

HP Configuration Management

Proxy Server

for the AIX, HP-UX, Linux, Solaris, and Windows® operating systems

Software Version: 5.10

Installation and Configuration Guide

Document Release Date: April 2008

Software Release Date: October 2007



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

© Copyright 2002-2008 Hewlett-Packard Development Company, L.P.

Trademark Notices

Linux is a registered trademark of Linus Torvalds.

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

OpenLDAP is a registered trademark of the OpenLDAP Foundation.

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

TFTP SERVER

Copyright © 1983, 1993

The Regents of the University of California.

OpenLDAP

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

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

OpenSSL License

Copyright © 1998-2001 The OpenSSLProject.

Original SSLeay License

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

DHTML Calendar
Copyright Mihai Bazon, 2002, 2003

Documentation Updates

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 lists new features added for the Configuration Management v 5.10 and 5.00 releases.



This guide reflects the new default installation paths for the Configuration Management products. Please read the *CM 5.1x Release Notes* for more information.

Table 1 New features added for Configuration Management 5.10 and 5.00

Chapter	Version	Changes
Chapter 2	5.00	Page 32, System requirements have changed for Windows and UNIX platforms. Refer to this topic and to the latest release notes document for details on supported platforms.
Chapter 2	5.00	Page 42, Requirements for Remote Installations from the CM Portal have changed. The CM Portal v 5.00 does not support installing CM Proxy Servers to UNIX devices.
Chapter 2	5.00	Page 38, Installing the CM Proxy Server Locally for UNIX, type <code>./setup</code> to launch a local installation on a UNIX machine.

Chapter	Version	Changes
Chapter 3	5.00	Page 95, Using CM Proxy Servers to Install CM agents remotely from the CM Portal, updated for new terms and task name: Install Radia Client task was renamed Install CM Agent.
Chapter 5	5.10	Page 109, The CM Enterprise Proxy Server (using Apache) on Windows , new chapter explains how to install and uninstall the Enterprise Proxy Server using Apache.
Chapter 5	5.10 Apr 08	Page 115, Preloading (or Synchronizing) the Data Cache , corrected the command used to preload the CM Enterprise Proxy Server. The corrected command is: http://proxy_host_or_IP_address:port/proc/rps/sync This is the same command as the one used to preload the CM Proxy Server.
All	5.0	Removed references to the Staging Server; this Infrastructure component is no longer available with CM Software Versions 5.00 and above.

Table 2 indicates changes made to this document for earlier releases.

Table 2 Document changes

Chapter	Version	Change
Chapter 2	2.1	Page 33, UNIX System Requirements : Added new UNIX platforms on which the CM Proxy Server can be installed: <ul style="list-style-type: none"> • Solaris operating system Version 2.5.1 or above, SPARC CPU or Sunx86 platform. • Red Hat Enterprise Linux Version 2.1 or above. • SUSE LINUX Enterprise Server Version 8 or 9. Also removed references to Motif 1.2 libraries from the UNIX System Requirements listings.

Chapter	Version	Change
Chapter 2	2.1.1	Page 68, Creating the Entitlement Policy for a Static Cache Preload : expanded the procedures to include more detail on performing each step from the CM Admin CSDB Editor. Also removed steps to load PRDMAINT files using an _ALWAYS connection.
Chapter 2	2.1.1	Page 71, Preloading Deployment Options , added new subtopics for Preloading using SSL and Preloading Using Multicast.
Chapter 2	2.1.1	Page 73, Preloading Using SSL (TCPS or HTTPS) : new topic discusses how to configure the CM Proxy Server for a preload using SSL and TCP (TCPS), as well as a preload using SSL and HTTP (HTTPS). Both implementations rely upon the installation of SSL components and certificates, as discussed in the <i>HP CM SSL Implementation Guide</i> .
Chapter 2	2.1.1	Page 76, Preloading Using Multicast : new topic discusses how to preload a CM Proxy Server using multicast, includes an example of using multicast with dynamic windows, and where to find the session logs. This requires the installation and configuration of the HP Configuration Management Multicast Server (CM Multicast Server).
Chapter 2	2.2	Page 81, Preloading Windows Installer Enabled Applications : <ul style="list-style-type: none"> • Added the following best practice information: Using a single application and a ZSTOP expression on the ACP package is considered the best practice model. This model is applied automatically when you publish Windows Installer Applications using the Advanced publishing mode of the CM Administrator Publisher (Publisher) and apply the default Admin Install Point (AIP) options. • Deleted the model to preload <i>all</i> ACP packages through the use of a common package suffix and a single ACP service. Replaced it with a warning against adopting the model because it presents unnecessary overload on your infrastructure.
Chapter 3	2.1.1	Page 91, CM Portal and the CM Proxy Server : updated the Management Portal task list and descriptions, and deleted references to Activity Log and Statistical Data Collection.

Chapter	Version	Change
Chapter 3	2.2	<p>Page 91, CM Portal and the CM Proxy Server: updated content to reflect Management Portal (v2.1 and above) and task name changes.</p> <ul style="list-style-type: none">• Install Client was renamed Install Radia Client• Manage Proxy Server was renamed Assign Proxy Server• Purge Dynamic Cache was renamed Purge Proxy Server Dynamic Cache

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 HP Software Support web 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 a support contract.

To find more information about access levels, go to:

www.hp.com/managementsoftware/access_level

To register for an HP Passport ID, go to:

www.managementsoftware.hp.com/passport-registration.html

Contents

1	About the CM Proxy Server	13
	Who this Guide is for	14
	What this Guide is about	14
	What is the CM Proxy Server?.....	15
	When to use a CM Proxy Server	17
	CM Proxy Server Processing.....	18
	Cache Definitions and Support.....	19
	Static Cache.....	19
	Preloader Process	20
	Preloader and Desired-State Policy Resolution.....	20
	Dynamic Cache.....	22
	Dynamic PassThru	23
	Dynamic Cache Management	23
	What is a Co-Located CM Proxy Server?	24
	When to use a Co-located CM Proxy Server.....	25
	HP OVCM Integration Server and the CM Proxy Server	26
	CM Portal and the CM Proxy Server	26
	Summary	28
2	Installing and Configuring the CM Proxy Server	29
	Installation and Configuration Overview	30
	CM Proxy Server System Requirements.....	31
	Hardware Requirements and Recommendations	31
	Windows System Requirements.....	32
	Platform Support	33
	UNIX System Requirements	33
	Platform Support	33
	CM Proxy Server Installation	33

Windows and UNIX Installation Notes	34
Installing the CM Proxy Server to a Local Directory	35
Installing the CM Proxy Server Locally for Windows.....	35
Installing the CM Proxy Server Locally for UNIX.....	38
Starting and Stopping the CM Proxy Server for UNIX	41
Installing the CM Proxy Server to a Remote Location.....	42
Requirements for Remote Installations from the CM Portal	42
Preparing and Locating Configuration Files for Remote Proxy Server Installs ...	43
Performing the Install Proxy Server Task.....	44
CM Proxy Server Directory Structure	47
Applying Product Updates	47
Configuring the CM Proxy Server	48
CM Proxy Server Configuration File Overview	48
RPS.CFG Configuration Parameters Table	49
Editing the RPS.CFG File	55
Configuring the Dynamic Cache Parameters.....	56
Coding Multiple Upstream Hosts for Dynamic Cache Fail-over Support.....	58
The Date-Based Purge of the Dynamic Cache	59
Saving the Index File.....	59
Specifying a Size-Based Purge of the Dynamic Cache	60
Configuring the CM Proxy Server for an Internet Proxy (Firewall) Environment	62
Examples of TCP Parameters for Static Cache Preloader.....	62
Examples of HTTP Parameters for Dynamic Cache PassThru.....	62
Co-Locating a CM Proxy Server with a CM Configuration Server for HTTP Support.....	63
Configurations that Require a Co-located CM Proxy Server	63
Installing and Configuring a Co-located CM Proxy Server.....	64
Safeguarding the CM-CSDB from a Dynamic Cache Purge	66
Removing the Use of ZHTTPMGR for HTTP Support.....	66
Configuring the CM-CSDB for the Static Cache Preload	67
Creating the Entitlement Policy for a Static Cache Preload.....	68
Preloading Deployment Options	71
Preloading Using HTTP	72
Preloading Using SSL (TCPS or HTTPS).....	73
Preloading Using Multicast	76
Preloading using Multicast with Dynamic Windows	79
Session Logs for a Preload Using Multicast	80
Preloading Windows Installer Enabled Applications	81

Model 1: Create one Application (ZSERVICE) that includes a ZSTOP expression on the ACP Package.....	81
Model 2: Create separate Applications (ZSERVICES) for MSI Packages and ACP Packages	82
Configuring CM agents for Use with the CM Proxy Server	83
Using HTTP for CM agent Communication	83
Using TCP/IP for CM agent Communication	85
Additional Configuration Topics.....	87
Enabling the CM Configuration Server for HTTP Support	87
Summary	88
3 CM Proxy Server Administration	89
Starting and Stopping the CM Proxy Server for Windows.....	90
CM Portal and the CM Proxy Server	91
Preloading the CM Proxy Server	92
Synchronizing (preloading) the CM Proxy Server using the CM Portal.....	92
Purging the Dynamic Cache using the CM Portal.....	93
Using CM Proxy Servers to Install CM agents remotely from the CM Portal	95
Summary	97
4 Troubleshooting.....	99
CM Proxy Server Installation Directory	100
About the Log Files.....	100
Changing the Logging Level.....	101
Common Problems and Solutions	102
Performance Problems	102
Errors and Solutions	103
Testing the CM Proxy Server Preload	104
Troubleshooting Questions	105
Collecting Information for HP Technical Support	105
How to Obtain Version Information	106
Reporting a Problem for a CM Proxy Server.....	107
Summary	108

5 The CM Enterprise Proxy Server (using Apache) on Windows ...	109
Platform Support	109
System Requirements.....	109
Secured Network Requirement	109
CM Infrastructure Requirements	110
Co-located Proxy Server using Apache Requirements	110
Caching Proxy Server using Apache Requirements.....	110
Installation Tasks	110
Server Installation when Co-located with the Configuration Server	110
Server Installation for Data Caching.....	111
Stopping and Starting the CM Proxy Server using Apache	112
About the Configuration File: httpd.conf	113
Resetting the Log Level.....	113
Removing the CM Proxy Server using Apache	114
Data Cache Management.....	115
Preloading (or Synchronizing) the Data Cache	115
Automatic Purge of Cache above Max Size.....	115
Comparison Chart of CM Proxy Server and CM Enterprise Proxy Server	116
A Product Name Changes	117
Glossary.....	119
Index	125

1 About the CM Proxy Server

At the end of this chapter, you will:

- Understand the role of the HP Configuration Management Proxy Server (CM Proxy Server).
- Understand when to use a CM Proxy Server.
- Know how to use the CM Proxy Server.

Who this Guide is for

This book is for HP Configuration Management (CM) system administrators who want to install the CM Proxy Server in their enterprise environments to cache data at a location between the CM Configuration Server and their subscribers. To use some of the features in this publication, you should be familiar with the CM Portal, the CM Configuration Server, the CM Admin Configuration Server Database Editor (CM Admin CSDB Editor), and the CM agents.

What this Guide is about

The *HP Configuration Management Proxy Server Installation and Configuration Guide (CM Proxy Server Guide)* describes:

The Integration Server-based CM Proxy Server for Windows and Unix:

- what the CM Proxy Server is, and its static and dynamic cache processes.
- how to install and configure the CM Proxy Server:
 - as an agent when servicing CM agents.
 - as a server when co-located with the CM Configuration Server for HTTP download support.
- how to implement the CM Proxy Server with your CM Configuration Server and CM agents.
- how to administer the CM Proxy Server using the CM Portal 5.10 or greater.

The Apache-server based CM Enterprise Proxy Server for Windows:

- how to install, configure, and uninstall the CM Enterprise Proxy Server using Apache:
 - as an agent when servicing CM agents.
 - as a server when co-located with the CM Configuration Server for HTTP download support.
- how to implement the CM Enterprise Proxy Server with your CM Configuration Server and CM agents.

For more information, refer to [The CM Enterprise Proxy Server \(using Apache\) on Windows](#) on page 109 and the [Comparison Chart of CM Proxy Server and CM Enterprise Proxy Server](#) on page 116.

What is the CM Proxy Server?

When the CM Proxy Server is used, it is the primary repository for CM agent data. Once the CM agent determines the resources needed for its desired state, it can request those resources from the CM Proxy Server. Requests are made using either HTTP (recommended for all new installations) or TCP/IP. The CM Proxy Server has the ability to service multiple, concurrent CM agent requests using both protocols simultaneously. [Figure 1](#) on page 16 depicts the CM infrastructure using a CM Proxy Server to deploy applications to CM agents.

Figure 1 CM infrastructure using CM Proxy Server



When to use a CM Proxy Server

CM Proxy Servers are beneficial in your environment if you have many CM agent computers requesting the same resources from the same location. When data is cached on the CM Proxy Server, the demand placed on the CM Configuration Server is decreased, allowing the CM Configuration Server to allocate more resources to other tasks.

Placing CM Proxy Servers at strategic points in your network increases the rate at which data is transferred. The connection between subscribers and the CM Proxy Server may be more efficient than the connection between the subscribers and the CM Configuration Server. The factors that determine the efficiency of a connection between a server and an agent computer include hardware capability, network bandwidth, workload on the servers, network traffic patterns, and the volume of software to be distributed.



The CM Proxy Server is not a generic proxy, but rather specifically designed to manage and distribute CM resources.

This publication describes:

- CM Proxy Server components and processes.
- The installation of the CM Proxy Server components.
- The configuration and implementation of the CM Proxy Server.
- The configuration of your CM Configuration Management Database (CM-CSDB) and CM agents for use with CM Proxy Servers.
- The administration of the CM Proxy Server.

CM Proxy Server Processing

The logical flow for a typical CM agent request to a CM Proxy Server is as follows (assuming all components are enabled):


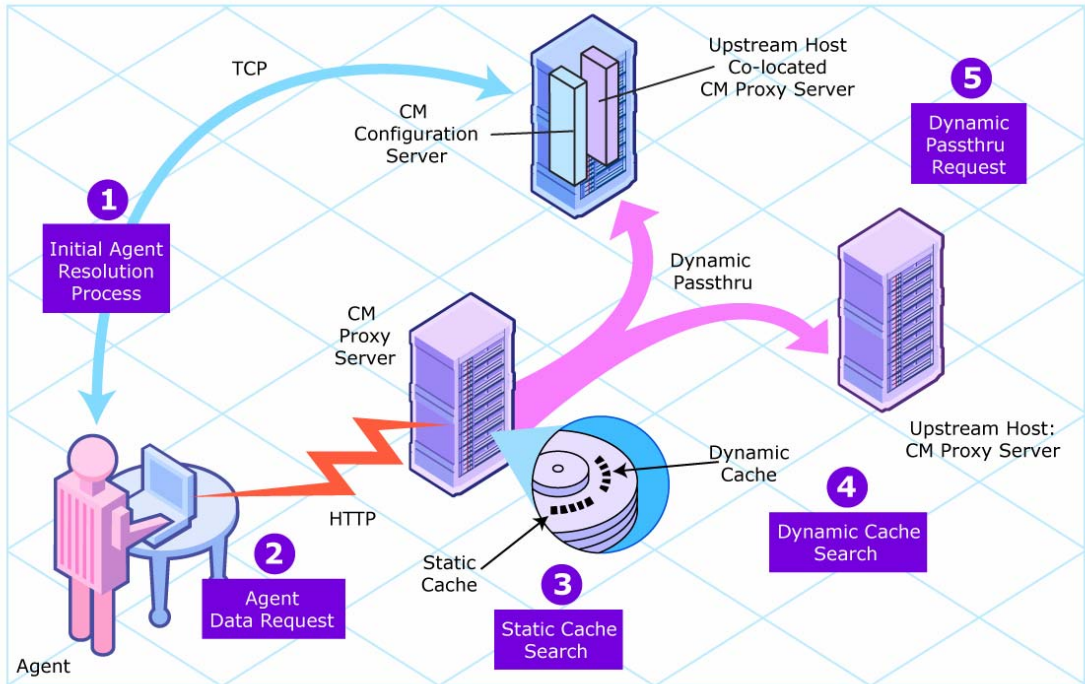
- 1 The CM agent's resolution process indicates it needs resources, and it should request them from a CM Proxy Server.
- 2 The CM agent sends a request to the CM Proxy Server, which is received by the CM Proxy Server front-end protocol. The agent request is validated, and passed to the cache manager.
 -  The default (and recommended) protocol for CM agent communication with the CM Proxy Server is HTTP. Optionally, TCP is also available. A CM Proxy Server can service multiple, concurrent agent requests using both protocols simultaneously.
- 3 The local static cache is searched, and if the data is found, the request is satisfied and the data is sent to the CM agent.
- 4 If the data is not in the local static cache, the local dynamic cache is then searched. If the data is found, the request is satisfied.
- 5 If the file does not reside in the dynamic cache, Dynamic PassThru requests the file from the defined upstream host (typically, another CM Proxy Server) using HTTP. If there is a connection failure with the upstream host, and multiple upstream hosts were defined (for fail-over support), Dynamic PassThru tries the next host on the list. The original request is satisfied, and the file is stored in the dynamic cache for future requests.

Figure 2 on page 19 illustrates the CM Proxy Server process flow for handling CM agent requests.

Figure 2 CM Proxy Server process flow



Cache Definitions and Support

The CM Proxy Server supports two types of cache locations: static and dynamic.

Static Cache

The **static cache** is the primary cache location for the CM Proxy Server. The static cache can be configured to operate in one of two ways:

- **Static Type = Agent**
When set to agent, the static cache is populated by the Preloader. For performance efficiency, this static cache should be preloaded with all resources that are expected to be distributed by the CM Proxy Server to

CM agents. The static cache is typically preloaded during off hours, so the required resources are available when requested by a CM agent. For a discussion of this process, see [Preloader Process](#) below.

- **Static Type = Server** (when co-located with the CM Configuration Server)

When set to server, the static cache points to a native CM-CSDB on the same machine as the CM Proxy Server. This co-located (or co-resident) CM Proxy Server provides a means to download resources from the CM-CSDB using HTTP. (The CM Configuration Server can only download resources using TCP/IP.) For details on when downloading resources from the CM-CSDB using HTTP is required, see [What is a Co-Located CM Proxy Server?](#) on page 24.

In both cases, the CM Proxy Server views static cache as read only.

Preloader Process

The Preloader populates the static cache of a CM Proxy Server using a process that parallels the standard CM agent resolution and deployment process. When the Preloader runs, it uses TCP to connect to the assigned CM Configuration Server for a resolution of the CM Proxy Server's predefined desired state. The required resources are then deployed to the CM Proxy Server's static cache. In addition, resources no longer included in the CM Proxy Server desired state are removed from the static cache.



As part of the CM Proxy Server installation, a small version of the CM Application Manager agent is also installed. These components provide the functionality to support the Static Cache Preload process.

The preload resources can be deployed using TCP or HTTP. HTTP is available when the CM Configuration Server has a co-located CM Proxy Server.

Preloader and Desired-State Policy Resolution

The Preload process is an application of the usual CM desired state policy resolution for CM agents, with the following specific elements. Each element is illustrated in [Figure 3](#) on page 22.

1 Define Entitlement

The entitlement for Preloading a CM Proxy Server is defined in the POLICY Domain as follows:

- **User**
The machine identity of the CM Proxy Server being managed (or preloaded).
- **Applications**
The software that is being preloaded to the CM Proxy Server's static cache. This should include all applications normally requested by the set of CM agents that will be assigned to the CM Proxy Server.

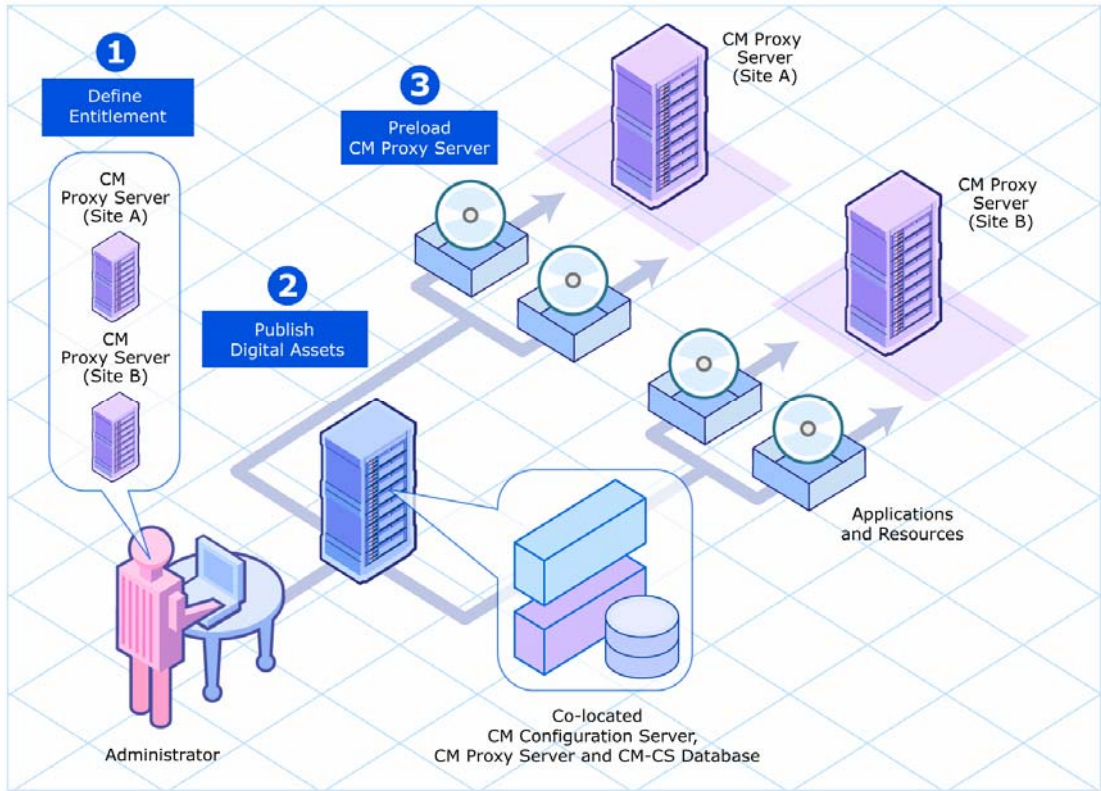
2 Publish Digital Assets

- **Application Files**
The components that make up the applications. When publishing MSI applications for distribution from a CM Proxy Server, use the techniques discussed in this guide to have the Administrator Control Point (ACP) preloaded to the CM Proxy Servers but not distributed to the CM agents.

3 Preload CM Proxy Servers

- **Deployment Source and Protocol**
Resources to preload the CM Proxy Servers can come from the CM Configuration Server or another CM Proxy Server. Resources can be deployed using TCP or HTTP. Resources deployed from a CM Configuration Server using HTTP use the HTTP port of a co-located CM Proxy Server.
- **Deployment Destinations**
In this case, the CM Proxy Server's static cache location is the Preload deployment destination.

Figure 3 CM Proxy Server Preload as a desired state policy resolution



Dynamic Cache

The **dynamic cache** is an optional, secondary cache location for the CM Proxy Server. When enabled, the dynamic cache is populated on demand by the Dynamic PassThru component of the CM Proxy Server using HTTP. When a requested resource is not found in the primary (static) cache, the dynamic cache is searched. If the requested resource is not found in the dynamic cache, the Dynamic PassThru process obtains the resource from an upstream host. The dynamic cache is viewed as a safety net for requests that fall through the static cache search.

Dynamic PassThru

When a CM agent request is received for a resource that does not exist locally, the CM Proxy Server can request these resources from an upstream host, such as a CM Proxy Server co-located with the CM Configuration Server, or another CM Proxy Server. These resources are then returned to the requesting CM agent, as well as stored locally in the dynamic cache for subsequent requests. Dynamic cache resources are transferred using HTTP.

For fail-over support, you can designate more than one upstream host for obtaining dynamic cache. If the CM Proxy Server fails to connect with the first host on the list, it attempts to connect with the second listed host, and so on, to obtain the dynamic cache resources.

Dynamic Cache Management

Dynamic PassThru also manages this cache, purging files that have not been requested in a previously configured number of days. (This avoids keeping files in the dynamic cache after they exist in the static cache.) To support the purge process, an index file is maintained to keep track of when files were last used. The dynamic cache cleanup of "aged" files can be run from the CM Portal using the Purge Dynamic Cache task. The purging of aged files will also run whenever the index file is saved. You can schedule the index file to be saved on a daily or more frequent basis. However, a scheduled save of the index file is skipped if dynamic cache resources were not used since the last save.

The dynamic cache can also be purged, as necessary, when a user-specified maximum file size is exceeded. The least-used files are deleted until the dynamic cache size is below the maximum file size. A "freespace" purge option allows you to purge down to a low-water mark, which is a certain percentage below the maximum file size. This "freespace" eliminates constant purging in an active dynamic cache environment.

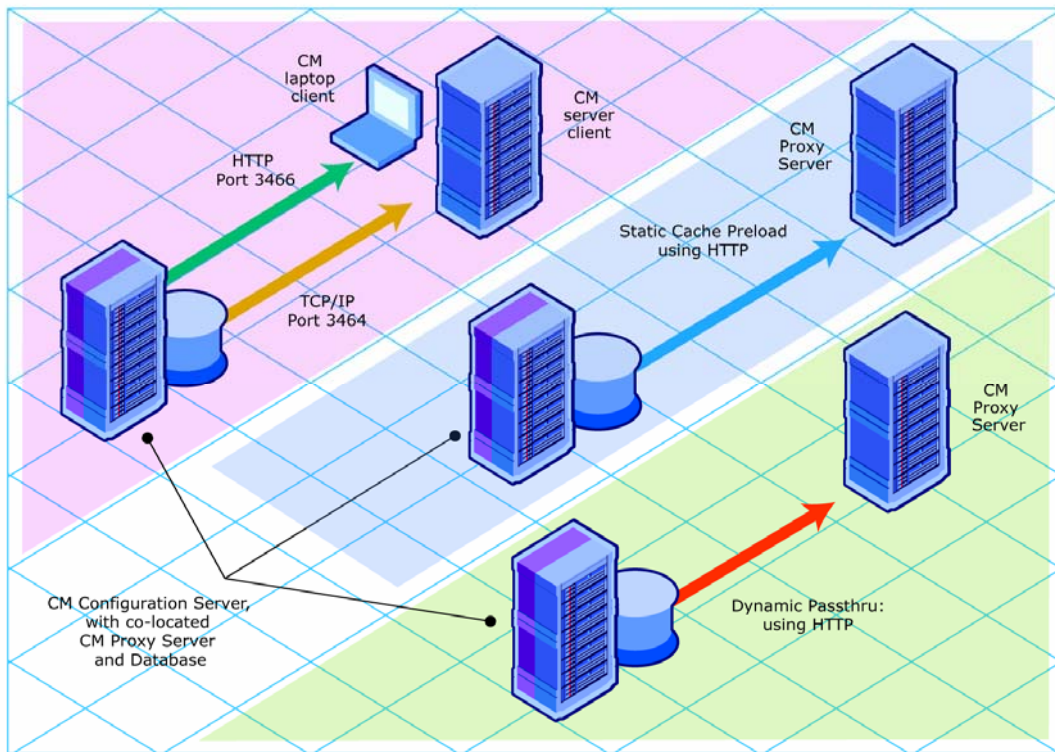
Another purge option allows you to define "large files", and then exempt these large files from the first pass of a size-based purge. If large files are purged and then later requested, an undue load could be placed on the network. Use the large file options to alleviate this load.

What is a Co-located CM Proxy Server?

The CM Configuration Server communicates with other servers and CM agents using TCP/IP. It no longer supports a native HTTP data download capability. To obtain HTTP download capability, you need to use a co-located CM Proxy Server.

A **co-located** CM Proxy Server is a CM Proxy Server placed on the same machine as the CM Configuration Server to provide a source for downloading CM-CSDB resources to another CM server or agents using HTTP. It is defined with a static cache type of *server*, instead of agent. It does not manage its own static cache, but merely points to the CM-CSDB on the CM Configuration Server. Thus, it requires no preloading (or synchronization), and normally has its dynamic cache disabled. This is shown in [Figure 4](#) below on the left path.

Figure 4 Co-located CM Proxy Server enables HTTP downloads



For details on installing and configuring a co-located CM Proxy Server, see [Co-Locating a CM Proxy Server with a CM Configuration Server for HTTP Support](#) on page 63.

When to use a Co-located CM Proxy Server

You need a CM Proxy Server co-located with the CM Configuration Server for HTTP support in the following configurations:

- To support CM agents configured to retrieve resources from the CM-CSDB using HTTP (instead of TCP/IP).
- To support a subordinate, or downstream, CM Proxy Server that is obtaining its dynamic cache resources from the CM-CSDB. Dynamic cache resources must be obtained using HTTP.
- To support preloading a subordinate, or downstream, CM Proxy Server using HTTP instead of TCP/IP.

Each configuration requiring a co-located CM Proxy Server is discussed below:

- **CM agents using HTTP to obtain their resources**
CM agents always obtain their policy resolution from the CM Configuration Server. By default, the CM agents then obtain their resources from the CM-CSDB using TCP/IP. To have CM agents obtain their resources from the CM-CSDB using HTTP, instead, you need to add a co-located CM Proxy Server with the CM Configuration Server, and then direct the CM agents to obtain their resources from the co-located CM Proxy Server. For details on directing CM agents to obtain their resources from a CM Proxy Server, see [Configuring CM agents for Use with the CM Proxy Server](#) on page 83.
- **Preloading a CM Proxy Server from the CM-CSDB using HTTP**
By default, a CM Proxy Server is preloaded from the CM-CSDB using TCP/IP. Optionally, it can be preloaded from the CM-CSDB using HTTP, instead. This configuration would also require a CM Proxy Server co-located with the CM Configuration Server for HTTP support, as shown in [Figure 4](#) on page 24 in the middle path. For details on using this option, see the topic [Preloading Deployment Options](#) on page 71.
- **CM Proxy Server using the CM Configuration Server as its dynamic cache upstream host**
Enabling the dynamic cache for a CM Proxy Server means that when a CM agent requests resources from the CM Proxy Server, and the resources are not in the local cache, the Dynamic Cache PassThru process

immediately requests the resources from its predefined upstream host using HTTP.

When a CM Proxy Server is enabled for dynamic caching, and is using the CM Configuration Server as the upstream host for obtaining its dynamic cache resources, you need to use a co-located CM Proxy Server for HTTP download support. This is because the Dynamic PassThru process uses HTTP exclusively. [Figure 4](#) on page 24 shows this configuration on the right-side path.

For details on specifying the dynamic cache and upstream host, see [Configuring the Dynamic Cache Parameters](#) on page 56.

HP OVCM Integration Server and the CM Proxy Server

The CM Proxy Server runs as a loaded module under the control of the CM Integration Server (HP OVCM Integration Server *or* CM Integration Server). The CM Integration Server is a base component for various CM infrastructure modules, such as the CM Portal and the CM Policy Server. It provides web services that are shared by loaded modules, resulting in a single entry point for all HTTP (web-based) requests. This integration provides performance, efficiency, and ease of maintenance in an adaptable and cohesive (server) framework.

The location of the CM Integration Server is the base installation directory of the CM Proxy Server. If the CM Integration Server is not currently present, it is installed with the CM Proxy Server.

CM Portal and the CM Proxy Server

The CM Portal provides a web-based, single access point from which CM administrators manage their entire CM environment regardless of location or computing platform. Administrative tasks can easily be distributed to administrators in remote locations based on roles and policies.

The CM Portal provides the ability to both install and perform many administrative functions for your CM Proxy Servers. The remote install from the CM Portal honors a pre-configured *.INI file, so the installed CM Proxy Server is ready to go. In addition, the CM Portal can be used to start, stop, preload (synchronize) the static cache, and purge the dynamic cache of any CM Proxy Server in your Network.

In conjunction with the ability of the CM Portals to install CM agents remotely, CM Proxy Servers can also be used to assist the CM Portal in distributing CM agent install scripts. This serves to spread the workload of deploying large numbers of CM agents between the CM Portal and CM Proxy Servers, just as the CM Proxy Servers assist the CM Configuration Server in deploying applications to the CM agents.

Summary

- CM Proxy Servers enable an additional server to act as an extension of the CM Configuration Server. The CM Proxy Server stores a copy of the application software that CM distributes, and delivers it to the CM agent computers that are attached to the server.
- Each CM agent will receive resources directly from the CM Proxy Server. The recommended protocol for CM agent communications is HTTP, although multiple, concurrent protocols are supported.
- A CM Proxy Server's static cache is preloaded with the applications defined for it in the CM-CSDB. The preload process connects using TCP, but can have resources deployed using TCP or HTTP. HTTP is available when the CM Configuration Server has a co-located CM Proxy Server.
- A CM Proxy Server enabled for dynamic cache will request resources from a predefined upstream host when they are not currently available in its local static or dynamic cache. Multiple upstream may be defined to provide fail-over support after a connection error. Dynamic cache resources are downloaded to the CM Proxy Server using HTTP. The dynamic cache offers a number of purge options to remove old files and to keep it under a specified maximum size.
- A CM Proxy Server co-located with the CM Configuration Server is used whenever you need to obtain resources from the CM-CSDB using HTTP. The CM Configuration Server no longer supports downloading resources using HTTP.
- The potential benefit of a CM Proxy Server must be evaluated individually for each server and its attached CM agent computers.

2 Installing and Configuring the CM Proxy Server

At the end of this chapter, you will:

- Be able to install the CM Proxy Server software locally using installation media, or remotely using the CM Portal.
- Be able to access and apply any updates to bring the product to the latest level.
- Be able to configure the CM Proxy Server after installation for different options, including the use of the dynamic cache and several preload options.
- Understand how to configure the different CM components for use with the CM Proxy Server.

Installation and Configuration Overview

Before you can use a CM Proxy Server, you must prepare your CM environment. To configure your enterprise for using CM Proxy Servers, you will need to complete the following tasks:

- ❑ Install the CM Proxy Server on the designated server.
 - Read the topics on system requirements and installation notes, and then follow the steps to install the CM Proxy Server locally or remotely (using the CM Portal). Separate procedures are given for local Windows and UNIX installations.
 - If you are installing the CM Proxy Server co-located with the CM Configuration Server (to provide a source for downloading resources from the CM-CSDB using HTTP), see [Co-Locating a CM Proxy Server with a CM Configuration Server for HTTP Support](#) on page 63.
 - Also visit the HP Technical Support web site to check for the latest available updates to the product, such as a Service Pack update.
- ❑ Review and modify the CM Proxy Server configuration parameters after installation. For example, edit the configuration file to enable and configure the dynamic cache.
See [Configuring the CM Proxy Server](#) on page 48.
- ❑ Create a distribution policy in the CM Configuration Server database for preloading the CM Proxy Server static cache.
See [Configuring the CM-CSDB for the Static Cache Preload](#) on page 67.
- ❑ Preload the CM Proxy Server static cache.
See [Preloading Deployment Options](#) on page 71.
- ❑ Assign the appropriate subscribers to the CM Proxy Server.
See [Configuring CM agents for Use with the CM Proxy Server](#) on page 83.

CM Proxy Server System Requirements

Hardware Requirements and Recommendations

- **Static Type of Agent**
In general, a CM Proxy Server with a static type of agent is most dependent on network bandwidth and disk I/O speed. Use the recommendations given in Table 3 below to obtain desired performance on your CM Proxy Servers. The CM Proxy Server will run on lesser machines, but performance will probably suffer under peak loads.
- **Static Type of Server**
A CM Proxy Server co-located with the CM Configuration Server for HTTP support has a static type of server. Most hardware requirements that satisfy the CM Configuration Server's needs more than accommodate the CM Proxy Server, especially the requirements for processor speed, memory, and disk drive speed. Refer to the *HP Configuration Management Getting Started Guide (CM Getting Started Guide)* for specific requirements. For additional considerations, see Table 3 below.

Table 3 CM Proxy Server Hardware Recommendations

Component	Static Type = Agent	Static Type = Server
Overall	In general, the CM Proxy Server is most dependent on network bandwidth and disk I/O speed.	A machine sized for the CM Configuration Server more than accommodates a co-located CM Proxy Server.
Processor	A higher processor speed is more important than having multiple processors. Thus, we recommend as fast a processor as is practical (for example, 2 GHz).	Use the CM Configuration Server requirements for speed. However, multi-processors are strongly recommended for this configuration.
Memory	At least 512 MB. As with all systems, the more memory the better.	CM Configuration Server requirements are fine.

Component	Static Type = Agent	Static Type = Server
Disk Space	Provide at least double the anticipated total volume of resources to be housed (that is, your anticipated static and dynamic cache).	CM Configuration Server requirements are fine.
Disk Drive Speed	Fast access disk drives are highly advisable.	CM Configuration Server requirements are fine.
Network Interface Card (NIC)	A fast network card is a plus. Use a 1 GB NIC if your network supports it.	A second network card is helpful to address configurations where network volume becomes a constraining factor (large volume due to the size or number of resources to be transferred to CM agents). When using two network cards, the CM Configuration Server is homed to one NIC IP address and the CM Proxy Server to the other.
Network Configuration	Minimize the number of router hops between CM agent requesters and their respective CM Proxy Server to improve performance.	If servicing CM agents, recommendation for a static type of Agent applies.

Windows System Requirements

- Connection to a computer running the CM Configuration Server.
- One of the following supported Windows operating systems, including x64 versions where applicable, and minimum Service Pack levels as identified in the release notes document that accompanies this release:
 - Windows XP Professional
 - Windows 2000 Server
 - Windows Server 2003 and Server 2003 R2
 - Windows Vista Business, Business Enterprise

Platform Support

For detailed information about supported platforms, see the release note document that accompanies this release.

UNIX System Requirements

- Connection to the computer running the CM Configuration Server.
- One of the following supported UNIX platforms:
 - AIX operating system:
Version 5.1, 5.2 or 5.3.
 - HP-UX operating system:
Version 11.0, 11.11, 11.23 or 11.31 on PA-RISC-2 architecture
Version 11.23 or 11.31 on Intel Itanium architecture
 - Red Hat Enterprise Linux, ES and AS:
Version 3 or 4 on x86 and AMD64/EM64T architectures
 - Red Hat Enterprise Linux Server:
Version 5 on x86 and AMD64/EM64T architectures
 - SUSE Linux Enterprise Server:
Version 9 or 10 on x86 and AMD64/EM64T architecture
 - Solaris operating system:
Version 8, 9, or 10 on SPARC; Version 9 or 10 on x86 architecture

Platform Support

For detailed information about supported platforms, see the release note document that accompanies this release.

CM Proxy Server Installation

There are two methods for installing the CM Proxy Server:

- Install the CM Proxy Server directly onto a local server.
- Install the CM Proxy Server remotely through the CM Portal. For more information, refer to the *CM Portal Guide*.

Windows and UNIX Installation Notes

- To complete the CM Proxy Server installation prompts, you need to understand the CM Proxy Server Preload process that resolves and loads the static cache. For details, see [Cache Definitions and Support](#) on page 19.
- Before you begin, locate your HP license file. You need this license file to install the products that you have purchased. If you need assistance, contact HP Technical Support.

During installation of the CM Proxy Server, the license file is renamed `license.nvd`, and is copied to the CM Integration Server's module directory.

- After installation, the Windows CM Proxy Server service is started automatically; but the UNIX CM Proxy Service does not.
- After installing the product from the CM Management Infrastructure media, check the HP Technical Support web site to see if a maintenance patch is needed to bring the product to the latest level. For details, see [Applying Product Updates](#) on page 47.
- To install the CM Proxy Server on a UNIX system, make sure the user who is installing the CM Proxy Server is logged in as root, and has adequate rights to create and update the target installation directory.



For the CM Proxy Server to operate correctly on Solaris platforms, the UNIX userID running the CM Proxy Server must include the directory `/usr/sbin` in the UNIX PATH environment variable setting. Contact your local system administrator if you need assistance.



In order for CM to install correctly on HP-UX platforms, you must mount the CM infrastructure media using `pfs_mount`. The CM infrastructure media is created using the Rock Ridge format. Since the HP-UX standard mount procedure is incompatible with the Rock Ridge file system type, HP has made available the PFS package (Portable File System) that allows their workstations to recognize this format. Specific instructions follow.

To mount the CM media placed on a DVD, insert it and type

```
/usr/sbin/pfs_mount -v -x unix /dvdrom/mnt
```

where:

`/dvdrom` is your physical media device.

To un-mount, type

```
/usr/sbin/pfs_umount /mnt
```

See your local UNIX systems administrator and UNIX man pages for more information.

Installing the CM Proxy Server to a Local Directory

This section describes how to install the CM Proxy Server to a local machine for both Windows and UNIX operating systems.

- Instructions for Windows begin below.
- Instructions for UNIX begin on page 38.

Following the installation, proceed with [Configuring the CM Proxy Server](#) on page 48.

Installing the CM Proxy Server Locally for Windows

This section describes how to install the CM Proxy Server to a local machine running Windows.

To install the CM Proxy Server locally for Windows

- 1 Double-click the `setup.exe` file from the CM Proxy Server installation source directory. The source directory is found on the CM media at the following path:

```
Drive:\Infrastructure\extended_infrastructure\proxy_server\  
win32
```

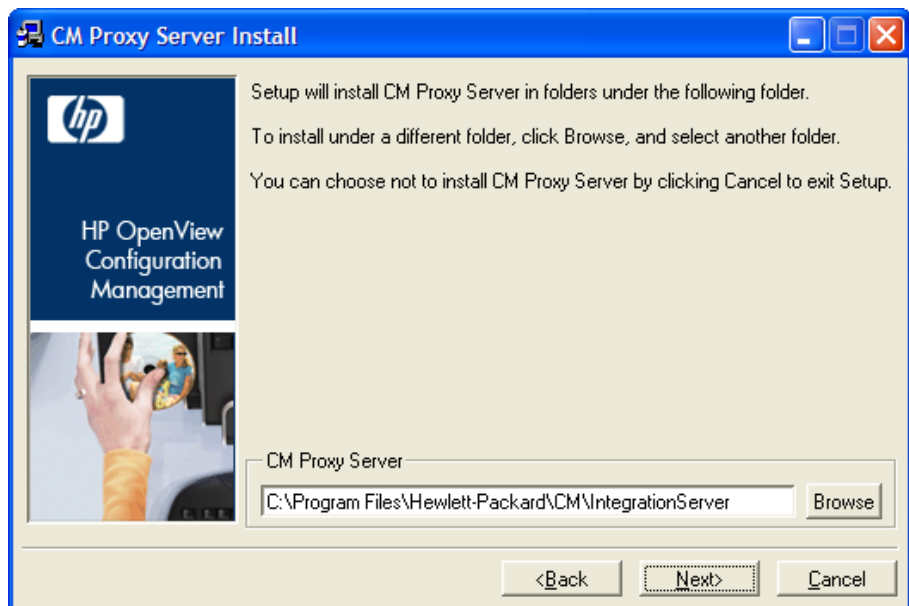
The Welcome window for the CM Proxy Server Setup program opens.

- 2 Click **Next**.

The End-User License Agreement window opens for you to read the licensing terms for this product. You must accept the terms before the CM Proxy Server can be installed.

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

The CM Proxy Server directory window opens for you to select or enter the base directory for the CM Proxy Server install. This CM Proxy Server base directory specifies the location of the foundation CM Integration Server component. The default is C:\Program Files\Hewlett-Packard\CM\IntegrationServer.



If an instance of the CM Integration Server component [httpd.tkd] is already on the target machine, then the Proxy Server Directory window is bypassed and the CM Proxy Server is installed automatically to the existing CM Integration Server folder. Continue with step 5.

- 4 Type the name of the base directory in which to install the CM Proxy Server, accept the default directory shown in the text box, or click **Browse** and navigate to the directory in the Browse dialog box.



For each value requested during this installation procedure, press **Enter** to accept the default.

5 Click **Next**.

The License File window opens.

6 Browse to or type the name of your License File in the text box. You must enter a valid license file to continue the installation.

The license file will be copied to the `/modules` folder as `license.nvd` during the installation.

7 Click **Next**.

The CM Configuration Server IP Address window opens.

8 In the Server IP Address text box, type the IP Address or DNS name of the host CM Configuration Server. The CM Proxy Server connects to this host during the preload process to obtain its static cache resolution and static cache files. The default is `localhost`.



- Leave the default entry of `localhost` if you are co-locating this CM Proxy Server with a CM Configuration Server to enable HTTP download support. For additional details, see [Co-Locating a CM Proxy Server with a CM Configuration Server for HTTP Support](#) on page 63.
- The CM Proxy Server Preload process must always connect to the host CM Configuration Server specified in the Server IP Address field for its static cache resolution. However, you can configure the CM Proxy Server to obtain the static cache files from another CM Proxy Server, if desired. For details, see [To change the deployment source or protocol for a preload to use HTTP](#) on page 72.

9 Click **Next**.

The CM Configuration Server Port window opens.

10 Accept or type the TCP port number of the CM Configuration Server to be used during the preload process for the static cache. The default port number is 3464.

11 Click **Next**.

The CM Configuration Server User ID window opens.

12 Specify the user ID that the CM Proxy Server will use to connect to the CM Configuration Server for its static cache preload resolution. The default is `RPS`.



The CM user ID entered must correspond to an instance in the Primary.Policy.User class in the CM-CS Database, where the static cache desired state policy for this CM Proxy Server is defined. See [Configuring the CM-CSDB for the Static Cache Preload](#) on page 67.

13 Click **Next**.

The Installation Settings window opens.

14 Review the settings in the Installation Settings window. If you want to change any of these settings, click **Back**.

15 Click **Install** to begin the CM Proxy Server installation.

The Installation Progress window opens.

16 When the installation is finished, the Successful Installation window opens.

17 Click **Finish** to exit the installation program.

You have successfully installed the CM Proxy Server Windows to a local directory. The service for the CM Proxy Server is the HP OVCM Integration Server (httpd), which is started.

- To apply any available product updates at this time, see [Applying Product Updates](#) on page 47.
- To complete the configuration of the CM Proxy Server for various options, see [Configuring the CM Proxy Server](#) on page 48.

Installing the CM Proxy Server Locally for UNIX

This section describes how to install the CM Proxy Server to a local site for UNIX.

Following installation, proceed with the topic [Configuring the CM Proxy Server](#) on page 48.

To install the CM Proxy Server locally for UNIX

1 The CM Proxy Server media is located on the CM DVD media at the following location:

```
/Infrastructure/extended_infrastructure/proxy_server
```

Depending on your version of UNIX, change your current working directory to the correct `/proxy_server` subdirectory on the installation media.

Example: For HP-UX, type:

```
cd /dvdrom/Infrastructure/extended_infrastructure/  
proxy_server/hpux
```

- 2 At the command prompt, type `./setup`, and then press **Enter**.

The Welcome window for the CM Proxy Server Setup program opens.

- 3 Click **Next**.

The End-User License Agreement window opens for you to read the licensing terms for this product. You must accept the terms before the CM Proxy Server can be installed.

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

The installation directory window opens for you to select or enter the base directory for the CM Proxy Server install.

The default CM Proxy Server install directory is:

```
/opt/HP/CM/IntegrationServer
```

- 5 Accept the default CM Proxy Server location, or type or browse to an alternate directory where you would like to install the CM Proxy Server.

This CM Proxy Server base directory specifies the location of the CM Integration Server component, installed with the product.

- 6 Click **Next**.

The License File window opens.

- 7 Type the location and name of your License File, or click **Browse** to select the file from the Browse dialog box.

- 8 Click **Next**.

The CM Configuration Server IP Address window opens.

- 9 Type the IP Address or hostname of the host CM Configuration Server the CM Proxy Server will connect to during a preload to obtain its static cache resolution and static cache files.



Leave the default entry of `localhost` if you are co-locating this CM Proxy Server with a CM Configuration Server to enable HTTP download support. For additional details, see [Co-Locating a CM Proxy Server with a CM Configuration Server for HTTP Support](#) on page 63.

The CM Proxy Server Preload process must always connect to the host CM Configuration Server specified in the Server IP Address field for its static cache resolution. However, you can configure the CM Proxy Server to obtain the static cache files from another CM Proxy Server, if desired. For details, see the procedure [To change the deployment source or protocol for a preload to use HTTP](#) on page 72.

10 Click **Next**.

The CM Configuration Server Port window opens.

11 Accept or type the TCP port number of the CM Configuration Server to be used to connect to the CM Proxy Server for the static cache Preload resolution. The default port number is 3464.

12 Click **Next**.

The CM Configuration Server User ID window opens.

13 Type the user ID that the CM Proxy Server will use to connect to the CM Configuration Server to obtain its static cache preload resolution. The default is RPS.



The user ID entered must correspond to an instance in the `Primary.Policy.User` class of the CM-CSDB, where the static cache desired state policy for this CM Proxy Server is defined. See [Configuring the CM-CSDB for the Static Cache Preload](#) on page 67.

14 Click **Next**.

The Installation Settings window opens.

15 Review the settings. If you want to change any of them, click **Back** until you reach the area of the installation you would like to change, and then click **Next** until you return to the Installation Settings window again.

16 Click **Install** to begin the CM Proxy Server installation.

The Installation Progress window opens.

17 When the installation is finished, the Successful Installation window opens.

18 Click **Finish** to exit the installation program.

You have successfully installed the CM Proxy Server locally for UNIX.


- To apply Product Updates at this time, see [Applying Product Updates](#) on page 47.
- To complete the configuration of the CM Proxy Server for various options, see [Configuring the CM Proxy Server](#) on page 48.
- To start or stop the CM Proxy Server for UNIX, use the commands discussed in the next topic, [Starting and Stopping the CM Proxy Server for UNIX](#).

Starting and Stopping the CM Proxy Server for UNIX

To start the CM Proxy Server for UNIX

- 1 Change your current directory to the directory where you installed the CM Proxy Server (`/opt/HP/CM/IntegrationServer` by default).
- 2 Type `./nvdkit httpd.tkd`
- 3 Press **Enter**.
- 4 The CM Proxy Server is started on your computer.

To stop the CM Proxy Server for UNIX

 The following are general guidelines and the commands are examples that may vary slightly depending on the UNIX type you are using.

- 1 Obtain the process ID for the CM Proxy Server by listing all the UNIX processes and extracting the process ID for `nvdkit`.

```
ps -f | grep nvdkit | sed /grep/d | awk '{ print $2 }'
```

- 2 Run the following command.

```
kill <PID>
```

The CM Proxy Server is stopped on your computer.

Installing the CM Proxy Server to a Remote Location

The CM Proxy Server can be installed remotely using the CM Portal from any web browser. During the installation, you will receive status information, and if the installation fails, it can be rescheduled.

The CM Portal also allows you to select a pre-configured CFG file during the Install Proxy Server task. Using this option means the installed Proxy Server can be fully configured and ready to run. See [Preparing and Locating Configuration Files for Remote Proxy Server Installs](#) on page 43 for more information.



The following sections require you to be familiar with the CM Portal. For detailed information, refer to the *CM Portal Guide*.

Requirements for Remote Installations from the CM Portal

In order to install CM infrastructure products from the CM Portal, you must be aware of the following requirements.

- The remote computer must be running a platform supported by the CM Proxy Server. Refer to the latest *Configuration Management Release Notes* document for exact information on the supported platforms.
- The installation files for the CM product must be stored in the CM Portal's `\media` directory. The CM Portal installation program will copy these files automatically when you opt to install the *components for remote infrastructure installations* from the installation dialog boxes. See the *CM Portal Installation and Configuration Guide* for more information.

If you did not copy these files using the installation program, you must manually copy them from the appropriate media location to the `\media\extended_infrastructure` directory of where the Portal was installed. The directory structure of this directory should mirror the media layout.

- 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 CM Portal creates the packing list when you launch the remote installation.
- For CM Portal 5.x and above, the Devices container must have an entry for each machine to which you are installing the CM Proxy Server. Refer to the *CM Portal Guide* for more information.

Preparing and Locating Configuration Files for Remote Proxy Server Installs

Optionally, use these procedures to prepare one or more fully configured `RPS.CFG` files before you run the CM Portal Install Proxy Server task. This allows you to install a Proxy Server that is already configured and ready to go.

The pre-configured `RPS.CFG` files must be placed in a specific media location for the CM Portal to use them. When you run the Install Proxy Server task from the CM Portal, the task will prompt you to select a specific CFG file, if multiple ones exist.

To prepare a pre-configured `RPS.CFG` file for use with the Install Proxy Server task

- 1 Prepare a fully configured `rps.cfg` file.

Perform a local installation of the CM Proxy Server on a test machine running the same platform as the intended CM Proxy Server platform. Edit the resulting `rps.cfg` file using the directions given in [Configuring the CM Proxy Server](#) on page 48.

- 2 Place the configured `rps.cfg` file in the appropriate CM Portal media directory. The location of a configured `rps.cfg` file reflects the platform on which you are installing the CM Proxy Server. For example, the location to place a Windows CM Proxy Server configuration file is similar to this:

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

Use the steps below to place the `rps.cfg` file at the appropriate `\media` location for the CM Portal.

- a Go to the directory where the CM Portal is installed.

The default is:

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

- b Go to the following folder in the CM Portal directory:

```
\media\extended_infrastructure\proxy_server\platform\media
```

where *platform* reflects the platform on which you are installing the CM Proxy Server, such as win32.

- c Add an `\etc` folder to the `\media` directory named in the previous step.
 - d Copy the `rps.cfg` file to this platform-specific `\etc` folder:

```
\managementportal\media\extended_infrastructure\proxy_server\platform\media\etc
```
- 3 Run the Install Proxy Server task from the CM Portal, as usual. See [Performing the Install Proxy Server Task](#) below. The installation task will transfer the fully configured `rps.cfg` file. If you prepare more than one configuration file, use the RPS Config File drop-down list to select the appropriate one during the Install Proxy Server task.

Performing the Install Proxy Server Task

Use these steps to install one or more CM Proxy Servers from the CM Portal 5.0 or greater.



You may also want to check for the latest information available on this topic on the [HP Support](#) web site.

To install the CM Proxy Server to a remote location

- 1 Access the CM Portal from any web browser using the URL, Username and Password assigned by your CM Portal administrator.
- 2 Navigation to the location where you want to install the CM Proxy Server. For example, you can select a single device from the Devices container or you can select a group of devices from the Groups container.



If a group of devices is selected as the audience (target), the CM Proxy Server will be installed on all members of the group.

- 3 From the Operations task group, click **Install Proxy Server**.
- 4 Click **Next**.

The Install Proxy Server—RPS Options dialog box opens.



Install Proxy Server

- 1 Query – 2 Select – 3 **RPS
Opts** – 4 Schedule – 5 Summary

Install Options

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:

Next Back Cancel

- 5 In the CM-CS Host Name text box, type the name or IP address for the CM Configuration Server.
- 6 In the CM-CS Port number text box, type the port number for the CM Configuration Server.
- 7 In the User text box for Install Options, type the user ID to use to connect to the CM Configuration Server.
- 8 If available, select which RPS configuration file to use during the installation from the RPS Config File drop-down list. This field only appears if multiple customized `rps.cfg` configuration files have been added to the CM Portal.
 - ▶ To make customized CM Proxy Server configuration files available for selection during this task, see [Preparing and Locating Configuration Files for Remote Proxy Server Installs](#) on page 43.
- 9 In the User text box for Remote CM Agent Credentials, type the administrator ID to obtain administrative authority on the target device's domain.
 - ▶ In order to take advantage of the Install Proxy Server task, consider creating a standard administrator ID across the domains in your network.
- 10 (*Windows only*) 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.

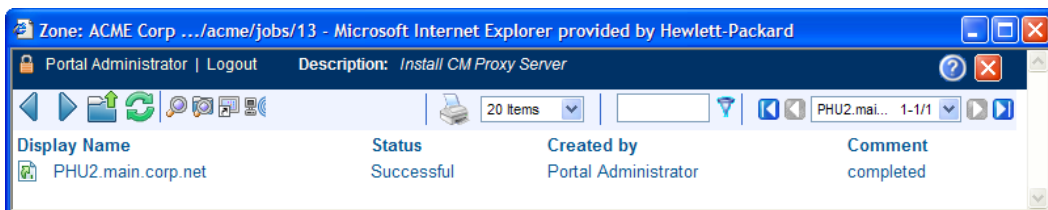
12 In the Schedule dialog box, specify when you want this job to run. See *Scheduling Jobs* in the *CM Portal Guide* for more information.






13 Click **Next**.


The Install Proxy Server—Summary dialog box opens.

14 Click **Submit**.

The Job Status page opens for this job. The page automatically refreshes every 60 seconds or when there is a status change. Press **F5** to manually refresh it.



- Click  to go up one level in the job or directory tree. For example, after viewing job details, click this icon to return to the Job Group Summary.
- Click  if you want to refresh the status of the installation.
- Click  to view detailed properties for the job or job group. This gives you detailed information on the job status.
- Click  to add a shortcut for Jobs to your Desktop.
- Click  to obtain a printable view of the Jobs Status page.

15 When you are done viewing the job status, click  to close the Job Status page, and return to the CM Portal.

You have finished installing the CM Proxy Server. The HP OVCM Integration Server service is automatically started at the end of the installation.



All devices running a CM Proxy Server can be found in the **Zone** → **Cross References** → **Infrastructure Services** → **Proxy Server** group container of the CM Portal. See *About the Zone Containers* in the *CM Portal Guide* for more information.

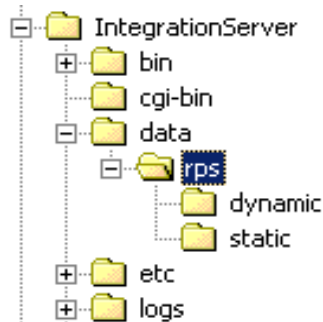
CM Proxy Server Directory Structure

The CM Proxy Server is installed, by default, into the following folders:

- For Windows, `Drive:\Program Files\Hewlett-Packard\CM\IntegrationServer`.
- For UNIX, `/opt/HP/CM/IntegrationServer`

Installing the CM Proxy Server adds the following subdirectories to the `IntegrationServer\data` folder, which store the Proxy Server's dynamic and static cache.

Figure 5 CM Proxy Server directory structure



Applying Product Updates

Product updates for licensed users of the CM Proxy Server are available for download from the [HP Support](#) web site.

- Check this site after installing the product from the CM infrastructure media to see if later software patch updates are available to bring the product to the latest level.
- Check this site on a regular basis to learn about available product maintenance.

Configuring the CM Proxy Server

CM Proxy Server Configuration File Overview

The CM Proxy Server installation creates a configuration file, `rps.cfg`, located in the `/etc` folder of the CM Proxy Server base installation directory. Following a local install, review the configuration parameters and make modifications to the `rps::init` section for the front-end communications protocol or the static or dynamic cache. [Table 4](#) on page 50 defines all parameters in the `rps.cfg` file and their default values.

Sample `rps.cfg` File After an Installation

The code below shows a sample `rps.cfg` file after product installation. Your `rps.cfg` file may show additional entries.

```
rps::init {  
  
    -httpd                1  
    -httpd-prefix         "/RESOURCE"  
  
    -static-root          "C:/Program~/Hewlett-Packard/CM/IntegrationServer/  
data/rps/static"  
    -static-trace         0  
    -static-type          agent  
    -static-host          localhost  
    -static-port          3464  
    -static-user          RPS  
    -static-ssl           0  
  
    -dynamic              0  
    -dynamic-root         "C:/Program~/Hewlett-Packard/CM /IntegrationServer/  
data/rps/dynamic"  
    -dynamic-prefix       "/RESOURCE"  
    -dynamic-url          "http://upstream:3466"  
    -dynamic-trace        0  
    -dynamic-maxsizeMB    0  
    -dynamic-makeidx      1  
  
}  
#  
# END OF CONFIG  
#  
# DO NOT REMOVE  
#  
rps::start
```


By default, after the installation:

- 1 Http front-end protocol is enabled; Stager front-end protocol (for TCP) is disabled.
- 2 Static cache is configured with entries from the install. The `-static-root` entry defines the data store location, and the `-static-host`, `-static-port` and `-static-user` entries define the static cache preload operation.
- 3 Dynamic cache operations are disabled.

Refer to the following topics to configure your `rps.cfg` file:

- [RPS.CFG Configuration Parameters Table](#), below. This defines all of the configuration parameters available in this release.
- [Configuring the Dynamic Cache Parameters](#) on page 56.
- [Configuring the CM Proxy Server for an Internet Proxy \(Firewall\) Environment](#) on page 62.
- [Co-Locating a CM Proxy Server with a CM Configuration Server for HTTP Support](#) on page 63.

RPS.CFG Configuration Parameters Table

[Table 4](#) on page 50 summarizes the parameters in the `rps.cfg` file and their default values. Parameters are listed in alphabetical order.

The configuration parameters in the `rps.cfg` file fall into three categories:

- **Front-end CM agent communication options: `-httpd (http)` or `-stager (TCP/IP)`**
By default, the CM Proxy Server is configured with the `-httpd` front end enabled. This uses the HTTP front end protocol to communicate with CM agents. When needed, the `-stager` front-end option is also available to communicate with agents using TCP/IP; for details, see [Using TCP/IP for CM agent Communication](#) on page 85.
- **Static cache settings**
The group of `-static*` parameters configure the static cache and its TCP connection to the CM Configuration Server to obtain a preload resolution. Modify the `-static*` parameters in the `rps.cfg` file to change the values set during the installation or to set additional options, such as tracing.



To configure a CM Proxy Server co-located with the CM Configuration Server, you need to modify the static cache parameters after installation. See the topic [Co-Locating a CM Proxy Server with a CM Configuration Server for HTTP Support](#) on page 63.

- **Dynamic cache settings**
The dynamic cache is not configured during the install. You must manually enable it (that is, change `-dynamic` from 0 to 1 in `rps.cfg`) and specify its options by editing the `rps.cfg` file. For details, see [Configuring the Dynamic Cache Parameters](#) on page 56.

Table 4 Configuration file `rps.cfg` parameters

Parameter	Default	Description
<code>-dynamic</code>	0	When set to 1, the dynamic cache is enabled and an entry in <code>-dynamic-url</code> is required to specify the upstream host. When set to 0, the dynamic cache is disabled, and all <code>-dynamic*</code> parameters are disregarded.
<code>-dynamic-allow-shared-resource-purge</code>	0	When set to 0, safeguards against purging dynamic cache from a CM-CSDB. Recommend keeping at 0. Set to 1 to remove the safeguard.
<code>-dynamic-defdmn</code>		HTTP upstream URL (CM Configuration Server's) domain.
<code>-dynamic-defcls</code>		HTTP upstream URL (CM Configuration Server's) class.
<code>-dynamic-freespace</code>	10	A percentage of the <code>-dynamic-maxsizeMB</code> to be left as free disk space after executing a size-based purge. The default is 10 %. When a size-based purge is triggered, the purge will delete files until the cache file size is reduced by this percentage below the maximum size. Used with <code>-dynamic-maxsizeMB</code> .

Parameter	Default	Description
-dynamic-largefile-mindays	0	Specifies the minimum days a 'large file' should be retained (during a size-based purge). Disabled when set to 0 (default). Used with <code>-dynamic-maxsizeMB</code> and <code>-dynamic-largefile-size</code> .
-dynamic-largefile-size	0	Specifies the size of a 'large file' in bytes. To specify the size in MB, enclose in quotation marks, such as "250 mb". When not equal to 0, files of this size or greater are excluded from deletion during the first pass of a size-based purge. Disabled when set to 0 (default). Used with <code>-dynamic-maxsizeMB</code> .
-dynamic-maxdays	7	The number of days to keep un-requested resources in the dynamic cache (if a file is regularly requested, it would never be deleted). Defines "aged" files for dynamic cache cleanup. Files that have not been requested for longer than this period are deleted from the cache whenever the Purge Dynamic Cache task is run from the CM Portal, and whenever the dynamic index file is saved. (See <code>-dynamic-savetod</code> and <code>-dynamic-savefreq</code> for frequency.)
-dynamic-maxsizeMB	0	Maximum size of dynamic cache. 0 indicates no maximum. To set a maximum size, enter the number of MB, such as 200 for 200 MB.
-dynamic-makeidx	1	When set to 0, turns off making the dynamic cache idx file (no purge). A date-based purge of aged files is performed whenever the index file is saved. (See <code>-dynamic-maxdays</code>).
-dynamic-prefix	"/RESOURCE"	HTTP upstream URL prefix (append <code>Domain.Class.OID</code>).

Parameter	Default	Description
-dynamic-proxy-host	""	To pass through an Internet proxy machine or a Firewall proxy when connecting to the Dynamic Cache Upstream Host machine, enter the Internet proxy's hostname or IP address.
-dynamic-proxy-pass	""	To pass through an Internet proxy machine or a Firewall proxy when connecting to the Dynamic Cache upstream host machine, enter the connecting User's password.
-dynamic-proxy-port	""	To pass through an Internet proxy machine or a Firewall proxy when connecting to the Dynamic Cache Upstream Host machine, enter the Internet Proxy port number to use.
-dynamic-proxy-user	""	To pass through an Internet proxy machine or a Firewall proxy when connecting to the Dynamic Cache Upstream Host machine, enter the connecting User name.
-dynamic-root	See description.	The fully-qualified location to store the dynamic cache. For example: "C:/Program Files/Hewlett-Packard/CM/IntegrationServer/data/rps/dynamic"
-dynamic-savefreq	90	When <code>-dynamic-savetod</code> is disabled (-1), specifies how often (in minutes) to save index file and cleanup cache. The save index file process is skipped when there are no changes to be applied.
-dynamic-savetod	-1	Specifies time of day (hh:mm:ss) to save dynamic index file and cleanup cache each day. Overrides <code>-dynamic-savefreq</code> . Disabled when set to -1. The save index file process is skipped when there are no changes to be applied.
-dynamic-ssl	0	When set to 1, enables the SSL protocol for use with an Internet proxy.

Parameter	Default	Description
-dynamic-trace	0	When set to 1, information is recorded for diagnostic tracing.
-dynamic-url	"http://upstream:3466"	<p>HTTP upstream URL (append <code>prefix</code>). Replace <code>upstream</code> with the upstream host the CM Proxy Server makes a connection with for obtaining dynamic cache. The upstream host can be CM Proxy Server co-located with the CM Configuration Server, or another CM Proxy Server. To change the default port (3466) modify the <code>PORT</code> setting in the <code>httpd.rc</code> file located in the <code>/etc</code> directory where you installed the CM Proxy Server.</p> <p>Optionally, define multiple upstream hosts for fail-over support. Enclose all entries in one set of quotation marks. Space separate each upstream host. For example:</p> <pre>"http://upstream1:3466 http://upstream2:3466"</pre>
-httpd	1	When set to 1, HTTP front end is enabled, supporting HTTP communication with CM agents. Do not change.
-httpd-prefix	"/RESOURCE"	The URL prefix registered to CM Integration Server. Do not change.
-httpd-trace	0	This parameter is reserved for future use.
-stager	0	Staging on or off. When set to 1, the stager (native TCP/IP) front end is enabled. Not recommended for use with current agents. Typically used to transition only from older agents.
-stager-addr	0.0.0.0	Restricts IP address used by CM Proxy Server (if using multiple IP addresses on one computer).
-stager-port	3461	Listening port used by the stager front end.

Parameter	Default	Description
-stager-trace	0	When set to 1, information is recorded for diagnostic tracing.
-static-host	localhost	Agent upstream host (example, CM Configuration Server). Used for initiating the Preloader connect. Replace with IP address of the upstream host.
-static-logsize	1000000	Specifies the size of the Preloader <code>connect.log</code> file in bytes. <code>connect.log</code> is in the CM Integration Server's <code>/logs/rps</code> folder. When the logsize is reached, a backup file (<code>.BAK</code>) is created. By default, this file is <code>connect.bak</code> . If a backup file already exists, it will be overwritten.
-static-port	3464	Agent upstream TCP port. Used during preload.
-static-proxy-host	""	To pass through an Internet proxy machine or a Firewall proxy when connecting to the Agent upstream host during Preload, enter the Internet proxy's hostname or IP address.
-static-proxy-pass	""	To pass through an Internet proxy machine or a Firewall proxy when connecting to the Agent upstream host during the Preload, enter the connecting User's password.
-static-proxy-port	""	To pass through an Internet proxy machine or a Firewall proxy when connecting to the Agent upstream host during the Preload, enter the Internet Proxy port number.
-static-proxy-user	""	To pass through an Internet proxy machine or a Firewall proxy when connecting to the Agent upstream host during the Preload, enter the connecting User name.
-static-root	<i>See description</i>	The fully qualified location of the Preloader's data store (IDMDATA). For example: "C:/Program Files/Hewlett-Packard/CM/IntegrationServer/data/rps/static"

Parameter	Default	Description
-static-type	agent	When set to agent, the static cache is populated by the Preloader. Set to server to point the cache to a native CM-CSDB (where the CM Proxy Server is installed on the same computer as the CM Configuration Server).
-static-ssl	0	When set to 1, indicates the Preloader is to use SSL.
-static-trace	0	When set to 1, information is recorded for diagnostic tracing.
-static-user	RPS	Agent upstream identity on the CM-CSDB in Primary.Policy.User (ZUSERID). Used during preloading. The services connected to this user ID will be preloaded into the static cache on the CM Proxy Server.

Editing the RPS.CFG File

To edit the RPS.CFG File

Before modifying the `rps.cfg` file, stop the service for the CM Proxy Server. See [Starting and Stopping the CM Proxy Server for Windows](#) on page 90 or [Starting and Stopping the CM Proxy Server for UNIX](#) on page 41.

- 1 Make your modifications to the `rps::init` section of the `rps.cfg` file.
- 2 After making your modifications, restart the service.

Syntax Notes

- When the following parameters are disabled (that is, set to 0), all other options related to the parameter are disregarded:

-dynamic
-httpd
-stager

For example, if `-dynamic` is 0, the entire set of `-dynamic*` parameters are disregarded.

- Use quotation marks to enclose entries that include special characters or spaces. For example, the following `-dynamic-root` entry uses quotation marks to enclose the fully-qualified location of the dynamic cache store.

```
-dynamic-root "C:/Program Files/Hewlett-Packard/CM/
IntegrationServer/data/rps/dynamic"
```

- Use slashes [/] to specify the paths for the `-dynamic-root` and `-static-root` parameters in both Windows and UNIX environments. For example:

```
-dynamic-root "C:/Program Files/Hewlett-Packard/CM/
IntegrationServer/data/rps/dynamic"
```

Configuring the Dynamic Cache Parameters

When dynamic caching is enabled, agent requested resources not available on the CM Proxy Server's local cache would be requested on demand from a designated upstream host. The resources are downloaded from the upstream host using HTTP, placed in the dynamic cache of the CM Proxy Server, and provided to the CM agent.



Dynamic cache use is never recommended for a CM Proxy Server co-located with a CM Configuration Server. For details, please see [Co-Locating a CM Proxy Server with a CM Configuration Server for HTTP Support](#) on page 63.

The minimal `rps.cfg` entries required for dynamic caching are simply the `-dynamic` and `-dynamic-url` parameters, which enable the dynamic cache and define the upstream URL for obtaining the requested files. (The `-dynamic-root` location is set during the install.)

```
rps::init {
...
    -dynamic 1
    -dynamic-url http://<upstream>:3466
...
}
```

The balance of the dynamic cache entries are optional. If absent from the `rps::init` section, the default values are assumed. Use Table 5 as a guide to configuring the dynamic cache for your environment.



See [Table 4](#) on page 50 for complete definitions of each parameter listed in [Table 5](#) on page 57.

Table 5 Dynamic Cache parameter summary

Objective	RMS.CFG Parameters to Use
Specify an upstream host and http port; either a CM Configuration Server enabled for HTTP downloads, or another CM Proxy Server. Specify multiple hosts for fail-over support. Required.	-dynamic 1 -dynamic-url "http://upstream:3466" or -dynamic-url "http://upstream:3466 http://upstream2:3466 http://upstreamN:3466"
Specify where to store the dynamic cache on the CM Proxy Server.	-dynamic-root
Save the index file that is used to track when files were last requested. A save also purges "aged" dynamic cache files not requested in a specific number of days. Schedule the index file save daily or every <i>nn</i> minutes. Note: A scheduled index file save (and thus the data-based purge) is skipped if there are no changes in the index file at that time.	-dynamic-maxdays -dynamic-makeidx -dynamic-savefreq -dynamic-savetod
Set a maximum cache size. If the maximum cache size is exceeded, the least recently used files are deleted until the maximum size is reached. Options: <ol style="list-style-type: none">1 Set a low-water mark (freespace) for a size-based purge.2 Define 'large files' to be exempt during the first pass of the size-based delete.	-dynamic-freespace -dynamic-maxsizeMB -dynamic-largefile-size -dynamic-largefile-mindays
Revise the safeguard against purging the dynamic cache stored on a shared resource, such as the CM Configuration Server.	-dynamic-allow-shared-resource-purge

Objective	RMS.CFG Parameters to Use
Set diagnostic tracing.	-dynamic-trace
Provide server, port, user, and password information to pass through an Internet Proxy or Firewall required to connect to the upstream host. Also, enable SSL protocol.	-dynamic-proxy-host -dynamic-proxy-port -dynamic-proxy-user -dynamic-proxy-pass -dynamic-ssl
Override the default prefix.domain, and class OID for obtaining resources from the upstream URL. Not normally needed.	-dynamic-prefix -dynamic-defdmn -dynamic-defcls

Coding Multiple Upstream Hosts for Dynamic Cache Fail-over Support

When dynamic cache is enabled, the upstream host and port are defined in the `-dynamic-url` parameter of the `rps.cfg` configuration parameter. Multiple hosts may now be specified in the `-dynamic-url` parameter, using a blank separated list, to provide for a second, third, or more, upstream host with which to attempt to connect if a connection with the previously listed host fails. If all defined hosts in the list fail, an error will be returned to the CM Proxy Server user.

For example, if you code the `-dynamic-url` as:

```
-dynamic-url "http://111.111.111.11:3466 http://upstream2:3466 http://upstream3:3466"
```

the CM Proxy Server will first attempt to connect to **http://111.111.111.11** on port 3466 to obtain its dynamic cache. If that connection fails, it will attempt to connect to the second upstream host in the list, **http://upstream2** on port 3466. If the second connection fails, it will attempt the third entry, **http://upstream3** on port 3466. If the third connection fails, an error message is generated.



Use one set of quotation marks to enclose the entire list of upstream hosts. Otherwise, you will receive a syntax error.

The Date-Based Purge of the Dynamic Cache

Every time a file is requested from the Dynamic Cache, the request date is recorded and maintained. If a file has not been requested in a pre-defined maximum number of days, it is deleted whenever a date-based purge occurs. Use the `-dynamic-maxdays` parameter in `rps.cfg` to specify the maximum number of days to keep unrequested files in the dynamic cache. The default is 7 days.

A date-based purge can be triggered in the following ways:

- 1 Explicitly from the CM Portal by running the task: Purge Dynamic Cache. See the later topic, [Purging the Dynamic Cache using the CM Portal](#) on page 93.
- 2 Whenever the dynamic cache index file is saved. For details, see the following topic, [Saving the Index File](#).

Saving the Index File

An index file is maintained to keep track of when files in the Dynamic Cache were last used. Every so often this index file is saved to update the “last-used” date in the dynamic cache files. Whenever the index file is saved, a date-based purge of the dynamic cache also takes place to cleanup “aged” files.

The schedule for saving the index file is established using either the `-dynamic-savetod` or `-dynamic-savefreq` parameters. Use the `-dynamic-savefreq` parameter to schedule the index file save process every `nn` minutes.



For a date-based purge to occur, the index file save process must run. The index file save process is skipped when there are no changes to be applied to it. Therefore, if a dynamic cache has had no resources requested of it or added to it since a previous save, the index file save is skipped and the date-based purge is also skipped.

To use either of these options, first ensure the following dynamic cache parameters are specified:

```
-dynamic 1
-dynamic-makeidx 1
-dynamic-maxdays <max days to hold unrequested files>
```

- Use the `-dynamic-savetod` parameter to set a daily schedule for saving the dynamic index and purging the dynamic cache. A `-dynamic-savetod` entry overrides a `-dynamic-savefreq` entry. Valid values are `-1` (disabled) or `hh:mm:ss`. Seconds may be omitted.

Example: To set a time-of-day for the purge to occur daily, use the `-dynamic-savetod` parameter with the time specified in the format `hh:mm:ss`. For example, the following set of parameters will automatically run a purge of the dynamic cache each day at 3:00 AM to delete files that have not been requested for seven days.

```
-dynamic          1
-dynamic-makeidx  1
-dynamic-maxdays 7
-dynamic-savetod 3:00
```

- If `-dynamic-savetod` is not specified, use the `-dynamic-savefreq` parameter to specify how often (in minutes) to save the index file and purge the dynamic cache.

Example: The following set of parameters automatically runs a purge of the dynamic cache every 120 minutes for files unrequested for seven days.

```
-dynamic          1
-dynamic-makeidx  1
-dynamic-maxdays 7
-dynamic-savefreq 120
```

Specifying a Size-Based Purge of the Dynamic Cache

Use the following options to automatically have files deleted from the dynamic cache to keep its size in check.

- Automatically run a size-based purge when the maximum size is exceeded.

The maximum size of the dynamic cache is specified in the `-dynamic-maxsizeMB` parameter in `rps.cfg`. When this maximum size is exceeded, a size-based purge of the dynamic cache will run automatically, purging the least recently used files until the target size is reached.

For example, the following entries specify an automatic purge of the least recently used files if the dynamic cache exceeds 300 MB. The purge process deletes the least recently used files until the cache is below the maximum size, or, to the size required by the new `-dynamic-freespace` parameter (next feature).

```
-dynamic 1
-dynamic-maxsizeMB 300
```

- Define a "freespace" amount to be available after a size-based dynamic cache purge

When a size-based purge is triggered, you may specify a `-dynamic-freespace` option to purge the dynamic cache down to a low-water mark (as a percentage of the maximum file size). This allows you to bring the cache size down to a predefined manageable size whenever it reaches the maximum file size. Use this option to eliminate repetitive calls to the purge process if upstream downloads occur frequently.

To specify the `-dynamic-freespace` parameter, define a percentage of free space required upon completion of a size-based purge. For example: the following options will trigger a purge of the dynamic cache when it reaches 300 MB, and will purge the least recently used files until the dynamic cache size is more than 10% below 300, or under 270 MB.

```
-dynamic 1
-dynamic-maxsizeMB 300
-dynamic-freespace 10 <percentage below the maxsizeMB
after the purge>
```

- Exempt large files from the first-pass of a size-based purge

Normally, when a size-based purge takes place, the least recently used files are purged from the dynamic cache first. If large files are purged and then later requested, an undue load could be placed on the network. Use the following two "large file" parameters to allow the purge process to skip over the files that meet these large file criteria during an initial purge.

```
-dynamic-largefile-size <defines minimum large file size,
in bytes>
-dynamic-largefile-mindays <defines minimum days large files
stay in cache>
```

Example: The following entries define large files as "25 MB" and the minimum number of days to remain in the cache as 15. So, the first pass of the purge will exempt files 25 MB or larger that have remained in the cache less than 15 days, even if they meet the normal "least recently used" criteria.

```
-dynamic 1
-dynamic-maxsizeMB 300
-dynamic-freespace 10
-dynamic-largefile-size "25 MB"
-dynamic-largefile-mindays 15
```

If, after purging the non-large files, the desired (reduced) cache size is not achieved, then the purge process will be repeated without regard to the large file settings.

Configuring the CM Proxy Server for an Internet Proxy (Firewall) Environment

The following examples illustrate how to use the set of `-static-proxy*` and `-dynamic-proxy*` configuration parameters that provide support for environments with an Internet proxy or firewall server. Use these parameters to define the host, port, user name and passwords needed to pass through the firewall or Internet proxy for a static cache preload or a dynamic cache request.

Examples of TCP Parameters for Static Cache Preloader

The static cache Preloader uses TCP to connect to the CM Configuration Server for the initial resolution. In the examples below, 443 is defined in order to get through a firewall, which typically opens ports 80 and 443.

- **Simple Connection**

```
-static-host      "<RCS IP Address or hostname">
-static-port      3464
```

- **Connection through Web Proxy**

```
-static-proxy-host      "<Web-Proxy IP address or Hostname>"
-static-proxy-port      8080
-static-host            "<RCS IP Address or Hostname>"
-static-port            443
```

- **Connection through Web Proxy performing Basic User Authentication**

```
-static-proxy-host      "<Web-Proxy IP address or Hostname>"
-static-proxy-port      8080
-static-proxy-user      "<Web-Proxy Username>"
-static-proxy-pass      "<Web-Proxy Password>"
-static-host            "<RCS IP Address or Hostname>"
-static-port            443
```

Examples of HTTP Parameters for Dynamic Cache PassThru

The dynamic cache uses an HTTP port to connect to a CM Configuration Server enabled for HTTP-download support, or another CM Proxy Server.

Additional dynamic cache parameters are available to pass through an Internet or Firewall Proxy, with or without basic user authentication. The following examples illustrate how to use these Firewall Proxy parameters.

- **Simple Connection to upstream HTTP host and port**

```
-dynamic          1
-dynamic-url      http://upstream:3466
```

- **Connection through Web Proxy**

```
-dynamic          1
-dynamic-url      http://upstream:3466
-dynamic-proxy-host  "Web-Proxy IP Address or Hostname"
-dynamic-proxy-port 8080
```

- **Connection through Web Proxy performing Basic User Authentication**

```
-dynamic          1
-dynamic-url      http://upstream:3466
-dynamic-proxy-host  "Web-Proxy IP address or Hostname"
-dynamic-proxy-port 8080
-dynamic-proxy-user  "Web-Proxy-username"
-dynamic-proxy-pass  "Web-Proxy-Password"
```

Co-Locating a CM Proxy Server with a CM Configuration Server for HTTP Support

The CM Configuration Server does not provide native HTTP download capability. When you use a CM configuration that requires obtaining resources from the CM-CSDB using HTTP, you need to co-locate a CM Proxy Server on the same machine as the CM Configuration Server. The co-located CM Proxy Server is defined with a static type of server, instead of agent. This means it does not store its own static cache, but merely points to that of the CM-CSDB. It does not need to be preloaded.

Configurations that Require a Co-located CM Proxy Server

You need a CM Proxy Server co-located with the CM Configuration Server to provide HTTP download support in the following configurations:

- To support CM agents configured to obtain their resources from the CM-CSDB using HTTP, instead of TCP/IP.

- To support a subordinate, or downstream, CM Proxy Server, configured to obtain its dynamic cache from the CM-CSDB.
- To preload a subordinate, or downstream, CM Proxy Server from the CM-CSDB using HTTP, instead of TCP/IP.

For details on each of these configurations, see [When to use a Co-located CM Proxy Server](#) on page 25.

Once you co-locate a CM Proxy Server on the CM Configuration Server, you can use its IP address and port number (generally: 3466) to obtain the CM-CSDB resources using HTTP.

Installing and Configuring a Co-located CM Proxy Server

Use these procedures to establish a co-located CM Proxy Server with your CM Configuration Server in order to service HTTP requests for resources to be downloaded from the CM-CSDB.



The ability to service HTTP requests was previously provided through ZHTTPMGR, which is no longer supported. A co-located CM Proxy Server provides improved performance and scalability over ZHTTPMGR for enabling the CM Configuration Server for HTTP communications. Steps to remove ZHTTPMGR begin on page 66.

To install and configure a co-located CM Proxy Server

- 1 Install the CM Proxy Server on the same machine as the CM Configuration Server. Accept the default values throughout the install prompts.
For details, see [CM Proxy Server Installation](#) topics on page 33.
- 2 For Windows, stop the HP OVCM Integration Service (which starts automatically after the CM Proxy Service is installed).
- 3 Modify the following `rps.cfg` file parameters using the guidelines given in [Table 6](#) on page 65. The `rps.cfg` file is located in the `/etc` folder of the base install directory.



See [Table 4](#) on page 50 for a complete listing of `rps.cfg` parameters.

Table 6 Configuring the RPS.CFG file for a co-located CM Proxy Server

Parameter	Default	Set to this Value	Description
-static-root	See description	See description	The fully qualified location of the Preloader's data store. Enter the location of the CM-CSDB. Use slashes (/) as delimiters in the entry for Windows as well as UNIX. By default, this location is: Windows: C:/Program Files/Hewlett-Packard/CM/ConfigurationServer/DB UNIX: /opt/HP/CM/ConfigurationServer/DB
-static-type	agent	server	Set to server to point the static cache to a native CM-CSDB.
-dynamic	0	0	Use of the dynamic cache is NOT RECOMMENDED for a co-located CM Proxy Server. For details, see Safeguarding the CM-CSDB from a Dynamic Cache Purge on page 66.

Here's a sample `rps.cfg` file configured for a CM Proxy Server co-located with the CM Configuration Server.

```
rps::init {
    -httpd 1
    -httpd-prefix "/RESOURCE"
    -static-root "C:/Program Files/Hewlett-Packard/CM/
ConfigurationServer/DB"
    -static-type server
    -static-trace 0
    -static-host <leave default>
    -static-port 3464
    -static-user RPS
    -static-ssl 0
    -dynamic 0
    -dynamic-root <leave default>
    -dynamic-url http://upstream:3466 <leave default>
    -dynamic-trace 0
    -dynamic-maxsizeMB 0
    -dynamic-makeidx 0
}
```

```
}  
#  
# END OF CONFIG  
#  
# DO NOT REMOVE  
#  
rps::start
```

- 4 Restart the co-located CM Proxy Server.
- 5 If necessary, switch the dynamic cache upstream port number (specified in the `-dynamic-url` parameter of `rps.cfg`) for any CM Proxy Servers that were previously pointing to the CM Configuration Server port as its upstream host. These CM Proxy Servers should now point to the co-located CM Proxy Server port (3466) as their upstream port.

Safeguarding the CM-CSDB from a Dynamic Cache Purge

The recommended approach for configuring a CM Proxy Server co-located with the CM Configuration Server is to point the static cache at the CM-CSDB, set the `-static-type` to `"server"`, and disable the dynamic cache.

The CM Proxy Server includes automatic protection to guard against purging files from the CM-CSDB in the event that a co-located CM Proxy Server's dynamic cache is enabled. The `-dynamic-allow-shared-resource-purge` parameter, when set to 0 (default), prevents CM-CSDB files from being deleted during any dynamic cache purge process. This might occur when a co-located CM Proxy Server is unusually configured (against recommendation) as follows:

- dynamic cache is enabled
- dynamic cache root points to the CM-CSDB.

Using the default (`-dynamic-allow-shared-resource-purge` set to 0) protects your CM-CSDB from any dynamic cache purges.

Setting the parameter to 1 removes the safeguard and allows a purge of dynamic-cache files from the CM-CSDB.

Removing the Use of ZHTTPMGR for HTTP Support

If you previously used ZHTTPMGR to enable your CM Configuration Server for HTTP, you should remove that support and replace it with a co-located CM Proxy Server.

To remove ZHTTPMGR support from a CM Configuration Server

- 1 Locate the CM Configuration Server Settings file, EDMPROF. The specific EDMPROF file name and location for Unix and Windows are listed below:
 - On UNIX operating systems, it is `.edmprof`, located on the home directory of the UNIX user ID that installs, starts, stops, and maintains the CM Configuration Server.
 - On Windows operating systems, it is `edmprof.dat`, located in the `bin` folder of the CM Configuration Server directory.

If a CM Configuration Server was enabled for HTTP support through the use of ZHTTPMGR, the EDMPROF file will have the following entries in the `MGR_ATTACH_LIST` and `MGR_HTTP` sections:

```
[MGR_ATTACH_LIST]
CMD_LINE=(zhttpmgr ADDR=RCS_IP_Addr, PORT=8080) RESTART=YES

[MGR_HTTP]
HTTP_PORT=8080
```

- 2 In the `[MGR_ATTACH_LIST]` section, comment out the `CMD_LINE` entry for `zhttpmgr`.
- 3 In the `[MGR_HTTP]` section, comment out the `HTTP_PORT` entry.

Configuring the CM-CSDB for the Static Cache Preload

Each CM Proxy Server whose static type is set to `agent` (that is, not a CM Proxy Server co-located with the CM Configuration Server) requires a Preload entitlement policy defined in the CM-CSDB.

This Preload entitlement policy defines:

- The resources to be loaded onto the CM Proxy Server's static cache when the Preload runs.
- Where the resources should be distributed from and under which protocol. By default, the resources are distributed from the host CM Configuration Server using TCP.

The following additional preload configuration options are available, and discussed in the topic [Preloading Deployment Options](#) on page 71:

- Preload using HTTP from a co-located, or another, CM Proxy Server
- Preload using a Secure Socket Transfer (SSL) protocol
- Preload using multicast from a CM Configuration Server or another CM Proxy Server that has a co-located Multicast Server
- For Windows Installer Enabled Applications, the ACP resources to be loaded onto the CM Proxy Server, but not distributed to the CM agents. See [Preloading Windows Installer Enabled Applications](#) on page 81.

Use the following procedures to create a static cache desired-state policy entitlement in the CM-CSDB for each CM Proxy Server to be preloaded. This can be done before or after the CM Proxy Servers are installed and configured.

Creating the Entitlement Policy for a Static Cache Preload

To create the entitlement policy for the Preload of the Static Cache



This task requires a basic understanding of the CM-CSDB and how to create an entitlement policy. This topic is covered in the *Implementing Entitlement Policy* chapter of the *CM Application Manager and Application Self-service Manager Guide*.

- 1 Create a POLICY.USER instance in the CM-CSDB that matches the User ID entered during the CM Proxy Server install, or later specified in the `-static-user` parameter in the `/etc/rps.cfg` file. The User ID default is RPS. However, the User ID is often set to: `RPS_machine_name`.
- 2 Connect the POLICY.USER instance to the set of applications to be preloaded to the CM Proxy Server's static cache.



Alternatively, if multiple CM Proxy Servers require the same set of applications to be preloaded, create a PRIMARY.POLICY.WORKGRP instance to define the set of applications to be preloaded, and then connect each PRIMARY.POLICY.USER instance to the PRIMARY.POLICY.WORKGRP instance. For details, see [To configure a CM Proxy Server Workgroup to preload all database applications](#) on page 69.

For details on how to entitle a PRIMARY.POLICY.USER instance to application services, refer to the *Implementing Entitlement Policy* chapter of the *Application Manager and Application Self-service Manager Guide*.

To configure a CM Proxy Server Workgroup to preload all database applications

The following steps serve as one example of defining the applications to preload on a CM Proxy Server. This example preloads the CM Proxy Server with all available applications using a `POLICY.WORKGRP` instance. Your preload should specify the set of applications normally required by the CM agents assigned to that CM Proxy Server.

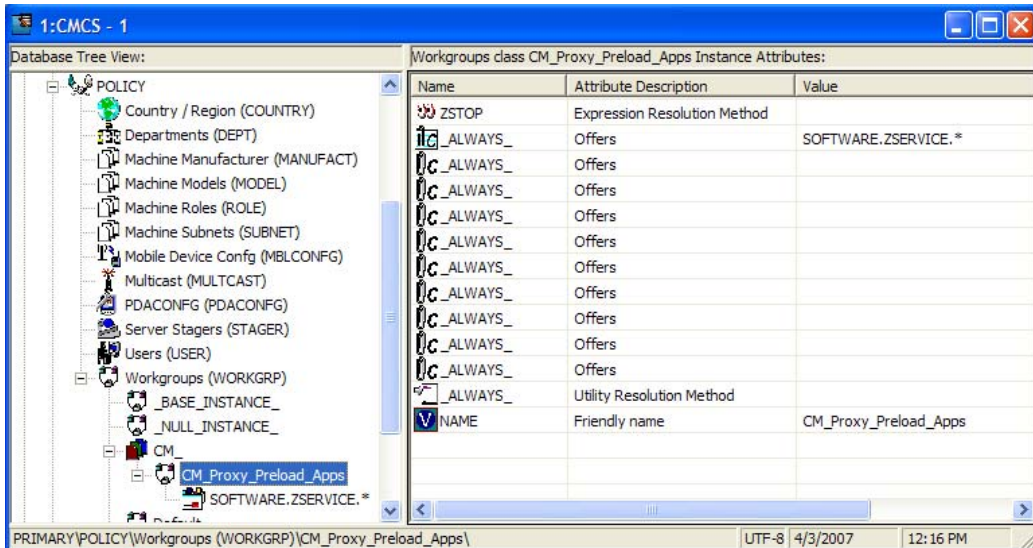
- 1 Use the CM Admin CSDB Editor to create a `PRIMARY.POLICY.WORKGRP` instance called `CM_PROXY_PRELOAD_APPS`.
 - a From the Start menu, select **Programs → HP OVCM Administrator → CM Admin CSDB Editor**.
 - b In the tree-view, double-click on the following icons to open them: **PRIMARY → POLICY → WORKGRP**.
 - c Right-click **WORKGRP** and select **New Instance** from the pop-up menu.

The Create Instance dialog box appears, allowing you to type a display name and an instance name. The display name defaults to the instance name if left blank.

- d Tab to the second text entry field below Create a new Workgroups (WORKGRP) instance named:.
 - e Type a name for the instance, for example: `CM_PROXY_PRELOAD_APPS`, and click **OK**.
- The `CM_` prefix of this instance is now displayed in the tree view and the full name of the instance is displayed in the list view.

- 2 Edit the instance to manually add an `_ALWAYS Offers` field value to preload all applications onto the CM Proxy Server. Details follow:
 - a Click on the **Workgroups (WORKGRP)** class entry in the tree view.
 - b Double-click on the **CM_Proxy_Preload_Apps** entry in the list view.
 - c Double-click on the top `_ALWAYS` attribute in the list view.
 - d In the edit instance dialog box, type the following Offers value:
`SOFTWARE.ZSERVICE.*`
 - e Click **OK**.

The following figure shows the `_ALWAYS` entry added to preload all applications.



- 3 Connect the PRIMARY.POLICY.USER instance for the CM Proxy Server(s) with this PRIMARY.POLICY.WORKGRP instance. Details on making this connection follow.



Refer to the Implementing Entitlement Policy chapter of the *CM Application Manage and Application Self-service Manager Guide* for comprehensive information on how to assign users to groups.

To connect a Policy User RPS instance to a Policy Workgroup instance

- 1 In the CM Admin CSDB Editor tree view, navigate to the PRIMARY.POLICY.USER class.
- 2 Double-click **Users** to expand the class instances.
- 3 Right-click on the **RPS** user instance that is to be connected to the Workgroup instance, and from the pop-menu that appears, click **Show Connections**.
- 4 In the resulting POLICY.CONNECTIONS dialog box, double-click the Class listing for **Workgroups**.

Now, CM_Proxy_Preload_Apps should be in the CSDB Editor list view of all Workgroup instances, and the Policy.User class should be open in the tree view.

- 5 Starting from the list view, use your mouse to drag the icon for the CM_Proxy_Preload_Apps workgroup instance over the selected RPS user instance in the tree view.



Your mouse icon changes to a paper-clip when you place it on the selected User.RPS instance. This indicates that the connection is allowed.

- 6 Complete the connection by dropping the CM_Proxy_Preload_Apps icon (by releasing the left mouse button) on the RPS user instance.

The Select Connection dialog opens, indicating a connection will be made between the selected User.RPS instance and the Workgroups.CM_Proxy_Preload_Apps instance.

- 7 Click **Copy** on the Select Connection dialog box to complete the _ALWAYS connection.

- 8 Click **Yes** to confirm the connection.

The User.RPS instance is connected to the Workgroups.CM_Proxy_Preload_Apps instance.

- 9 To test the preload, open a web browser window and type the following command:

```
http://CM_proxy_machine_name:3466/proc/rps/sync
```

For more information on using this command and where to check for the preloaded data files, see [Testing the CM Proxy Server Preload](#) on page 104.

To run the Preload from the CM Portal, see [Preloading the CM Proxy Server](#) on page 92.

Preloading Deployment Options

A CM Proxy Server's preload resolution is always performed on the host CM Configuration Server. However, there are several ways to configure the actual deployment of the static cache resources in a CM environment. These deployment options are set the same way that CM agents are configured to obtain their resources from the CM Proxy Server. For HTTP or HTTPS, this means associating a pre-configured STAGER instance with the CM Proxy Server's User instance in the CM-CSDB. For multicast, this means associating a pre-configured MULTICAST instance with a CM Proxy Server User or Workgroup instance in the CM-CSDB.

The configuration options for preloading the CM Proxy Server Static Cache include:

- [Preloading Using HTTP](#)
- [Preloading Using SSL \(TCPS or HTTPS\)](#)
- [Preloading Using Multicast](#)

These configuration options are discussed in the following topics.

You can also use the CM Portal to preload one or CM Proxy Servers. For more information, see [Preloading the CM Proxy Server](#) on page 92.

Preloading Using HTTP

By default, a CM Proxy Server's static cache is preloaded from the resources on the host CM Configuration Server using TCP. Use the following configuration steps to preload the static cache from the HTTP port of a co-located CM Proxy Server or another, pre-loaded, CM Proxy Server.

[To change the deployment source or protocol for a preload to use HTTP](#)

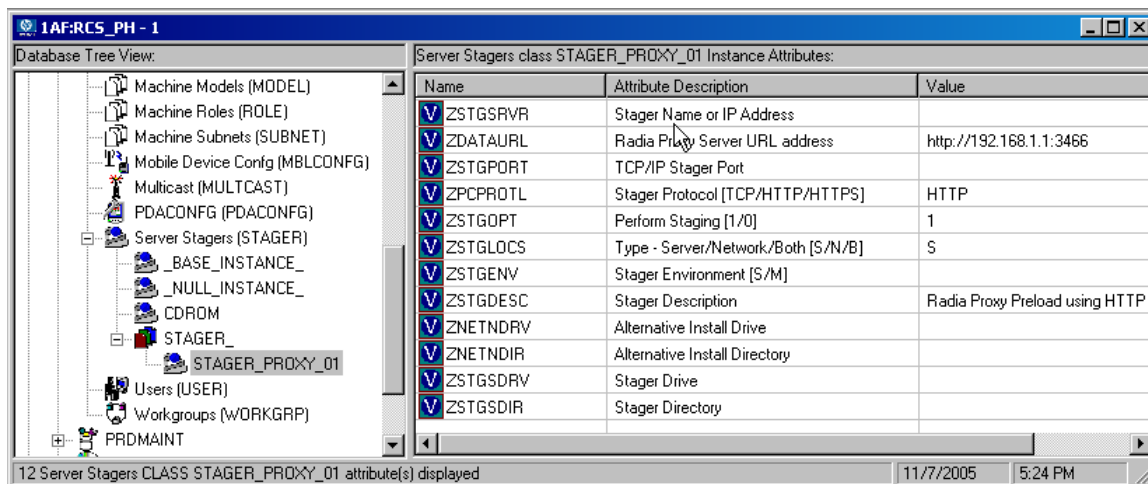
- 1 Using the CM Admin CSDB Editor, create a STAGER instance to be used to preload the CM Proxy Server from another CM Proxy Server, or to preload using the HTTP port of a co-located CM Proxy Server.
- 2 Set the **ZPCPROTL** and **ZDATAURL** attributes for the Stager instance to the values given in Table 7 below.

Table 7 shows the Stager instance attributes that are needed to preload a Proxy from a co-located or remote CM Proxy Server using HTTP.

Table 7 Stager Instance Attributes

Stager Attribute	Set to this Value
ZPCPROTL	HTTP
ZDATAURL	<code>http://<Your RPS IP Addr or Hostname>:3466</code> Replace <Your RPS IP Addr or Hostname> with the IP address or Hostname of the CM Proxy Server to be used to obtain the static cache Preload files, in lieu of the CM Configuration Server. For a co-located CM Proxy Server, this will be the same address as the CM Configuration Server.

The following figure shows the STAGER instance STAGER_PROXY_01 configured to preload using HTTP.



- 3 Locate the POLICY.USER instance for the CM Proxy Server that is to receive its preload using HTTP. This is usually named *RPS_machine_name*.
- 4 Associate the PRIMARY.POLICY.USER *RPS_machine_name* instance with the PRIMARY.POLICY.STAGER instance configured for a preload using HTTP.

When a CM Proxy Server connects to the CM Configuration Server for its Preload, its Preload distribution is resolved using the entries defined in its POLICY.USER instance. The connection to the STAGER_PROXY_01 instance means the Preload is deployed using HTTP from the CM Proxy Server URL specified in the STAGER instance.

Preloading Using SSL (TCPS or HTTPS)

The preload for a CM Proxy Server static cache can be obtained over a Secure Socket Layer (SSL) from a secured CM Configuration Server (this uses a secure TCP protocol, or TCPS) or from another, secured CM Proxy Server (this uses a secure HTTP protocol, or HTTPS).

Specific tasks related to using SSL to secure your CM Proxy Server preloads follow.

To preload using TCPS

Use these steps to enable CM Proxy Servers currently receiving their preloads from a CM Configuration Server using TCP to now use TCP over SSL (TCPS).

- 1 Refer to the *CM SSL Implementation Guide* for these SSL-related tasks:
 - Ensure the CM Configuration Server is configured for TCPS support.
 - Locate the required Certificate Authority files for SSL support on the CM Proxy Server.
- 2 On the CM Proxy Server machine receiving the preload, use a text editor to modify the `rps.cfg` file located in the `IntegrationServer\etc` directory. Establish the following settings:

```
rps::init {  
    -stager          0  
    -static-ssl     1  
    -static-port    <SSL port>
```

Where `<SSL port>` is the SSL port number on the secure CM Configuration Server. The default SSL port number is 443.

- 3 To apply these new `rps.cfg` file settings, restart the HP OVCM Integration Server service for the CM Proxy Server.
- 4 Execute the Proxy Preload using either of the following methods:
 - To manually run the proxy preload, open a web browser window and type the following command:
`http://cm_proxy_machine_name:3466/proc/rps/sync`
For more information on using this command and where to check for the preloaded data files, see [Testing the CM Proxy Server Preload](#) on page 104.
 - To run the Preload from the CM Portal, see [Preloading the CM Proxy Server](#) on page 92.

To verify the preload used a secure TCP protocol (TCPS), review the entries in the CM Proxy Server's preload log, `connect.log`. This log is located in the `IntegrationServer\logs\rps` directory. Look for the following entries:

```
Verified Certificate [C:\Program~\Hewlett~\CM\INTEGR~2\bin\rps\  
CACertificates\cacert.pem]
```

```
SSL Manager = <CM Configuration Server host or IP address>
```

```
SSL Port = 443
```

To Preload using HTTPS

Use these steps to enable CM Proxy Servers currently receiving their preloads from the HTTP port of another CM Proxy Server to now receive them using HTTP over SSL (HTTPS). The same steps apply whether or not the CM Proxy Server sending the preload resources is co-located with a CM Configuration Server or not.



See earlier topics in this guide for tasks related to:

- [Co-Locating a CM Proxy Server with a CM Configuration Server for HTTP Support](#) on page 63.
- [Preloading Using HTTP](#) on page 72.

- 1 Establish a secured CM Proxy Server that is the upstream source of your CM Proxy Server's preload using HTTP. Refer to the *CM SSL Implementation Guide* for full details on how to setup an SSL-secured CM Proxy Server. The tasks will include:

- Locating the required Certificate Authority files for SSL support.
- Verifying the CM Integration Server (for the CM Proxy Server) is configured for HTTPS support.

- 2 On a CM Proxy Server machine receiving the preload, use a text editor to modify the `rps.cfg` file located in the `IntegrationServer\etc` directory. Include a `-static-ssl` parameter set it to `1`, and make sure the `-stager` parameter is set to `0`.

```
rps::init {  
    -stager          0  
    -static-ssl     1  
    -static-port    <SSL port>  
}
```

Where `<SSL port>` is the SSL port number on the secured CM Proxy Server established in Step 1 above. The default SSL port number is 443.

- 3 To apply the new `rps.cfg` file settings, restart the HP OVCM Integration Server service for the CM Proxy Server receiving the preload.
- 4 Establish a PRIMARY.POLICY.STAGER instance as discussed in [Preloading Using HTTP](#) on page 72; however, use the values for ZPCPROTL and ZDATAURL given in [Table 8](#) on page 76. This table shows the Stager instance attributes needed to preload a CM Proxy Server using HTTPS.

Table 8 Stager Instance Attributes

Stager Attribute	Set to this Value
ZPCPROTL	HTTPS
ZDATAURL	<code>https://<RPS Source IP address>:<SSL_port></code> where <SSL port> is the SSL port number on the secured CM Proxy Server (see Step 1 on page 75). The default SSL port number is 443.

- 5 For each CM Proxy Server to be preloaded using HTTPS, associate its PRIMARY.POLICY.USER instance with this PRIMARY.POLICY.STAGER instance.
- 6 Execute the Proxy Preload as usual.

Preloading Using Multicast

A set of CM Proxy Servers can obtain their static cache preloads from an HP Configuration Management Multicast Server (CM Multicast Server). In this configuration, the CM Proxy Servers receiving their preload resources are configured the same way that CM agents are configured to receive resources from a multicast server.

The CM Proxy Server preloads can also receive their resources using the dynamic windows feature of a multicast server, as discussed on page 79.

To preload CM Proxy Servers using Multicast



HP recommends that administrators become thoroughly familiar with the operation of the CM Multicast Server before using it for a CM Proxy Server Preload. The CM Multicast Server is fully documented in the *HP Configuration Management Multicast Server Installation and Configuration Guide (CM Multicast Server Guide)*.

- 1 For each CM Proxy Server to participate in the preload, use the CM Admin CSDB Editor to create a POLICY.USER instance in the CM-CSDB that matches the User ID entered during the CM Proxy Server install, or later specified in the `-static-user` parameter in the `/etc/rps.cfg` file. The User ID default is RPS. However, the User ID is often set to: `RPS_machine_name`.

2 Using the CM Admin CSDB Editor, create a POLICY.WORKGROUP instance for the CM Proxy Servers to specify their desired state for the Preload of the Static Cache (as discussed on page 68). The procedure: [To configure a CM Proxy Server Workgroup to preload all database applications](#), shows an example using the friendly name CM Proxy Preload Apps.

3 Install and configure a CM Multicast Server. The CM Multicast Server can be co-located with the CM Configuration Server or co-located with another CM Proxy Server.

For detailed Multicast installation and configuration information, refer to the *CM Multicast Server Guide*.

4 Using the CM Admin CSDB Editor, also create a multicast policy instance just for Proxy Preloads. For example, follow these steps to create an instance named PRIMARY.POLICY.MULTICAST.MCPRELOAD.

5 Edit the MCPRELOAD instance attribute values.

- Set ALTADDRM to the IP address of where the CM Multicast Server is installed.
- Set CGMTDATE and CGMTTIME to specify a multicast session start date and time, in Greenwich Mean Time (GMT), so that the session will be active when the proxy preload command is to be executed.



The hours for the collection start time, CGMTTIME, are specified using a 24-hour (military) format.

- Also refer to the *CM Multicast Server Guide* for detailed information on the MULTICAST instance attributes and how to set their values.

The following figure illustrates an MCPRELOAD instance with CGMTDATE and CGMTTIME entries that will initiate a multicast session for the Proxy Preload on November 4, 2005 at 2 p.m. GMT.



The Proxy Preload command must be issued at the same time or shortly after the multicast collection session starts.

Database Tree View		Multicast class MCPRELOAD Instance Attributes:		
Name	Attribute Description	Value		
DOMAIN	Domain Name	&{ZOBJDOMN}		
CLASS	Class Name	&{ZOBJCLAS}		
INSTANCE	Instance Name	&{ZOBJNAME}		
MCAST	Enable Multicast [Y/N]	Y		
MODE	Broadcast or Multicast [M/B]	M		
MORDER	Service Installation Order [B/A/S]	5		
ADDRESS	Broadcast or Multicast Address	229.0.0.0		
PORT	Broadcast or Multicast UDP port	9512		
DELAYFP	Delay After First Packet (mil sec)	40		
DELAYBP	Delay Between Packets (mil sec)	40		
RESENDS	Number of Resends	1		
STORE	Backup Packets to Store for Resend	20		
CGMTDATE	Collection Start Date (YYYYMMDD)	20051104		
CGMTTIME	Collection Start Time GMT(HH:MM:SS)	14:00:00		
CWINDOW	Duration of Collection Window (min)	45		
MDELAY	Delay Before Multicast Start (min)	2		
MWINDOW	Duration of Multicast Window (min)	60		
TTL	Number of Router Hops	3		
BYPASCON	User to Prime Multicast Server			
ALTADDRM	Multicast Server IP	208.119.233.106		
ALTPORTM	Multicast Server Port	3463		
MINREF	Minimum Num Clients Requesting File	1		
MINSIZE	Minimum File Size for Multicast	1024		
ALWAYS_	Manager REXX Method	SYSTEM.ZMETHOD.MULTICAST		

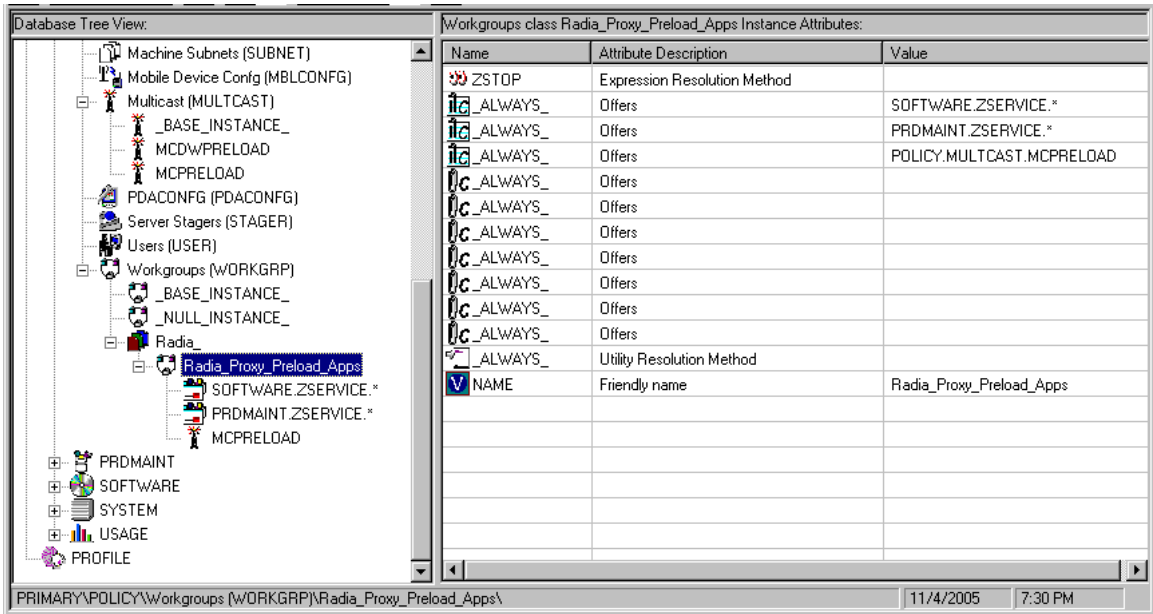
As specified in the previous figure, the collection phase (CWINDOW) will last 45 minutes, at which time the CM Multicast Server stops the collection process.

There will be a 2-minute delay (MDELAY) before the transmission begins. At the designated multicast start-time (CGMTTIME + CWINDOW + MDELAY = 14:47:00 GMT), the CM Multicast Server (specified by ALTADDRM) starts multicasting the files that are on the list is compiled from the various eligible CM agents.



Refer to the chapter *Configuring a CM Multicast Server Environment* in the *CM Multicast Server Guide* for additional information.

- 6 Connect the Workgroup Policy instance for the CM Proxy Preload Application to the POLICY.MULTICAST.MCPRELOAD instance as shown in the following figure. For details on making this connection, refer to the topics in the *CM Multicast Server Guide*.



- Issue the Proxy Preload command when the CGMTTIME and CGMTDATE apply.



For information on viewing the results of the multicast session, see [Session Logs for a Preload Using Multicast](#) on page 80.

Preloading using Multicast with Dynamic Windows

The Multicast Server offers the ability to configure dynamic (collection and transmission) windows. This means for a group of CM Proxy Servers being preloaded, multiple multicast distributions can be active concurrently.

This topic gives three sample configurations for using the multicast dynamic windows feature to preload CM Proxy Servers. Only three MULTICAST instance attributes are used to implement dynamic windows: ADDRESS, CGMTDATE, and CGMTTIME.



Before using this feature, please review the Multicast Dynamic Windows topic in the *CM Multicast Server Guide*.

Preload using Multicast with Dynamic Windows Example

The following MULTICAST instance values can be used to initiate a multicast session (using up to 22 dynamic windows) that will start at 05:01:00 GMT

each day. The empty value of CGMTDATE is used to specify a multicast session that will be run once a day.



A CM Proxy Server preload must also be scheduled for this same time each day for it to participate in the multicast session.

```
ADDRESS    = 235.0.0.000-021
CGMTDATE   = empty
CGMTTIME   = 05:01:00
```

```
CWINDOW    = 45
MDELAY     = 2
ALTADDRM   = <multicast_server_IP>
```

During this daily multicast session, the multicast server can issue IP addresses from 235.0.0.000 through 235.0.0.021. The addresses in this range will be used sequentially to accommodate overlapping windows for a group. When a given multicast session completes its transmission, the IP address is removed from the in-use list and is available once again.

The CWINDOW value of 45 specifies a collection window of 45 minutes.

Session Logs for a Preload Using Multicast

On a CM Proxy Server receiving a Preload from a Multicast Server, the preload session logs are found in the directory:

```
<IntegrationServer>\logs\rps
```

The following logs trace the activity of the collection, requests, and received items in a multicast session:

```
connect.log
radreqst.log
radcrecv.log
```



The `connect.log` for a CM Proxy Server Preload includes the collection information found in the `radclect.log` of a CM agent multicast session.

For details on the contents of these multicast session logs, refer to the Troubleshooting topic in the *CM Multicast Server Guide*.

Preloading Windows Installer Enabled Applications

There are two packages associated with each Windows Installer enabled application, the MSI package that includes the list of MSI Features, and the Administrator Control Point (ACP) package.

- ▶ An Administrative Control Point (ACP) is also known as a Windows Installer Administrative Installation Point (AIP).

The ACP package instance contains all of the file resources that are required by a Windows Installer product. If you are using CM Proxy Servers or Staging Servers, the ACP package needs to be deployed to these servers but not installed on the CM agent computers. Only the MSI package needs to be installed on the CM agent computers. There are two models for doing this.

Model 1: Create one Application (ZSERVICE) that includes a ZSTOP expression on the ACP Package

Create one Application (ZSERVICE) instance for both the MSI and ACP packages. Include a ZSTOP expression on the ACP package to prevent the CM agent computers from downloading it. Staging Servers and CM Proxy Servers ignore expressions, and will download the ACP package.

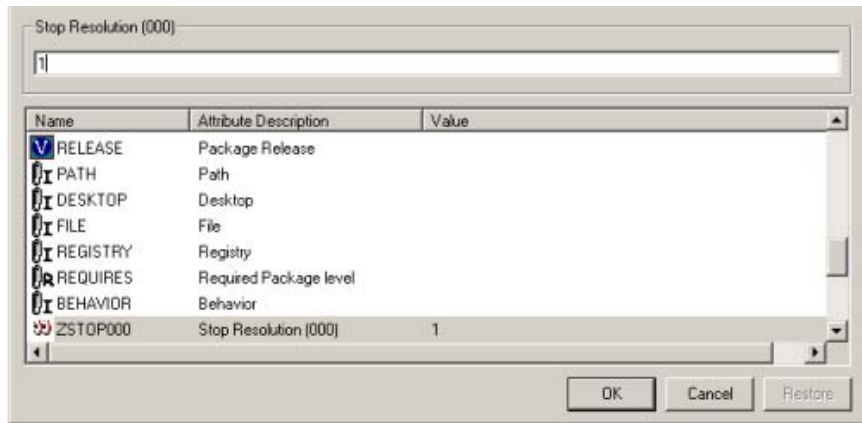
- ▶ This model is considered the best practice and is applied automatically when you publish Windows Installer Applications using the Advanced publishing mode of the CM Administrator Publisher (Publisher) and apply the default Admin Install Point (AIP) options. For more information on publishing Windows Installer Enabled applications, refer to the *CM Administrator User Guide*.

Use the procedure below if you need to apply the ZSTOP expression to an ACP package manually.

To enable an ACP package for preloading only

- 1 Use the CM Admin CSDB Editor to navigate to the ACP package that you want to preload.
- 2 Right-click on the ACP package and choose **Edit Instance** from the shortcut menu.
- 3 Click **ZSTOP000 Stop Resolution (000)** and type a value of 1.

Typing a value of 1 will prevent CM agent computers from resolving the ACP package, but will allow the CM Proxy Server or CM Staging Server to preload the ACP package.



- 4 Click **OK**.
- 5 Click **Yes** to confirm the change.
- 6 Connect the ACP package and the MSI package to the same service.

Model 2: Create separate Applications (ZSERVICES) for MSI Packages and ACP Packages

An alternative model is to create separate Application (ZSERVICE) instances for the MSI Package and the ACP Package. Deploy the MSI Package to the CM agent computers and the ACP Package to the CM Staging Server and CM Proxy Servers.



HP does *not* recommend naming ACP packages with a common suffix for the purpose of connecting *all* of the ACP packages to a single service and deploying this service to your CM Staging Servers and CM Proxy Servers. This method presents unnecessary overload on your infrastructure.

Configuring CM agents for Use with the CM Proxy Server

The CM Proxy Server functions as an extension of the CM Configuration Server. When used, the CM Proxy Server becomes the primary repository for CM agent data. Once a CM agent determines which resources it needs to achieve its 'desired state', it can request the resources from the CM Proxy Server.

After installing a CM Proxy Server, configure the desired set of CM agents to request their needed resources from the CM Proxy Server instead of the CM Configuration Server. This is done in the POLICY Domain of the CM Configuration Server's database.

Using HTTP for CM agent Communication

When the CM Proxy Server front-end protocol is HTTP, use these steps to configure your CM agents in the CM-CSDB. The HTTP front-end is enabled by default in the `rps.cfg` file (that is: `-httpd` is set to 1).



Although CM agent requests can be made using HTTP or TCP/IP, HTTP is the recommended protocol for communication with the CM Proxy Server. To use TCP/IP, see [Using TCP/IP for CM agent Communication](#) on page 85.

To configure CM agents for a CM Proxy Server using HTTP

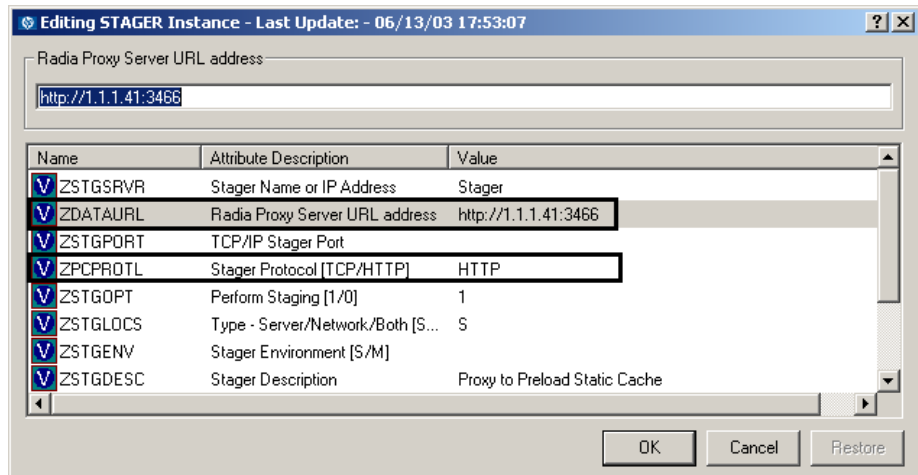
- 1 Use the CM Admin CSDB Editor to create and edit a POLICY.STAGER instance to define the CM Proxy Server as the deployment source for subscribers.
- 2 Update the following STAGER Class attributes to specify the CM Proxy Server information, as follows.
 - ZPCPROTL — Set the value of ZPCPROTL to indicate HTTP is the protocol the CM agents are to use for communicating with the CM Proxy Server.
 - ZDATAURL — When using HTTP, set the ZDATAURL field to store the URL and port for the CM Proxy Server. Storing the CM Proxy Server URL in the CM-CSDB allows the CM Proxy Server IP address or Hostname to be centrally controlled. Anytime this IP address or Hostname changes, the ZDATAURL field must be updated.

Thus, the recommended settings for enabling CM agents to request data from a CM Proxy Server using HTTP are:

ZPCPROTL = HTTP

ZDATAURL = http://<Your RPS IP Address or Hostname>:3466

Replace *Your RPS IP Address or Hostname* with the IP address or Hostname of your CM Proxy Server.



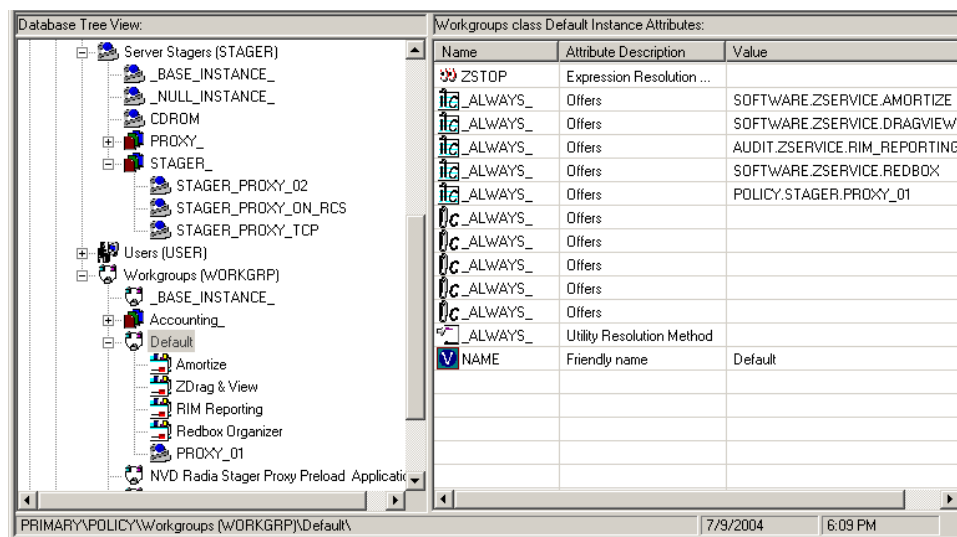
- 3 Connect the configured STAGER instance to the POLICY instances that represent the set of CM agents that will use this CM Proxy Server. This is usually one or more workgroups or departments.

To connect a STAGER instance to a Workgroups instance

In the following example, we connect the Default Workgroup to a pre-configured STAGER instance so that *all* subscribers will receive applications from the CM Proxy Server.

- 1 Open the CM Admin CSDB Editor, and navigate to the PRIMARY.POLICY.STAGER class.
- 2 Double-click the **Server Stagers (STAGER)** to see the STAGER instances.
- 3 Double-click the **Workgroups (WORKGRP)** to see the WORKGRP instances.
- 4 Connect the predefined STAGER instance to the appropriate WORKGRP instance (Default, in our example).

In this example, all CM agents that are members of the Default Workgroup will request their resources from the CM Proxy Server named in the STAGER instance Proxy_01 using HTTP communication.



Using TCP/IP for CM agent Communication



HTTP is the recommended protocol for CM agent communication with the CM Proxy Server. This topic discusses using the alternative TCP/IP protocol, when necessary.

Under certain circumstances, you may need to use the TCP/IP protocol to communicate with your CM agents.

To have the CM Proxy Server communicate with CM agents using TCP/IP, you must enable the `-stager` front-end in the CM Proxy Server Configuration file, `rps.cfg`. Set `-stager` to 1. By default, the `-stager-port` listening port is set to 3461. For details, refer to the `-stager*` parameters in [Table 4](#) on page 50.

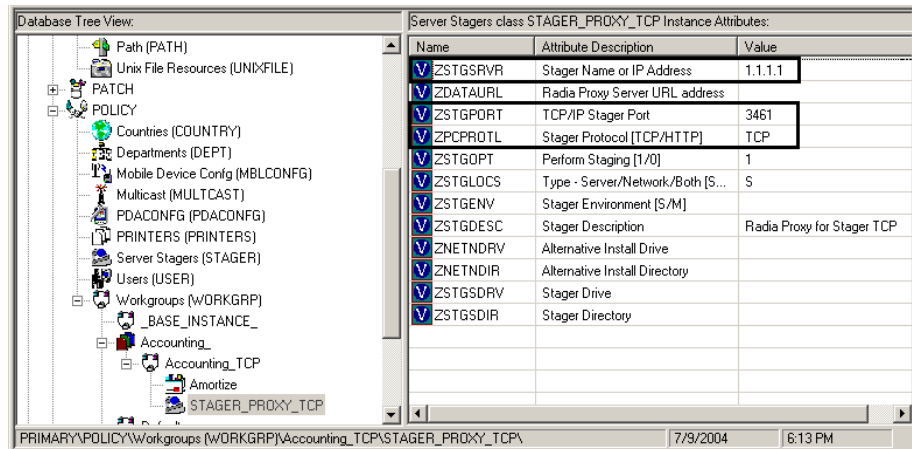
- To have the CM agents communicate with this CM Proxy Server using TCP/IP, create a `POLICY.STAGER` instance in the CM-CSDB that sets the following definitions for the STAGER Class attributes:

```
ZSTGSRVR = <CM Proxy Server IP Address or Hostname>
ZDATAURL = leave blank
ZSTGPORT = 3461 (the default CM Proxy Server TCP/IP Port)
ZPCPROTL = TCP
```

- If you are currently using TCP/IP to communicate between CM agents and Staging Servers, and would like to continue using TCP/IP with the CM Proxy Server, you need only change the IP address and port number of the Staging Server to the IP address and port number of the CM Proxy Server within Policy class. The policy instances will be unaffected.
 - Update the ZSTGSRVR attribute with the IP address of your CM Proxy Server.
 - Update the ZSTGPORT attribute with the port number of your CM Proxy Server for TCP, normally 3461.

Figure 6 below is a view of the CM Admin CSDB Editor screen showing the Stager instance attributes for CM Proxy Server serving CM agents using TCP.

Figure 6 STAGER instance attributes in CM Admin CSDB Editor



Additional Configuration Topics

Enabling the CM Configuration Server for HTTP Support

The CM Configuration Server no longer supports downloading resources from the CM-CSDB using the HTTP protocol. Previously, this was provided through the ZHTTPMGR method. To obtain database resources from the CM-CSDB using HTTP, use a CM Proxy Server co-located with the CM Configuration Server.

For details, see [Co-Locating a CM Proxy Server with a CM Configuration Server for HTTP Support](#) on page 63.

Summary

- You can install the CM Proxy Server locally or remotely.
- The CM Proxy Server component must be installed separately on each server to be used as a CM Proxy Server.
- The CM Integration Server is a foundation component of the CM Proxy Server. Start or stop the HP OVCM Integration Service (httpd) to start or stop the CM Proxy Server.
- Review the `rps.cfg` in the `/etc` folder of the CM Proxy Server install directory after an installation. Modify the parameters to set options, such as enabling and configuring the dynamic cache.
- The CM Configuration Server does not support the HTTP protocol. When you need to obtain resources from the CM-CSDB using HTTP, install a CM Proxy Server co-located with your CM Configuration Server. The co-located CM Proxy Server and port become the source for downloading resources from the CM-CSDB using HTTP.
- Create a preload distribution policy in the CM-CSDB for each CM Proxy Server in your infrastructure installed remotely from the CM Configuration Server.
- The CM agents must be configured to communicate with the CM Proxy Server. The default and recommended protocol is HTTP. TCP/IP is also supported.

3 CM Proxy Server Administration

At the end of this chapter, you will:

- Know how to start and stop the CM Proxy Server.
- Know how to preload the CM Proxy Server from the CM Portal.
- Know how to purge the dynamic cache from the CM Portal.
- Know how the CM Proxy Server can be used in conjunction with the CM Portal to deploy CM agent installs.
- Know which logs to use to troubleshoot a CM Proxy Server.

There may be special circumstances involved in your CM Proxy Server implementation. This chapter explores these possible situations:

- Starting and stopping the CM Proxy Server.
- Populating the CM Proxy Server before any CM agents try to install software.

Starting and Stopping the CM Proxy Server for Windows

Since the CM Proxy Server is a loaded module under the control of the CM Integration Server, in order to start and stop the CM Proxy Server, start and stop the CM Integration Server service on your computer. To do so, use the Service Control Manager window, as you would with any other Windows services. The CM Integration Server service is started automatically after the CM Proxy Server is installed on Windows platforms.

On UNIX platforms, the CM Integration Server service is not started automatically after installation; it must be started manually after the installation program is finished. See [Starting and Stopping the CM Proxy Server for UNIX](#) on page 41 for instructions.

For this example, we are using Windows 2000 Server.

To start the CM Proxy Server service

- 1 From your Windows Desktop, click **Start** → **Control Panel** → **Administrative Tools** → **Services**.

The Service Control Manager window opens.

- 2 Right-click on the service **HP OVCM Integration Server (httpd)** and select **Start** from the shortcut menu that opens.

The CM Proxy Server is now running on your computer.

To stop the CM Proxy Server service



You can also use the CM Portal to start and stop the CM Proxy Server. Refer to the *CM Portal Guide* for detailed information.

- 1 From your Windows desktop, click **Start** → **Programs** → **Control Panel** → **Administrative Tools** → **Services**.

- 2 The Service Control Manager window opens.
- 3 Right-click on the service **HP OVCM Integration Server (httpd)** and then select **Stop** from the shortcut menu that opens.

The CM Proxy Server has been stopped.

CM Portal and the CM Proxy Server

You can use the CM Portal to remotely install as well as manage your CM Proxy Servers. The CM Proxy Server-related tasks available through the CM Portal are summarized below. For complete information, also refer to the *CM Portal Installation and Configuration Guide (CM Portal Guide)*.

- **Install Proxy Server**

Permits remote installation of a CM Proxy Server using a default or a pre-configured `rps.cfg` file. For details, see [Installing the CM Proxy Server to a Remote Location](#) on page 42.

- **Synchronize Proxy Server (Preload)**

Preloads the selected CM Proxy Servers with services defined in the CM-CSDB. Permits an immediate or scheduled preload for one or all CM Proxy Servers in the CM Portal Zones. The status of a Synchronize Proxy Server job will report the following events:

- Submission of the job request to the CM Proxy Server.
- Start of session between the CM Proxy Server and CM Configuration Server (for preloading the files to the CM Proxy Server static cache).
- When the preload is complete.

For details, see [Preloading the CM Proxy Server](#) on page 92.

- **Purge Proxy Server Dynamic Cache**

Every time a file is requested, the request date is recorded and maintained. If a file has not been requested in a pre-defined maximum number of days, it is deleted from the Dynamic Cache. This purging of aged files can be initiated through the CM Portal.

For details, see [Purging the Dynamic Cache using the CM Portal](#) on page 93.

- **Assign Proxy Server**

When using the CM Portal to install many CM agents remotely, the Assign Proxy Server task gives you the option of using the CM Proxy

Servers to assist in the delivery of the install payload to the CM agents. This option offloads work from the CM Portal to the assigned CM Proxy Servers in your enterprise. For details, see [Using CM Proxy Servers to Install CM agents remotely from the CM Portal](#) on page 95.

Preloading the CM Proxy Server

After installation, through the CM Portal, you can choose to preload your CM Proxy Server with services defined in the CM-CSDB. These services will be copied to the static cache located on the CM Proxy Server.

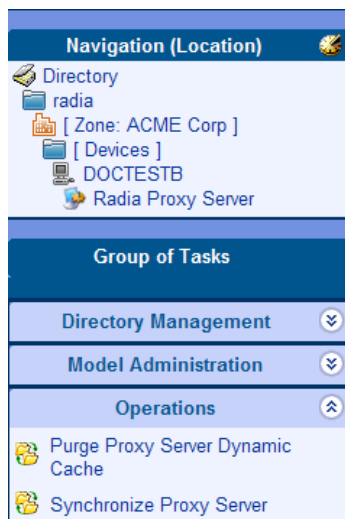
- ▶ For a discussion of how to prepare Windows Installer Enabled applications for preloading to a CM Proxy Server, see [Preloading Windows Installer Enabled Applications](#) on page 67.

Synchronizing (preloading) the CM Proxy Server using the CM Portal

From any web browser use the CM Portal's Synchronize Proxy Server task to force the CM Proxy Server to connect to the CM Configuration Server to preload the files to the static cache on the CM Proxy Server.

To synchronize the CM Proxy Server using the CM Portal

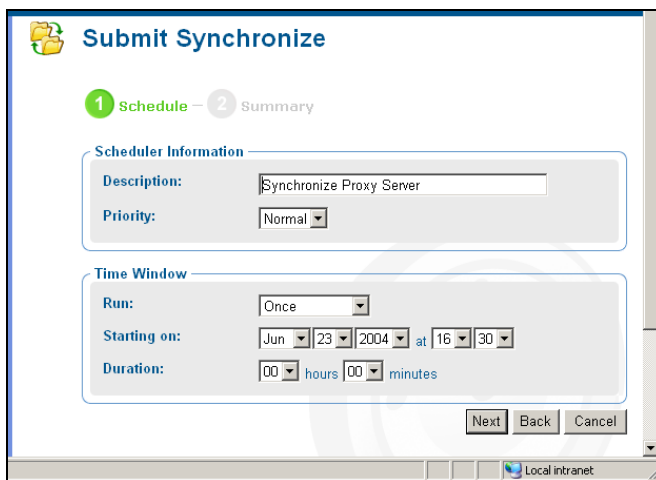
- 1 Access the CM Portal from any web browser.
- 2 Use the Navigation aid to select the CM Proxy Server on the Device that you want to synchronize.



- ▶ Alternatively, go to the **Proxy Server** group located in the **Zone** → **Cross References** → **Infrastructure Services** container to synchronize all CM proxy servers in a zone at once.

- 3 In the Operations task list, click **Synchronize Proxy Server**.

The Submit Synchronize – Schedule window opens.



The screenshot shows a web-based window titled "Submit Synchronize". At the top, there are two tabs: "Schedule" (active) and "Summary". Below the tabs, there are two main sections: "Scheduler Information" and "Time Window".

Scheduler Information:

- Description: Synchronize Proxy Server
- Priority: Normal

Time Window:

- Run: Once
- Starting on: Jun 23 2004 at 16:30
- Duration: 00 hours 00 minutes

At the bottom right of the form, there are three buttons: "Next", "Back", and "Cancel". The window title bar at the bottom indicates "Local intranet".

- 4 In the Schedule window, specify when you want this job to run.

- 5 Click **Next**.

The Submit Synchronize – Summary window opens.

- 6 Click **Submit**.

A list of the jobs appears.

The status of the synchronize proxy job will report the following events:

- Submission of the job request to the CM Proxy Server.
- Start of session between CM Proxy Server and CM Configuration Server (for preloading the files to the static cache on the CM Proxy Server).
- Job completed.

Purging the Dynamic Cache using the CM Portal

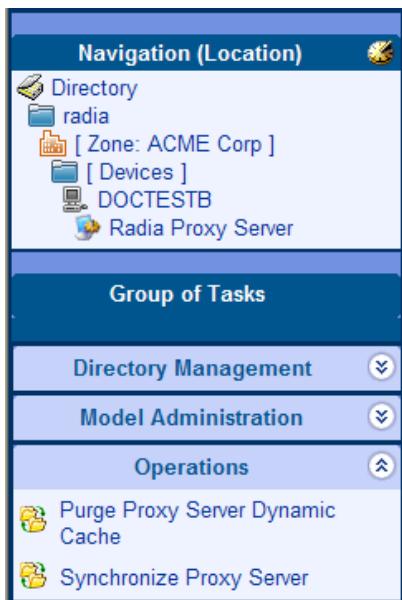
Use the Purge Proxy Server Dynamic Cache task of the CM Portal to purge the dynamic cache of the CM Proxy Server of aged files.

Refer to the *CM Portal Guide* for more information.

- ▶ The same purge process occurs whenever the dynamic cache index file is saved. To set the dynamic cache parameters that schedule a save of the index file, see [The Date-Based Purge of the Dynamic Cache](#) on page 59.

To purge the dynamic cache of the CM Proxy Server

- 1 Access the CM Portal and navigate to the CM Proxy Server on the device whose cache you want to purge.
 - ▶ To schedule a dynamic cache purge of all CM Proxy Servers in your network at once, go to the **Proxy Server** group located in the **Zone** → **Cross References** → **Infrastructure Services** container to begin the task.



- 2 In the Operations task group, click **Purge Proxy Server Dynamic Cache**. The Schedule window opens.
- 3 In the Schedule window, specify when you want this job to run. For more information, see Scheduling Jobs in the *CM Portal Guide*.
- 4 Click **Next**. The Submit Purge—Summary window opens.

5 Click **Submit**.

A list of the jobs appears. Now, you can use the View Properties task of the CM Portal to view detailed information, such as the status of the job.

Using CM Proxy Servers to Install CM agents remotely from the CM Portal

Just as CM Proxy Servers are used to efficiently offload the distribution of applications to CM agents, the CM Portal supports the use of CM Proxy Servers to efficiently offload the task of remotely installing CM agents.

This feature requires the following CM components:

- CM Portal 5.00 or greater; CM Portal 5.10 to support tasks involving CM agents on UNIX platforms.
- CM Proxy Server 5.00 or greater, with an installed CM Portal Agent (also known as an RMA).

From the CM Portal, Administrators may use the Assign Proxy Server task to assign a group of managed devices (that is, computers which have a CM Portal Agent installed on them) to a CM Proxy Server. This assigned CM Proxy Server becomes the code source for a later CM Portal request to install a CM agent on the managed device. Thus, the workload of downloading scripts to install CM agents remotely can be distributed between the Portal and a number of CM Proxy Servers.

All tasks are performed from the CM Portal. For details, see the topics *Assigning Proxy Servers* and *Installing CM agent* in the *CM Portal Guide*. An overview of the process involves five steps:

- 1 Create a group of all devices to be assigned to a given CM Proxy Server (*Recommended*).
- 2 Use the Assign Proxy Server task to assign the group of devices to the Proxy Server.

At this time, the CM Portal delivers the CM agent install payload to the CM Proxy Server.

- 3 Use the Install CM Agent task to schedule a job to have the CM agent remotely installed on the group of devices.

The CM Portal schedules a CM agent install job for each device in the group.

- 4 When each CM agent install job executes, the device contacts the assigned CM Proxy Server.
- 5 The CM Proxy Server synchronizes its CM agent payload with the CM Portal using delta processing, and then deploys it to the device.

The initial delivery and delta synchronization of the CM agent install payload from the CM Portal to the CM Proxy Server rely upon the underlying HP OVCN Integration Server components of both the CM Portal and CM Proxy Servers.

Summary

- You can start and stop the CM Proxy Server locally or remotely via the CM Portal.
- You can purge the CM Proxy Server's dynamic cache from the CM Portal.
- You can preload the CM Proxy Server's static cache using the CM Portal.
- From the CM Portal, you can designate the CM Proxy Server to deliver CM agent installs for an assigned set of computers. This feature uses the underlying HP OVCM Portal server component to synchronize the CM agent payload with the CM Portal and then deliver it to machines requesting the CM agent installs.

4 Troubleshooting

At the end of this chapter, you will:

- Be familiar with the CM Proxy Server log files.
- Be familiar with troubleshooting the most common error messages.
- Know how to collect the required files and version information when working with HP Technical Support.
- Know how to preload the CM Proxy Server manually, from any web browser.

CM Proxy Server Installation Directory

By default, the CM Proxy Server is installed into the following directories:

Windows: `SystemDrive:\Program Files\Hewlett-Packard\CM\IntegrationServer`

UNIX: `/opt/HP/CM/IntegrationServer`

About the Log Files

The CM Proxy Server writes several logs, which can be used to track progress and diagnose problems. The log files are stored in the logs subdirectory of the CM Proxy Server installation directory.

The log files are:

- `httpd-port.log`
Replace *port* with your port number, for example, `httpd-3466.log`. Logs the CM Proxy Server activities of the TCL web server that it runs on. Can be found in the logs subdirectory of the CM Proxy Server installation directory.
- `httpd-port.YY.MM.DD.log`
This log contains the web server activity for each day. If the log is empty, it means that there was no activity that day.
- `httpd-3466.error.txt`
This log contains messages written to any logs that contain the prefix **ERROR**. This allows you to view all errors in a single location.
- `CONNECT.LOG`
Log created in the `\logs\rps` subdirectory of the CM Proxy Server installation directory when the CM Proxy Server connects to the CM Configuration Server to preload the static cache. Displays information related to the preload and the modules involved, such as `RADCONCT`.

Each time you start the web server a new log is written. The old log is saved as `httpd-port.nn.log`.

Changing the Logging Level

By default the trace level is set to 3, which is the informational tracing level. This displays INFO, WARNING, and ERROR messages.

To change the log level, you can either run the following at a command prompt from the CM Proxy Server installation directory:

```
nvdkit httpd.tkd -log_level 4
```

or

modify the log level in the `httpd.rc` configuration file found in the `\etc` folder of the CM Proxy Server install directory. Use the following procedures.

To change the log level in the `httpd.rc` file

- 1 Stop the foundation service for the CM Proxy Server; this is HP OVCM Integration Server (`httpd`).
- 2 Open the `httpd.rc` file, which is located in the `\etc` directory of where the CM Proxy Server was installed. For Windows, the default location of the file is:

`SystemDrive:\Program Files\Hewlett-Packard\CM\IntegrationServer\etc\httpd.rc`. The following is an excerpt from the `httpd.rc` file.

```
# Config Array
# Element           Default
# =====
# HOST               [info hostname]
# PORT               3466
# HTTPS_HOST        [info hostname]
# HTTPS_PORT        443
# DEBUG             0
# DOCROOT            [file join $home htdocs]
# IPADDR             0.0.0.0
# HTTPS_IPADDR      0.0.0.0
# WEBMASTER          support.mail@hp.com
# UID                50
# GID                100
# NAME               $tcl_service
# LOG_LEVEL          3
# LOG_LIMIT          7
# AUX_LOG_LINES     5000
#
Overrides Config {
    PORT          3466
    LOG_LEVEL     4
```

```

}
#
# (Re)Initialize Logging
#
Log_Init

```

- 3 Locate the `Overrides Config` entry below the `Config Array` list of elements and default values.
- 4 Within the `Overrides Config` starting and ending brackets { }, type **LOG_LEVEL** and the appropriate trace level, space delimited, Select the appropriate trace level from [Table 9](#) below.

Table 9 Trace Levels

Trace Level	Description
0	No logging.
1	Logs errors only.
2	Logs warnings and errors.
3	Logs informational messages, warnings, and errors. <i>Recommended trace level setting for customers.</i>
4	Logs all debug information. <i>Recommended for experienced customers only.</i>
5-9	Full trace <i>Not recommended for customer use.</i>

- 5 Save the file changes.
- 6 Restart the CM Integration Server service.

Common Problems and Solutions

Performance Problems

Anti-virus software can reset `IRPStackSize` to a non-recommended, low value, causing performance issues for CM Integration Server -based products. If you are experiencing performance problems in a Windows environment, check that the `IRPStackSize` in the Windows Registry is set to an adequate value for your operating system. If `IRPStackSize` is set too low, it may severely impair your CM Integration Server's network performance, especially under heavy load situations. On the CM Proxy Server, for example,

if IRPStackSize is set below the normal range for the operating system, application deployment will be slowed considerably.

To check for an adequate IRPStackSize value

Use your operating system's registry editor to check if the value of IRPStackSize is set too low. If it is, back up the Windows Registry and then increase the IRPStackSize value to be within the recommended range.

The IRPStackSize setting can be found in the following registry location:

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters]
```



For Windows 2000 Server and Server 2003, the IRPStackSize value is not created during installation. If there is no value for it at the above location, the default value is used—which is no problem. If IRPStackSize is found at the above registry location, verify that it falls within the recommended values.

To obtain the recommended values for IRPStackSize as well as detailed instructions of how to change the IRPStackSize value, see the following Symantec and Microsoft documents:

- [How to Change the IRPStackSize for Computers registry value](#)
- [IRPStackSize Parameter in Windows 2000 and Windows 2003](#)
- [Antivirus Software May Cause Event ID 2011](#)

These links were active as of this writing.

Errors and Solutions

These topics address some of the errors you may find when analyzing a CM Proxy Server log.

- If you receive the following error, you are not properly licensed for the CM Proxy Server (or the license expired) and will need to obtain the correct license file through Tech Support in order to run this product.

```
ERROR: "C:/Program~/Hewlett-Packard/CM/CM Integration  
Server/modules/rps.tkd", Not licensed for this product
```

- If you receive the following error in the `CONNECT.LOG` during preload, you must check the CM Configuration Server log. The '650' error means something went wrong on the server side and the application was not delivered correctly.

```
[17:10:21 [RADCONCT / 000005a4] SYSTEM --- RADCONCT exit
status [650]

[17:10:21 [RADCONCT / 000005a4] SYSTEM --- RADCONCT [Server
stopped application configuration.]

NVD000010A [radconnect_term] 17:10:21 [RADCONCT / 000005a4]
SYSTEM --- RADCONCT Return Code [650]

NVD000005E [radconct_cleanu] 17:10:21 [RADCONCT / 000005a4]
SYSTEM --! RADCONCT Exit code [650]
```

- If you receive the following error in the `CONNECT.LOG` during preload, you have not assigned any services/applications to the default RPS user instance. (Services will be preloaded whether they are Mandatory or Optional. Stop Expressions are also ignored.)

```
13:43:36 Warning: RPS/Static: sync: Radskman rc:[109]
[Presently there are no applications available in the software
catalog. Please contact your system administrator for
assistance.] (CHILDSTATUS -1 109)
```

If additional logging is need, you may be asked to increase the log level. You can change the log level at the command prompt by running `nvdkit httpd.tkd -log_level 4`, or by adding the log level to the `httpd.rc` configuration file found in the `/etc` folder.

Testing the CM Proxy Server Preload

Use the following command to manually perform a CM Proxy Server preload distribution. This is often used in a test environment, but can also be used in a production environment, if desired.

To manually perform the Preload from a web browser

You can manually perform a CM Proxy Server's preload by typing the following command into a web browser:

```
http://proxy_machine_name:3466/proc/rps/sync
```

You will not get any feedback from the process—just a blank screen.

Check the CM Proxy Server machine for activity and check the following CM Proxy Server directory for data files.

```
Integration_Server\DATA\RPS\STATIC\000D\
```

where: *Integration_Server* represents the base installation directory where the CM Proxy Server is installed. By default, this is: `C:\Program`

Files\Hewlett-Packard\CM\IntegrationServer for Windows, and
/opt/HP/CM/IntegrationServer for UNIX.

Troubleshooting Questions

To expedite a solution, you should be prepared to answer the following questions before you contact technical support. This will expedite the solution.

- What has changed in your environment?
- What are the build numbers of your RPS.TKD, NVDKIT, and HTTPD.TKD modules? See [Collecting Information for HP Technical Support](#) below.
- What error messages were received?
- What actions was the CM Proxy Server performing when the problem occurred? For example, was the RPS serving files or preloading data?
- If you use HTTP, can you download existing data from the CM Proxy Server.

To test this, open an Internet Explorer browser session and type:

```
http://host:port/RESOURCE/SOFTWARE/FILE/<an existing resourceID in static or dynamic cache>
```

Collecting Information for HP Technical Support

If you need to contact HP Technical Support for assistance, be sure to collect the following information:

- 1 Version information for `nvdkit`, `httpd.tkd` and `rps.tkd`. For details, see, [How to Obtain Version Information](#) on page 106 .
- 2 The logs directory including all subdirectories, stored by default in the following locations:

Windows: `Drive:\Program Files\Hewlett-Packard\CM\IntegrationServer\logs`
UNIX: `/opt/HP/CM/IntegrationServer/logs`
- 3 The `etc` directory files (no subdirectories), stored by default in the following locations:

Windows: *Drive:\Program Files\Hewlett-Packard\CM\IntegrationServer\etc*

UNIX: */opt/HP/CM/IntegrationServer/etc*

- 4 For preload problems, also collect the CM Proxy Server lib directory and contents (except any 000D compressed data subdirectory), stored by default in the following locations:

Windows: *Drive:\Program Files\Hewlett-Packard\CM\IntegrationServer\etc\rps*

UNIX: */opt/HP/CM/IntegrationServer/etc/rps*

How to Obtain Version Information

To gather the version information for RPS.TKD, NVDKIT, and HTTPD.TKD

- 1 From a command prompt, navigate to where the CM Proxy Server was installed; this is the location for *nvdkit.exe*.
Your license file (*license.nvd*) needs to be copied to this folder.
- 2 Type the NVDKIT commands for each of the components, as given in the following table.

Table 10 CM Proxy Server - Version and Build

Component	Location	Command to Obtain Version Number
RPS.TKD	<i><RPS-Install>/modules</i>	NVDKIT VERSION MODULES RPS.TKD
NVDKIT	<i><RPS-Install></i>	NVDKIT VERSION
HTTPD.TKD	<i><RPS-Install></i>	NVDKIT VERSION HTTPD.TKD

The following figure shows an example of obtaining the version information.

```

(C) Copyright 1985-2000 Microsoft Corp.

C:\>cd Novadigm\Inte*

C:\Novadigm\IntegrationServer>nvdkit version modules rps.tkd
Kit Version: 2.1
Tcl Version: 8.2.2+

C:/Novadigm/IntegrationServer/modules:

C:/Novadigm/IntegrationServer/modules/rps.tkd:
    module rps, build 20 20021112 19:56:05 UST

C:\Novadigm\IntegrationServer>nvdkit version
Kit Version: 2.1
Tcl Version: 8.2.2+

C:/Novadigm/IntegrationServer/nvdkit.exe:
    module nvdkit, build 131 20021223 19:52:46 UST
    module tclkitsh, build 48 20021205 23:57:46 UST
    module lib/nvd.sql, build 17 20020412 19:04:14 UST
    module lib/nvdtcl, build 54 20021223 18:15:34 UST
    module lib/vfs, build 13 20020503 17:54:14 UST

C:\Novadigm\IntegrationServer>nvdkit version httpd.tkd
Kit Version: 2.1
Tcl Version: 8.2.2+

C:/Novadigm/IntegrationServer/httpd.tkd:
    module httpd, build 60 20021217 20:05:17 UST

C:\Novadigm\IntegrationServer>

```

- 3 Collect this output for HP Technical Support.

Reporting a Problem for a CM Proxy Server

Once you have exhausted the options laid out in this topic and reviewed your logs for typical errors, go to the HP Support web site to report or resolve the problem.

Whenever you contact HP Technical Support for assistance regarding a CM Proxy Server, be prepared to collect the items discussed in the topic [Collecting Information for HP Technical Support](#) on page 105. At a minimum, collect your `HTTPD:3466.log` plus an output showing the versions of your RPS, NVDKIT, and HTTPD.TKD modules available.

Summary

- Review the `HTTP-port.log` files and the `CONNECT.LOG` files to troubleshoot CM Proxy Server errors.
- Review the common error messages and solutions given in this topic.
- Collect the version information, required log files, and other relevant directories and files before contacting HP Technical Support or submitting a support case.
- You can enter a command from any web browser to manually preload a CM Proxy Server.

5 The CM Enterprise Proxy Server (using Apache) on Windows

At the end of this chapter, you will:

- Be familiar with the system requirements for the CM Enterprise Proxy Server using Apache (CM Proxy Server using Apache) Windows.
- Know how to install the CM Proxy Server using Apache.
- Know how to remove the CM Proxy Server using Apache.

Platform Support

The CM Proxy Server using Apache is supported on Windows platforms only.

For information about the Windows platforms that are supported in this release, see the accompanying release notes.

System Requirements

Secured Network Requirement

The CM Proxy Server using Apache must be installed in a secured network environment, such as behind a firewall. This version does not support SSL communications.

- ▶ If the CM Proxy Server using Apache is installed behind a firewall, and you will be accessing it from outside the firewall, make sure that the firewall allows incoming network connections on port 8080. If not, you will not be able to access the CM Proxy Server using Apache from outside of the firewall.

CM Infrastructure Requirements

Before installing the CM Proxy Server using Apache, you will need to have the following installed in your enterprise. If the following are already installed, you will need to identify which ones will be used by the CM Proxy Server using Apache.

Co-located Proxy Server using Apache Requirements

- CM Configuration Server (Windows only)

Caching Proxy Server using Apache Requirements

- CM Configuration Server *for catalog resolution*
- Upstream server *for CM managed-services data source*

An upstream server can be any of the following:

- Co-located CM Proxy Server on AIX, HP-UX, Linux, Solaris, or Windows
- Co-located CM Proxy Server using Apache on Windows
- CM Proxy Server (in a multi-tier environment) running on AIX, HP-UX, Linux, Solaris, or Windows
- CM Proxy Server using Apache (in a multi-tiered environment) running on Windows

Installation Tasks

You will need to complete the following tasks to use all the features of the CM Proxy Server using Apache. Be sure to have the IP address, hostname, and port for your CM Configuration Server or other upstream CM Proxy Server available.

Server Installation when Co-located with the Configuration Server

Be sure to have the IP address, hostname, and port for your CM Configuration Server or other upstream CM Proxy Server available.

To install a CM Proxy using Apache co-located with a Configuration Server

- 1 Prepare the Configuration Server Environment by disabling any existing CM Proxy Server (rps) module loaded in a CM Integration Server.
 - a Prior to installing a 5.10 Proxy Server using Apache co-located with a Configuration Server, check to see if the HP OVCM Integration Server service (httpd) was previously installed on the machine. If so, comment out this line in the `\IntegrationServer\etc\httpd.rc` file:

```
Load Proxy Server
#module load rps
```
 - b Restart the HP OVCM Integration Server service if it will continue to host other modules, such as the Policy Server or Usage Manager.
- 2 From the installation media, navigate to the `\Infrastructure\extended_infrastructure\proxy_server\apache\win32` directory.
- 3 Double-click the installation executable: `rps.msi`.
- 4 Follow the prompts and provide the appropriate answers using the guidelines below:
 - The default installation directory is:

```
<drive:>\Program Files\Hewlett-Packard\CM\ProxyServer
```

If your Configuration Server is located at a different root directory, browse to the root directory of your Configuration Server and append the folder name `\ProxyServer`.
 - Choose the Proxy Type of **Co-located with Configuration Server**.
 - Choose a Server Port that is not currently in use.
- 5 After installation, Windows Services will display the following friendly service name and description on the local computer:
HP OVCM Proxy Server Apache/2.2.4 (Win32)
The installed service is `httpd-rps`.

Server Installation for Data Caching

Be sure to have the IP address, hostname, and port for your CM Configuration Server and upstream server available. See [Caching Proxy](#)

[Server using Apache Requirements](#) on page 110 for the list of supported upstream servers.



Modifying the upstream server after installation is not supported on the Enterprise Proxy Server using Apache. For more information, refer to [About the Configuration File: httpd.conf](#) on page 113.

To install a caching CM Proxy Server using Apache

- 1 From the installation media, navigate to the `\Infrastructure\extended_infrastructure\proxy_server\apache\win32` directory.
- 2 Double-click the installation executable `rps.msi`.
- 3 The installation process will check for adequate disk space and other requirements.
- 4 Follow the prompts and provide the appropriate answers.
 - The default installation directory is:
`<drive:>\Program Files\Hewlett-Packard\CM\ProxyServer`
 - Choose the Proxy Type of **Caching Proxy Server**
 - Choose a Server Port that is not currently in use. The default is 3466.
- 5 After installation, the following two Windows Services will be installed and running on the local computer:
 - Service: `httpd-rps` (HP OVCM Proxy Server)
This is the Apache 2.2 http-server for the CM Proxy Server.
 - Service: `httpd-rps-cache` (HP OVCM Proxy Server Cache Purge)
This is the service that purges the cache every 30 minutes to keep it under the maximum size, as specified during the installation.

Stopping and Starting the CM Proxy Server using Apache

To stop the CM Proxy Server using Apache service

To stop the service, use Windows Services and stop the service for HP OVCM Proxy Server. Alternatively, type the following from a command prompt:

```
net stop httpd-rps
```


To start the CM Proxy Server using Apache service

To start the service, use Windows Services and start the service for HP OVCN Proxy Server. Alternatively, type the following from a command prompt:

```
net start httpd-rps
```

About the Configuration File: httpd.conf

After running the MSI program, a configuration file, `httpd.conf`, is located in the `conf` directory of where the CM Proxy Server was installed. By default, this location is:

```
<drive:>\Program Files\Hewlett-Packard\CM\ProxyServer\conf
```

The `httpd.conf` file can be used to reset the log level. Refer to [Resetting the Log Level](#) below.

Do not adjust the other directives configured through the MSI program, unless directed to do so by HP customer support.



Customers familiar with the Integration Server-based CM Proxy Server may be accustomed to modifying the configuration file, `rps.cfg`, after installation. However, HP does not support adjusting entries in the `httpd.conf` file after the CM Proxy Server using Apache is installed using `rps.msi`. The only exception to this rule is [Resetting the Log Level](#), as discussed below.

For more information on the directives placed in the `httpd.conf` file, refer to the following Apache Directive Index web-page:

<http://httpd.apache.org/docs/2.2/mod/directives.html>

Resetting the Log Level

If HP support directs you to change the Log Level for troubleshooting, use the steps below to modify the `LogLevel` value in `httpd.conf` configuration file and restart the HP OVCN Patch Manager Service:

- 1 Refer to the following web-page for latest available LogLevel values:
<http://httpd.apache.org/docs/2.2/mod/core.html#loglevel>
- 2 Backup the existing `httpd.conf` file, located in the `\conf` folder of where you installed the CM Proxy Server using Apache.
- 3 Open the `httpd.conf` file using a text editor.

- 4 Locate the `LogLevel` directive, and modify the value. For example, from:

```
#  
LogLevel warn
```

to

```
#  
LogLevel debug
```

- 5 Save your changes and restart the `httpd-rps` service (HP OVCM Proxy Server).

Following installation, refer to the following topics:

- [Data Cache Management](#) on page 115.
- [Preloading \(or Synchronizing\) the Data Cache](#) on page 115.
- [Automatic Purge of Cache above Max Size](#) on page 115.
- [Comparison Chart of CM Proxy Server and CM Enterprise Proxy Server](#) on page 116.

Removing the CM Proxy Server using Apache

Use the task below to remove the CM Proxy Server using Apache service.

To remove the CM Proxy Server

- 1 Double-click the `rps.msi` installation executable, located on the CM 5.1 media at the directory:
`\Infrastructure\extended_infrastructure\proxy_server\apache\win32.`
- 2 When the Proxy Server is already installed on the current computer, the Application Maintenance dialog opens. Click **Remove** to uninstall the Proxy Server.
- 3 Follow the prompts to finish uninstalling the CM Proxy Server using Apache from the computer.

Data Cache Management

The CM Proxy Server using Apache manages a single cache that is located in the `\cache` folder of where the CM Proxy Server was installed. By default, this is:

```
C:\Program Files\Hewlett-Packard\CM\ProxyServer\cache
```

The `\cache` directory is organized differently than the entries in a `\dynamic` or `\static` cache of previous Integration Server-based Proxy Servers; see [Table 11](#) on page 116 for more information.

Preloading (or Synchronizing) the Data Cache

To preload the CM Proxy Server using Apache:

- 1 Use the Identity entered during the installation of the CM Proxy Server using Apache to entitle it to services that are to be preloaded.
- 2 Open a web-page and issue the same command used to preload the CM Proxy Server:

```
http://proxy_host_or_IP_address:port/proc/rps/sync
```

For example, if you entered an Identity of `PROXY_ALL` during the installation, first entitle the `Primary.Policy.User.PROXY_ALL` instance to the appropriate services, then run the `/proc/rps/sync` command named above.

Automatic Purge of Cache above Max Size

The CM Proxy Server using Apache runs a service every 30 minutes to purge the data cache if it exceeds the **Max Size** entered during the `rps.msi` install.

Comparison Chart of CM Proxy Server and CM Enterprise Proxy Server

Table 11 below identifies similarities and differences between the CM Proxy Server and the CM Enterprise Proxy Server for this release.

Table 11 CM Proxy Server vs. CM Enterprise Proxy Server

CM Proxy Server	CM Enterprise Proxy Server
HTTP server: CM Integration Server	HTTP server: Apache server
Platform support: Windows Servers and UNIX	Currently Windows Servers only
Installation: <ul style="list-style-type: none"> • Setup.exe or CM Portal • Co-located setup requires post-install configuration 	Installation: <ul style="list-style-type: none"> • MSI Install (Portal may follow) • Supports co-located install (new)
Two cache locations: Static and Dynamic <ul style="list-style-type: none"> • Data structure reflects CM-CS database (FDCI) 	Single cache location named: "Cache" <ul style="list-style-type: none"> • Data structure independent of CM-CS database (not FDCI)
Downloads data both HTTP and TCP	Downloads HTTP only
Includes embedded CM-agent code	Includes embedded CM-agent code
Supports Preload, Dynamic Cache Purge and Migration	Supports Preload and Dynamic Cache Purge
Supports HTTPS	No current support for HTTPS

A Product Name Changes

If you have used Radia in the past, and are not yet familiar with the newly rebranded HP terms and product names, [Table 12](#) below will help you identify naming changes that have been applied to the Radia brand.

Table 12 Product Name and Term Changes

New Name/Term	Old Name/Term
CM agents	Radia clients
HP Configuration Administrator	Radia Administrator Workstation
HP Configuration Management	Radia
HP Configuration Management Admin CSDB Editor	Radia System Explorer
HP Configuration Management Application Manager	Radia Application Manager
HP Configuration Management Application Self-service Manager	Radia Software Manager
HP Configuration Management Configuration Server	Radia Configuration Server
HP Configuration Management Configuration Server Database	Configuration Server Database, Radia Database
HP Configuration Management Extensions for Windows Installer	Radia Extensions for Windows Installer
HP Configuration Management Integration Server	Radia Integration Server
HP Configuration Management Inventory Manager	Radia Inventory Manager
HP Configuration Management Multicast Server	Radia Multicast Server
HP Configuration Management Portal	Radia Management Portal
HP Configuration Management Reporting Server	Radia Reporting Server

Glossary

applications

Also called software, data, or services.

Applications are one type of content that CM can manage on subscriber computers. Use the CM Admin Publisher to create packages of data to be managed on your subscribers' computers.

attribute

Also called *field*, *variable*, or *property*.

An attribute is a single, descriptive data item in a class. The class template contains a definition (e.g., the name, data type, description, and length) for each attribute that makes up the class. Class instances contain a set of attributes and each attribute contains a value.

attribute property

An attribute property controls some aspect of how an attribute is processed on the CM Configuration Server and CM agent computer. Each attribute defined in a class template has a set of CM Configuration Server properties and a set of CM agent properties.

CM Admin Agent Explorer

The CM Admin Agent Explorer can be used to view or edit local objects, or create new objects. You can also use the CM Admin Agent Explorer to view objects located on a file server or on other computers to which you are connected via a local area network (LAN).

CM agent computer

A CM agent computer is a subscriber's computer that has the CM agent software installed on it.

CM Application Manager

The CM Application Manager (`radia_am.exe`) is the CM agent that manages mandatory services. The systems administrator uses the CM Admin CSDB Editor to specify the services that the CM Application Manager manages on the subscriber's computer. No user interface is available.

CM Application Self-service Manager

The CM Application Self-service Manager (`radia_sm.exe`) is the CM agent used to manage optional services. The systems administrator uses the CM Admin CSDB Editor to specify the services that are available to the subscriber.

The subscriber installs and manages services that are available from the CM Application Self-Service Manager user interface (Service List).

CM Configuration Server

Also called the *Manager*.

The CM Configuration Server distributes applications to CM agent computers. It maintains the CM-CSDB, which stores information that the CM Configuration Server needs to manage digital assets for distribution to CM agent computers.

CM Configuration Server DB

The CM-CSDB stores all of the information necessary to manage digital assets on a CM agent computer, including:

- The software and data that CM distributes.
- The "desired state" of each CM agent computer with respect to the managed content.
- The policies determining which subscribers can subscribe to which packages.
- Security and access rules for administrators.

Use the CM Admin CSDB Editor to manipulate the CM-CSDB.

CM Manager

See *CM Configuration Server*.

CM Portal

The CM Portal is a core CM product, used to manage many different CM assets.

CM Service

Also called a software application, application, or software.

A service is a group of related packages representing the set of digital assets managed by CM as a unit.

dynamic cache

The dynamic cache is the CM Proxy Server's secondary cache populated through Dynamic PassThru. When CM agents request data that is not available in the static cache, Dynamic PassThru sends a request to an upstream host, either a CM Proxy Server co-located with a CM Configuration Server, or another CM Proxy Server, to satisfy the request. Multiple upstream hosts may be defined for fail-over support: if the first named host fails to connect, Dynamic PassThru sends the request to the next upstream host on the list.

CM Admin CSDB Editor

The CM Admin CSDB Editor is used to manipulate the contents of the CM-CSDB.

Dynamic PassThru

The HTTP process used to populate the dynamic cache. When CM agents request data that is not available in the static cache or existing dynamic cache, Dynamic PassThru sends a request to an upstream host, either a CM Proxy Server co-located with a CM Configuration Server or another CM Proxy Server, to satisfy the request. Multiple upstream hosts may be defined for fail-over support: if the first named host fails to connect, Dynamic PassThru sends the request to the next upstream host on the list.

instance

Also called *class instance*.

An instance is a CM-CSDB object containing a specific occurrence of a class. This is analogous to a row in a relational data table or a record in a traditional flat file. The attributes of an instance contain the data describing one specific entity of that class.

method

A method is a program that performs functions that are meaningful in the context from which they are called.

Methods can be written in REXX or in a language that produces an executable that can validly run on the platform where it is invoked. The HP-supplied REXX run-time environment interprets REXX methods.

Agent methods, also known as Client methods, run on the subscriber's computer, while CM Configuration Server methods run on the CM Configuration Server computer.

object

An object is a data structure containing variables stored in a file with an `.EDM` suffix on the CM agent computer. An object can consist of one or more instances. Each instance contains the same set of variables. The values held in the variables can vary from instance to instance.

Use the CM Admin CSDB Editor to view, edit, or create objects.

preloading

Preloading is the process of loading the application to be distributed before any CM agents request the software. It requires a resolution of the CM Proxy Server's desired state on the CM Configuration Server before the applications can be loaded, either directly from the CM Configuration Server, or indirectly from another CM Proxy Server. The preload resolution is performed using TCP. The files may be deployed using TCP or HTTP, or a CM Multicast Server.

resource

Also called *file*.

A resource is a single component that is bundled into a package. Examples of resources are files, desktop links, and sets of registry keys.

REXX

CM REXX is an interpreted language that provides a simple way to customize various aspects of CM processing.

STAGER instance

The STAGER instance in the PRIMARY.POLICY Domain of the CM-CSDB contains information necessary for the CM agent to connect to the CM Proxy Server to obtain its needed resources. A STAGER instance can also specify the protocol and deployment source used to preload a CM Proxy Server.

static cache

The static cache is the CM Proxy Server's primary cache, managed by the Preloader. After installing the CM Proxy Server, this cache is preloaded with services as defined in the CM-CSDB as its desired state. The services may be deployed from the CM Configuration Server or another CM Proxy Server.

subscriber

A subscriber is the person who uses managed applications on a CM agent computer.

variable

A variable is a piece of named storage that contains a changing value. The variable's value forms a part of the CM agent's resolved desired-state and can influence the resolution process through messaging or symbolic substitution.

Index

A

- access levels, 9
- Activity Log Collection, 93
- agent, and static cache, 22
- AIX, 35
- ALTADDRM attribute, 79
- Apache-based Proxy Server. *See* CM Enterprise Proxy Server
- Application Manager. *See* CM Application Manager
- Application Self-service Manager. *See* CM Application Self-service Manager
- applications, definition, 121
- Assign Proxy Server task, 93
- attribute, 79
- attribute property, definition, 121
- attribute, definition, 121

B

- Basic User Authentication, 64

C

- CFG files, 45
- CGMTDATE attribute, 79
- CM Admin Agent Explorer, description, 121
- CM Admin CSDB Editor, description, 123
- CM agent computer, definition, 121
- CM Application Manager
 - description, 121
- CM Application Self-service Manager
 - description, 122
- CM Configuration Server

- description, 122
- enabling for HTTP, 89

- CM Enterprise Proxy Server
 - comparison with CM Proxy Server, 118
 - configuration file httpd.conf, 115
 - data cache management, 117
 - installation tasks, 112
 - installing a caching server, 113
 - installing a co-located server, 112
 - LogLevel, resetting, 115
 - Max Size of data cache, 117
 - platform support, 111
 - preloading, 117
 - purging data cache, 117
 - removing, 116
 - requirement for secured network, 111
 - requirements for caching server, 112
 - requirements for CM Infrastructure, 112
 - requirements for co-located server, 112
 - starting the service, 115
 - stopping the service, 114
 - synchronizing data cache, 117
 - Windows services, 114

- CM Infrastructure Server, 55

- CM Integration Server directory structure, 49

- CM Portal

- Assign Proxy Server task, 97
- CM Proxy Server tasks, 28
- description, 28
- Install CM Agent task, 97
- installing to remote location, 46
- Purge Dynamic Cache task, 25
- Purge Proxy Server Dynamic Cache task, 95
- Synchronize Proxy Server task, 94
- using Proxy Servers to install CM agents, 97

- CM Proxy Server

- Apache-based. *See* CM Enterprise Proxy Server
- benefits, 19

- co-located, 26
- configuring, 32, 50
- description, 17
- directory structure, 49
- firewall, configuration examples, 64
- installation options, 35
- installing CM agents, 97
- local installation, 37
 - UNIX, 40
 - Windows, 37
- log files, 102
- platform support
 - UNIX, 35
 - Windows, 35
- preloading, 94
- process flow, 21
- processing, 20
- purging dynamic cache task, 95
- remote installation, 44
- starting, 92
- starting for UNIX, 43
- stopping, 92
- stopping for UNIX, 43
- synchronizing, 94
- system requirements, 33
 - hardware recommendations, 33
 - UNIX, 35
 - Windows, 34

CM Proxy Server using Apache. *See* CM Enterprise Proxy Server

CM-CSDB, description, 122

co-located CM Proxy Server

- Apache-based. *See* CM Enterprise Proxy Server
- definition, 26
- installing and configuring, 66
- required configurations, 65
- static type of server, 22
- when to use, 27

configuring

- CM agent, 85
- Proxy Server, 32

CONNECT.LOG, 102

copyright notices, 2

D

- deployment destinations, definition, 23
- deployment source, definition, 23
- document changes, 5
- documentation updates, 4
- dynamic cache, 20
 - CM Configuration Server purge protection, 68
 - configuring parameters, 58
 - definition, 123
 - description, 24
 - fail-over support, 60
 - freespace after purge, 63
 - management, 25
 - purging, 25
 - purging from CM Portal, 93
 - size-based purge, 62
- Dynamic Cache Purge, 93
- dynamic parameter, 52
- Dynamic PassThru, 20, 25
 - description, 24
- dynamic-allow-shared-resource-purge parameter, 52, 68
- dynamic-defcls parameter, 52
- dynamic-defdmn parameter, 52
- dynamic-freespace parameter, 52
 - example, 63
- dynamic-largefile-mindays parameter, 53
 - example, 63
- dynamic-largefile-size parameter, 53
 - example, 63
- dynamic-makeidx parameter, 53
- dynamic-maxdays parameter, 53
- dynamic-maxdays parameter, 61
- dynamic-maxsizeMB parameter, 53
 - example, 62, 63
- dynamic-prefix parameter, 53
- dynamic-proxy-host parameter, 54

- dynamic-proxy-pass parameter, 54
- dynamic-proxy-port parameter, 54
- dynamic-proxy-user parameter, 54
- dynamic-root parameter, 54
- dynamic-savefreq parameter, 54
 - example, 62
- dynamic-savefreq parameter, 61
- dynamic-savetod parameter, 54
 - example, 62
- dynamic-savetod parameter, 61
- dynamic-ssl parameter, 54
- dynamic-trace parameter, 55
- dynamic-url parameter, 55
- dynamic-url parameter, 60

E

- entitlement, for Preloader, 22

F

- firewall server, 64
- freespace purge, 25

H

- HP OVCN Integration Server, installing CM agents from Proxy Server, 98
- HP OVCN Proxy Server, 114
- HP Technical Support, collecting information, 107
- HP-UX, 35
- HTTP configurations, 27
 - CM agents, 85
- httpd parameter, 55
- httpd.rc file, 103
- HTTPD.TKD, 107
- HTTPD:3466.log, 109
- httpd-3466.error.txt, 102
- httpd-3466.log, 102
- httpd-port.log, 102

Index

- httpd-port.YY.MM.DD.log, 102
- httpd-prefix parameter, 55
- httpd-rps service, 114
- httpd-rps-cache service, 114
- httpd-trace parameter, 55

I

- Install CM Agent task, 97
- Install Proxy Server task, 45
- installation directory, 102
- installation options, for the Proxy Server, 35
- installing the CM proxy server
 - remote directory, 44
- installing the CM Proxy Server
 - local directory, 37
- instance, definition, 123
- Internet proxy, 64
- IRPStackSize in Registry, 104

L

- large files, exempting from dynamic cache purge, 63
- legal notices
 - copyright, 2
 - restricted rights, 2
 - warranty, 2
- license file, required, 36
- license.nvd, location, 36
- Linux, 35
- log level, changing, 103
- logs
 - httpd-3466.error.txt, 102
 - httpd-port.log, 102
 - httpd-port.YY.MM.DD.log, 102
- logs\rps subdirectory, 102

M

- maintenance updates, 49

Manage Proxy Assignment task. *See* Assign Proxy Server task

MCPRELOAD instance, 79

method, definition, 123

MULTICAST instance, 79

N

Navigation aid, 94

new features, 4

NVDKIT, 107

nvdkit.exe, obtain version information, 108

O

object, definition, 124

P

Troubleshooting, 104

PFS package, 37

pfs_mount, 37

platform support, 111

Portable File System, 37

Preloader, description, 22

preloading

- deployment options, 73

- using HTTP, 74

- using HTTPS, 77

- using multicast, 78

- using multicast with dynamic windows, 81

- using SSL (TCPS and HTTPS), 75

- using TCPS, 76

- using the CM Portal, 94

preloading, definition, 124

problem reporting, 109

product updates, applying, 49

Purge Dynamic Cache task, 25

Purge Proxy Server Dynamic Cache task, 95

- periodic scheduling, 96

purging dynamic cache, 25

R

Red Hat Enterprise Linux, 35

resource, definition, 124

restricted rights legend, 2

REXX, description, 124

rps.cfg, 50

- configuration parameters, 52

- sample file, 50

rps.cfg file, 45

- editing, 57

- selecting, 47

- syntax, 57

RPS.TKD, 107

S

Schedule window, 95

Service Control Manager window, 92

Service Pack updates, 49

Services window, 92

Software Manager. *See* CM Application Self-service Manager

Solaris, 35

STAGER Class, 85

STAGER instance

- connecting to Workgroups, 86

Stager Instance attributes, 78

STAGER instance, description, 124

stager parameter, 55

stager-addr parameter, 55

stager-port parameter, 55

stager-trace parameter, 56

starting the CM Proxy Server for UNIX, 43

static cache

- definition, 124

- description, 21

static type

- agent, 33
 - server, 33
- static-host parameter, 56
- static-logsize parameter, 56
- static-port parameter, 56
- static-proxy-host parameter, 56
- static-proxy-pass parameter, 56
- static-proxy-port parameter, 56
- static-proxy-user parameter, 56
- static-root parameter, 56
- static-ssl parameter, 57
- static-trace parameter, 57
- static-type parameter, 57
- static-user parameter, 57
- Statistical Data Collection, 93
- subscriber, definition, 124
- Summary window, 95
- SUSE LINUX Enterprise Server, 35
- Synchronize Proxy Server task, 94

T

- TCP/IP configuration, 87

- technical support, 107
- ticket, opening, 109
- trace levels, 104

U

- updates to doc, 4
- upstream host, 20

V

- variable, definition, 125

W

- warranty, 2
- Web Proxy, 64

Z

- ZDATAURL field, 85
- ZHTTPMGR, 66
 - removing, 68
- ZPCPROTL field, 85
- ZSTGPORT attribute, 88
- ZSTGSRVR attribute, 88

