal Processing (see page "Managing Management Agent Signal Processing" on page 23)

The following table 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.

Additional Portal Configuration Parameters in RMP.CFG

Parameter	Definition
`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

Parameter	Definition
	server blade devices.
LISTENING_ ADDRESS	Specifies a valid network address (either an IP address, hostname, or DNS address) that is to be passed to Management 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 unsuccessful 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`
	
	Note: 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 Startup property when the Directory Service was configured.
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 RCA Definitive Software Library, and is accessible from the Services object (cn=services) located in the root of the Portal directory.

Parameter	Definition
	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 Management Agent, and contacting the Management 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).
`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.
`AUTH_LEVEL`	Enables faster RCA users authentication when you integrate an external directory service with RCA. If `AUTH_LEVEL` is set to 1, RCA authenticates the users that are direct members of the Authentication Group DN you configured in the RCA Console. RCA does not authenticate any sub group members in the Authentication Group DN. Hence, when you configure `AUTH_LEVEL`, you must make sure that all RCA users are added as direct members of the Authentication Group DN.

Configuring Directory Services

The Zone Configuration container includes the Directory Services container. This is where the Directory Service objects configured through the RCA Core Console are stored.

For more information, see the Configuration topics in the *Radia Client Automation Enterprise User Guide*.

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 Automatic, 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 an LDAP or LDAPS 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 Directory Service connecting to the RCA Configuration Server Database, 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 summarize the Manual Startup behavior for an LDAP(S) and RCA-CS Directory Service. If the Directory Service is connected to the Portal, its **Job activity** property indicates **started**.

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

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

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

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 *Radia Client Automation Enterprise Policy Server Reference 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 (`HPCA-RMP`).
2. Use a text editor to open the Portal configuration file, `rmp.cfg`, located by default in `<InstallDir>\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.
   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 HPCA Portal service (HPCA-RMP) and open the Portal.

Customizing Domain Filters (DNAMEs) for Policy Resolution

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 }
```

Note: See the Appendix B, Domain Filtering in the *Radia Client Automation Enterprise Policy Server Reference 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 `HPCA-RMP.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 `HPCA-RMP.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 `HPCA-RMP.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 `HPCA-RMP.rc` file and restart the Portal service.

Managing the Portal Zone Directory

The Portal Zone Directory is an OpenLDAP directory.

- To backup and restore the Portal Zone OpenLDAP directory, see the Admin Guide available at http://www.openldap.org/.
  Use standard tools available from http://www.openldap.org/ to backup and restore this directory.
- For information on Portal Directory Troubleshooting and logging the Slapd service, see the *Radia Client Automation Enterprise Troubleshooting Guide*.

Terms for Database Recovery

slapd - The stand-alone OpenLDAP daemon. It is started when the HP Client Automation Directory Service Windows service is started on the Core.

For more information on the use of this service with an OpenLDAP directory, see http://www.openldap.org/. Slapd is discussed on this page: http://www.openldap.org/doc/admin24/intro.html.

Restore Procedures

To manually restore the database from an external backup directory:

1. Stop the HPCA Portal service, `HPCA-RMP`.
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.

Managing Management Agent Signal Processing

The Portal uses three types of dedicated thread pools to handle the incoming requests from Management Agents. 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 Management Agent 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 Management Agent signals it will accept for concurrent processing. This is defined in the `OPEN_RMA_SIGNAL_SOCKETS_MAX` parameter.
- All incoming Management Agent requests are handled initially by the `RMA_SIGNAL_RECEIVER_THREADS` pool. These lightweight threads handle only the simplest tasks, such as Management Agent status checks when the device DN is known.
- Management Agent requests requiring a database update for a known DN are passed to the `RMA_SIGNAL_PROCESSOR_THREADS` pool.
- Management Agent requests requiring any Management Agent 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.

The following table summarizes the default and valid values for each parameter related to Management Agent signal processing.

Management Agent Signal Processing Parameters (`rmp.cfg`)

Management Agent 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 Management Agent signals concurrently being processed by the Portal. After reaching this maximum, the Portal will reject additional incoming signals.
`RMA_SIGNAL_RECEIVER_THREADS` Default: 20 Valid values: positive number	Number of lightweight threads to use to accept incoming Management Agent requests. These threads handle Management Agent status checks when the DN is known, or pass requests to appropriate Management Agent Signal Processor or Management Agent Registration pool.
`RMA_SIGNAL_PROCESSOR_THREADS` Default: 3 Valid Values: positive number	Number of threads to process database updates when the Management Agent device DN is known.
`RMP_REGISTRATION_THREADS` Default: 1	Number of threads to process Management Agent registration look-up or creation work when the DN is not known. If these threads have no work, they will automatically assist with any Management Agent signal processor work.

Parameter, Default, Valid Values	Definition
Valid Values: positive number	

Managing the Portal Web Services Token

The Portal Web Services (WS) require a valid token holding user credentials in order to perform Radia Client Automation activities.

The `WS_TOKEN_TTL` parameter in the `rmp.cfg` determines how long, in seconds, a given Portal Web Services (WS) user credential token is valid before it expires. During normal usage of the RCA Core Console, the token is routinely refreshed. If no user activity is detected within the `WS_TOKEN_TTL` period, the user's session will expire and they will be asked to log in again.

The default `WS_TOKEN_TTL` period is 1200 seconds (20 minutes).

Valid Values: positive number

Default: 1200 seconds

Routing Messages to Portal

By default all internal LDAP messages to the Portal except Satellite server messages, Proxy server messages, and OS Manager server messages are disabled. The `ZTASKEND` REXX program routes the messages that are not configured to be sent to the Portal to the RDBMS using Messaging server. When the external directory service is not being used, these messages help in providing internal policy resolution if the Management agent (formerly known as RMA) is not installed on the target device.

To modify the default `ZTASKEND` behavior, such that all messages are sent to the Portal, complete the following steps:

1. Open the file `ZTASKEND` file from the location `<InstallDir>\ConfigurationServer\rexx\NOVADIGM.`
2. Delete the following lines of code:
   - `Domname = strip( Upper(edmgetv( "PREFACE", "ZDOMNAME")) )`
   - ```
     If ( ( Ctype = "SATELLITE" | Ctype = "RPS" ) | (Domname = "OS" ) )
     Then Do
         BootCmd = BaseCmd || " -to CORE.RMP,CORE.ODBC -priority 10 "
     BootObjects
     End
     Else Do
     End
     ```
     ```

Make sure that you do not delete the following line in the Else condition:

```
BootCmd = BaseCmd || " -to CORE.RMP,CORE.ODBC -priority 10 "
BootObjects
```

3. Save and close the `ZTASKEND` file.

Note that when you enable all messages to the portal, the load increases on the Portal, which can further result in the reduced Portal performance.

We appreciate your feedback!

If an email client is configured on this system, by default an email window opens when you click here.

If no email client is available, copy the information below to a new message in a web mail client, and then send this message to radiadocfeedback@persistent.co.in.

Product name and version: Radia Client Automation Enterprise Portal, 9.00

Document title: Reference Guide

Feedback: