

# HP Operations Manager Dependency Mapping Automation

For Windows®, UNIX®, and Linux Operating Systems

Software Version: 8.20

---

## Installation and User's Guide

Manufacturing Part Number: None

Document Release Date: July 2011

Software Release Date: July 2011



## 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 2007-2011 Hewlett-Packard Development Company, L.P.

### Trademark Notices

Adobe® and Acrobat® are trademarks of Adobe Systems Incorporated.

AMD and the AMD Arrow symbol are trademarks of Advanced Micro Devices, Inc.

Google™ and Google Maps™ are trademarks of Google Inc.

Intel®, Itanium®, Pentium®, and Intel® Xeon® are trademarks of Intel Corporation in the U.S. and other countries.

iPod is a trademark of Apple Computer, Inc.

Java is a registered trademark of Oracle and/or its affiliates.

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

Oracle is a registered trademark of Oracle Corporation and/or its affiliates.

UNIX® is a registered trademark of The Open Group.

## Documentation Updates

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

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

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

**<http://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.

## Support

You can visit the HP software support web site at:

**[www.hp.com/managementsoftware/services](http://www.hp.com/managementsoftware/services)**

HP software online support provides an efficient way to access interactive technical support tools. As a valued support customer, you can benefit by using the support site to:

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

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

To find more information about access levels, go to:

**[www.hp.com/managementsoftware/access\\_level](http://www.hp.com/managementsoftware/access_level)**

To register for an HP Passport ID, go to:

**[www.managementsoftware.hp.com/passport-registration.html](http://www.managementsoftware.hp.com/passport-registration.html)**

# Contents

1	Overview	15
	Advantages of HPOM DMA	15
	Creating Business Service Views Automatically	16
	Launching UCMDB CI Change Information	18
	Sharing Configuration Item Information	20
	Identifying New Servers and Applications	21
2	HPOM DMA Users	23
	Service View Designers	23
	UCMDB Discovery Administrators	24
	Integrators	24
	HPOM Administrators	25
	HPOM Operators	26
	Application Support Engineers	26
3	Concepts of HPOM DMA	27
	Synchronizing Data	27
	Configuring Active Synchronization Tasks	30
	Getting Data from BAC or UCMDB	31
	Creating CI Hierarchies	31
	Enriching CI Hierarchies with Mapping Rules	32
	Applying Service Mapping	32
	Applying Node Mapping	34
	Applying Attribute Mapping	35
	Assigning User Roles and Profiles	38
	Manipulating CI Hierarchies with Scripting	39
	Mapping HPOM Messages to Services	41
	Mapping Messages to Virtual Services	43

Separating Hints and Hostnames .....	44
Mapping HPOM Messages to Services Synchronized from UCMDB.....	45
Customizing Service IDs .....	46
Assigning Custom Message Attributes to Messages.....	46
Discovering Services .....	48
<b>4 Preparing HPOM DMA .....</b>	<b>51</b>
Installation Distribution .....	51
Product Prerequisites .....	52
HP Operations Manager.....	52
Proxy System for HPOM for UNIX on PA-RISC Systems .....	53
HP Universal CMDB or HP Business Availability Center.....	54
HPOM Patches.....	56
HPOM DNS Requirements .....	56
HPOM for UNIX or Linux Agents.....	56
Microsoft Visual C++ 2005 SP1 Redistributable Package.....	57
Hardware Requirements for HPOM DMA.....	57
Temporary Disk Space Requirements During Installation .....	57
Browser Requirements for HPOM DMA .....	58
VMware Workstation Installations.....	58
Additional Prerequisites and Configurations.....	59
Enabling HPOM DMA to Access UCMDB or BAC .....	59
Installing IIS after the .NET Framework on Windows HPOM DMA Systems.....	60
Enabling Licensing on 64-bit Windows HPOM DMA Systems .....	60
Setting Up Discovery Data.....	61
Enabling UI Launch from HPOM to BAC or UCMDB.....	61
<b>5 Installing HPOM DMA .....</b>	<b>63</b>
Installing on Clusters .....	63
Applications Stopped and Restarted During Installation .....	64
Applications Stopped and Restarted on HPOM for UNIX or Linux .....	64
Applications Stopped and Restarted on HPOM for Windows .....	64
Repairing an HPOM DMA Installation .....	64

Loading the Installation Media on UNIX or Linux . . . . .	65
Installing HPOM DMA . . . . .	66
Configuring Smart Message Mapping in Cluster Environments . . . . .	71
Configuring HPOM for UNIX Clusters Environments. . . . .	71
Configuring HPOM on Linux Cluster Environments. . . . .	72
Starting the HPOM DMA Console . . . . .	73
Further Essential Installation and Configuration Steps. . . . .	73
<b>6 Installing HPOM DMA for HPOM for UNIX on PA-RISC Systems . . . . .</b>	<b>75</b>
Installing on Clusters . . . . .	76
Applications Stopped and Restarted During Installation . . . . .	76
Repairing an HPOM DMA Installation . . . . .	77
Loading the Installation Media. . . . .	77
Installing on the PA-RISC HPOM Host System . . . . .	78
Installing on the HPOM DMA Windows Host System . . . . .	80
Post-Installation Steps on the PA-RISC Host System . . . . .	85
Post-Installation Steps on the Windows Host System. . . . .	88
Starting the HPOM DMA Console . . . . .	89
Further Essential Installation and Configuration Steps. . . . .	89
<b>7 Configuring HPOM DMA. . . . .</b>	<b>91</b>
Managing Users and Passwords . . . . .	93
Adding a User . . . . .	93
Changing a Password . . . . .	94
Deleting a User . . . . .	94
Listing Users. . . . .	94
dmauser Usage . . . . .	95
Configuring UCMDB or BAC . . . . .	96
Deploying HPOM DMA Packages to UCMDB or BAC . . . . .	97
Reviewing the HPOM DMA Packages. . . . .	98
Adapting HPOM DMA TQL Queries. . . . .	102
Apply Enrichment Rules . . . . .	105
Configuring HPOM for UNIX or Linux . . . . .	107
Assigning the CMDB Service Group to an HPOM User. . . . .	107
Assigning the CMDB Node Groups to an HPOM User . . . . .	108

Assigning the OM DMA Policy Group . . . . .	108
Deploying the OM DMA Policy Group . . . . .	108
Creating Service Type Definitions Automatically . . . . .	108
Assigning User Profiles for Services on HPOM for UNIX or Linux. . . . .	109
Profile Prerequisites . . . . .	109
Mapping User Profiles. . . . .	110
Enabling User Profile Assignment. . . . .	110
Automating Policy Distribution . . . . .	111
Configuring HPOM Agent Types . . . . .	111
Update HPOM DMA After Adding a New Agent Type . . . . .	112
Configuring HPOM for Windows . . . . .	114
Creating Service Type Definitions Automatically . . . . .	114
Assigning User Roles for Services on HPOM for Windows . . . . .	115
User Role Prerequisites. . . . .	115
Mapping User Roles . . . . .	115
Enabling User Role Assignment. . . . .	115
Assigning and Deploying the OM DMA Policy Group . . . . .	116
Configuring HPOM DMA . . . . .	117
Specifying Web Service Endpoints. . . . .	117
Specifying Synchronization Content. . . . .	117
Synchronizing Nodes and Services . . . . .	118
<b>8 Upgrading HPOM DMA . . . . .</b>	<b>119</b>
Upgrading on Cluster Nodes. . . . .	119
Upgrading HPOM DMA 8.10 to 8.20 . . . . .	120
Updating the HPOM DMA Discovery Pattern in UCMDB or BAC . . . . .	122
Updating Containment Relationship Mappings . . . . .	123
<b>9 Additional Features for HPOM DMA. . . . .</b>	<b>125</b>
Installing and Configuring the UI Launch. . . . .	127
Configure a Profile Database or User Schema . . . . .	127
Prerequisites . . . . .	127
Add a Database . . . . .	128
Uploading Tools into HPOM for UNIX or Linux. . . . .	129
dmadrilldown-toolgen.sh Command Parameters. . . . .	129
Assigning Tool Groups . . . . .	131



Uploading Tools into HPOM for Windows.....	131
dmadrilldown-toolgen.bat Command Parameters.....	131
Configuring the UI Launch Web Application.....	133
Configuring Smart Message Mapping.....	134
Enabling Server MSI on UNIX or Linux.....	134
Enabling Server MSI on Windows.....	135
Starting and Stopping Smart Message Mapping.....	135
Customizing Smart Message Mapping.....	135
Configuring the Hint Separator.....	137
Configuring the Hostname Separator.....	138
Configuring Case Sensitivity.....	138
Configuring the Update Delay.....	139
Configuring the Polling Interval.....	139
Assigning Custom Message Attributes to Messages.....	140
Changing the Order of MSI Processes.....	140
Setting the Order in HPOM for UNIX or Linux.....	141
Setting the Order in HPOM for Windows.....	141
Smart Message Mapping Simulation.....	142
Customizing the ID of Services Synchronized from UCMDB.....	143
Customizing the Service ID with Attribute Mapping.....	144
Customizing the Service ID with Scripting.....	145
Selecting the Discovery Source.....	146
Disabling SPI Discovery Service Upload for HPOM for UNIX or Linux.....	146
Disabling SPI Discovery Service Upload for HPOM for Windows.....	147
Disabling Discovery from a SPI from the HPOM for Windows UI.....	147
Disabling Discovery from a SPI using XPL Configuration.....	148
Restricting Service Synchronization to Managed Nodes.....	149
Modifying the UCMDB or BAC Classloader.....	149
Installing the BAC or UCMDB Discovery Pattern for HPOM.....	150
Modifying the TQL Queries to Specify the HPOM Management Server.....	153
Integrating Business Process Monitoring.....	159
Forwarding BPM Alerts to HPOM.....	159
Setting Up CI Status Alerts.....	159
Setting Up Performance Limit Alerts.....	161
Synchronizing EUM Views.....	162

Installing the BAC Package for EUM Synchronization with HPOM DMA . . . . .	162
Activating the End User Monitors Synchronization Package. . . . .	164
<b>10 Licensing . . . . .</b>	<b>165</b>
OVkey Licenses . . . . .	165
Types of Licenses . . . . .	166
Checking Licenses. . . . .	167
Installing Licenses on 64-bit Windows HPOM DMA Systems. . . . .	167
Setting Up OVkey Licenses. . . . .	169
Getting the Required Information . . . . .	169
Requesting a Product License . . . . .	171
Requesting by Internet . . . . .	171
Requesting by Mail, Phone or Fax. . . . .	172
Receiving License Passwords . . . . .	173
Installing Product Licenses . . . . .	173
Verifying Product Licenses. . . . .	174
<b>11 Securing . . . . .</b>	<b>175</b>
Configuring Secure Communication between HPOM DMA and HPOM . . . . .	176
Exporting Certificates on HPOM for UNIX or Linux Management Servers. . . . .	177
Securing Clustered Systems with SSL . . . . .	179
Configuring Tomcat for non-SSL HTTP . . . . .	179
Exporting Certificates on HPOM for Windows Management Servers. . . . .	180
Configuring IIS for non-SSL HTTP . . . . .	182
Importing Certificates in HPOM DMA . . . . .	183
Restricting IIS Access to a Single Port . . . . .	186
Setting Up a Distributed System. . . . .	186
Adding the HPOM DMA Context. . . . .	187
Restricting Access to Localhost . . . . .	188
Change the Tomcat Server AJP Port . . . . .	188
LDAP Authentication . . . . .	190
Configuring LDAP Access . . . . .	193
Logging In Using LDAP Authentication . . . . .	195
<b>12 Backup, Restore, and Migration . . . . .</b>	<b>197</b>
Backing Up an HPOM DMA Configuration . . . . .	197

Backing Up HPOM DMA TQL Queries .....	198
Restoring the Default HPOM DMA Configuration .....	199
Moving an HPOM DMA Configuration .....	200
Recreate a Synchronization Package .....	200
Make a Copy of a Synchronization Package .....	202
<b>13 Uninstalling</b> .....	<b>203</b>
Uninstalling HPOM DMA .....	203
Post-Uninstallation Cleanup .....	206
Removing the HPOM DMA Synchronization Packages and Configuration Files . . .	206
Removing the HPOM DMA Data Files .....	206
Removing Log Files .....	206
Cleaning Up UCMDB or BAC .....	208
Cleaning Up HPOM for UNIX or Linux .....	211
Cleaning Up HPOM for Windows .....	211
Deleting Imported Services .....	211
Removing the OM DMA Policy Group .....	212
Deleting HPOM DMA Node Groups .....	212
Removing UI Launch Tools and Applications .....	212
Unconfiguring Smart Message Mapping .....	213
Resetting the Discovery Source to SPI Discovery .....	213
Resetting the Discovery on HPOM for UNIX or Linux .....	213
Resetting the Discovery on HPOM for Windows Using the GUI .....	214
Resetting the Discovery on HPOM for Windows Using XPL .....	214
Cleaning Up BPM Integration .....	215
Deleting CI Status Alerts .....	215
Deleting Performance Limit Alerts .....	215
<b>14 Performance and Configuration Tips</b> .....	<b>217</b>
Increasing Tomcat Server Memory .....	218
Adding Missing Node Attribute .....	218
Changing XPL Configuration Parameters .....	219
Web Service Client .....	219
Changing Non-XPL Configuration Parameters .....	221
HPOM for Windows Web Services .....	221
Tomcat Server .....	222

Changing the HPOM Web Service Credentials . . . . .	223
Changing the Port of HPOM DMA Tomcat . . . . .	223
Changing Log File Parameters . . . . .	224
Smart Message Mapping . . . . .	225
Messages Mapped to Wrong Nodes . . . . .	225
No Messages are Mapped . . . . .	225
Analyzing Synchronization Error Messages . . . . .	227
Analyzing LDAP Configuration Errors . . . . .	228
<b>A HPOM DMA Reference Information . . . . .</b>	<b>229</b>
Installation Locations . . . . .	229
Configuration Files . . . . .	231
Data Files . . . . .	234
Log Files . . . . .	235
Objects Installed on HPOM . . . . .	237
Node Groups . . . . .	237
Root Service . . . . .	237
Propagation and Calculation Rules . . . . .	237
Service Type Definitions . . . . .	238
Policies . . . . .	239
Standard Synchronization Package Locations . . . . .	241
HPOM DMA Default Synchronization Package . . . . .	243
Service Mapping . . . . .	243
Attribute Mapping . . . . .	243
All CI Types . . . . .	243
SQL Server, Oracle, and Sybase Database CI Types . . . . .	244
Host, NT, and Unix CI Types . . . . .	244
Pre-Mapping Script . . . . .	248
Host, NT, and UX CI Types . . . . .	248
IP CI Type . . . . .	248
UNIX OS Synchronization Package: dmaOS . . . . .	249
Node Mapping . . . . .	249
Windows OS Synchronization Package: dmaWinOS . . . . .	250
Node Mapping . . . . .	250

Informix Synchronization Package: dmaInformix . . . . .	251
Service Mapping . . . . .	251
Node Mapping . . . . .	251
Microsoft SQL Server Synchronization Package: dmaMSSQLServer . . . . .	252
Service Mapping . . . . .	252
Node Mapping . . . . .	252
Oracle Synchronization Package: dmaOracle . . . . .	253
Service Mapping . . . . .	253
Node Mapping . . . . .	253
Sybase Synchronization Package: dmaSybase . . . . .	254
Node Mapping . . . . .	254
Group Multiple Host Resource Types Synchronization Package . . . . .	255
Trigger Policy Distribution Synchronization Package . . . . .	255
My Company Synchronization Package: dmaMyCompany . . . . .	256
End User Management Synchronization Package: dmaEUM . . . . .	256
DNS Mapping Synchronization Package: dmaDnsMapping . . . . .	257
HPOM DMA Configuration Parameters in XPL . . . . .	258
Open Source Software . . . . .	262
<a href="#">Index</a> . . . . .	263



---

# 1 Overview

HP Operations Manager (HPOM) Dependency Mapping Automation (DMA) enables IT operations teams to align their activities more fully with the business services that the IT infrastructure supports. By providing automated dependency mapping and configuration consistency across multiple HPOM servers, HPOM DMA optimizes the ability of IT organizations to support their businesses, and enables enhanced productivity and efficiency within the operations teams.

## Advantages of HPOM DMA

HPOM DMA helps you to do the following:

- **Automate Maintenance**

Automate and simplify the creation and maintenance of business service views within HPOM to enable business-focused impact and root cause analysis for operational incidents.

- **Streamline Analysis**

Streamline incident analysis activities by providing drill-down from managed nodes or services in HPOM into their change history within the HP Universal CMDB (UCMDB).

- **Consolidate Information**

Consolidate systems and managed services information in a single place, the UCMDB database, to provide shared and consistent views across multiple HPOM servers.

- **Monitor Infrastructure**

Rationalize the process of identifying new servers and applications, and the deployment of HPOM monitoring to business-critical infrastructure.

# Creating Business Service Views Automatically

Aligning the activities of the IT organization with the needs of the business is an ongoing challenge that is under increasing scrutiny in many companies. IT investments and resources need to be targeted and prioritized so that they maximize the value that they deliver to the business processes and users that IT supports.

In IT operations environments, managing resources is a significant challenge because of the complexity associated with understanding the relationships between the business applications and the IT infrastructure that supports them.

HPOM DMA addresses this exact issue. By connecting HPOM to UCMDB — and the system and application service dependency information within it — HPOM DMA can construct business service views within HPOM. These business service views provide your operations staff with a unique insight into the impact of infrastructure events.

Configuration item (CI) information, such as systems, applications, network devices, business services, and the dependency information that defines the relationships between CIs, can be added to UCMDB in a number of ways:

- HP Software Discovery and Dependency Mapping can automatically populate and maintain both CI and dependency information in UCMDB.
- UCMDB federation capabilities can consume CI and dependency information from existing third party CMDBs, and make this information available to HPOM DMA.
- CI information can be manually loaded as part of the initial setup.

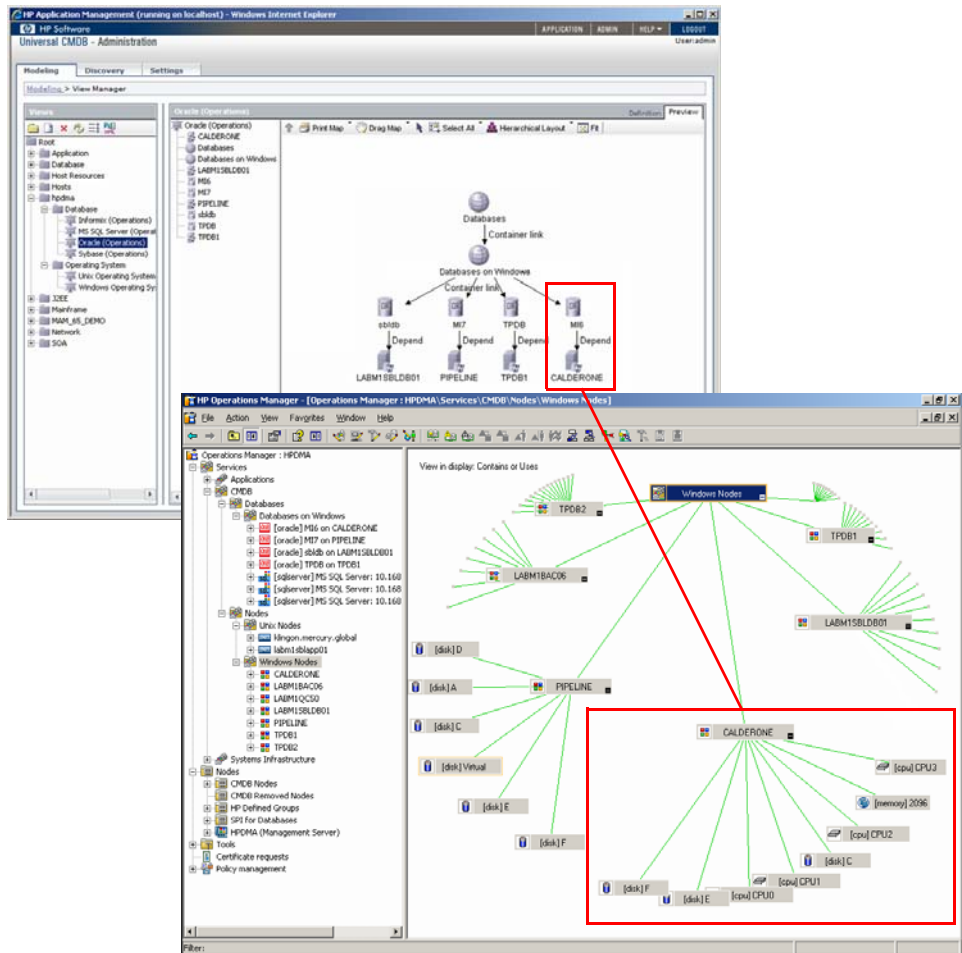
HPOM DMA consumes information from UCMDB, and uses it to populate the node banks within HPOM. HPOM DMA also creates service trees that can include discovered applications and the dependencies between these applications. For example, consider an online retail application with web servers situated in a DMZ (De-Militarized Zone) to service customers on the Internet. These web servers communicate with back-end database and application servers in the corporate intranet. The successful processing of customer orders depends on this interaction. HPOM DMA can automatically add this dependency information to the service maps within HPOM.



Service maps within HPOM include much greater business service context. Impact analysis indicates more than just the affected application. It shows the impacted business service. Your operations staff can use business service views to show when incidents are threatening the availability of the business processes which rely on the IT infrastructure.

Figure 1 the upper-left screen shows discovery data within UCMDB. The lower-right screen shows the associated CI information that HPOM DMA has added to the HPOM for Windows Service Map. It also shows some associated hardware dependency details.

**Figure 1 Discovery Data in UCMDB and CI Information in HPOM**



# Launching UCMDB CI Change Information

Surveys show that the majority of IT infrastructure incidents are caused by uncoordinated changes, such as equipment moves, configuration changes, or minor software or firmware updates. These changes often happen outside of the sanctioned change management processes, so there is no formal record of them in the change management system.

UCMDB discovery mechanisms have the ability to detect and record a wide variety of configuration changes to infrastructure elements. These changes are stored within UCMDB, and are available from within HPOM when HPOM DMA is installed.

When your operators see a notification of an infrastructure event within HPOM, using UI Launch, they can drill down directly into UCMDB change history. Your operators can review the change history for the impacted CI to determine if a recent change may be the root cause of the event. UI Launch significantly enhances the operator's ability to diagnose an event, and speeds up the problem analysis and resolution processes.

Figure 2 shows that the UNIX node klingon has encountered an issue (klingon is shown with a critical red status). Launching the change history facility enables viewing of UCMDB data. It reveals that a number of directory names have been changed, and that this may be causing some issues.

**Figure 2 UI Launch from HPOM to Show Change Report**

The screenshot displays the HP Operations Manager interface. A 'Select the Tool to Execute' dialog box is open over the 'klingon' node in the tree view. The 'Show Change Report in UCMDB' option is selected. Below, a web browser window shows the 'Change Report for klingon' page. The report includes a table of CI changes and a section for relationship changes.

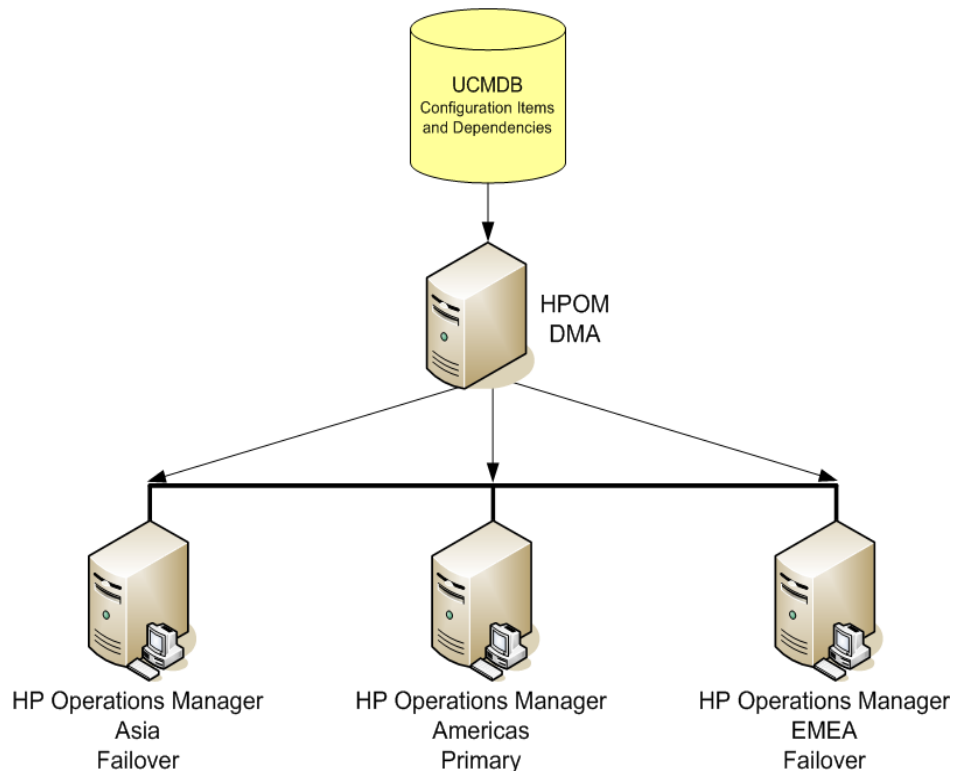
Type	CI label	CIT Name	CI attribute	New Value	Old Value	Change Date	Changer
Updated CI	klingon	Dir	Display Label	/home/sshhd	dir	8/12/07 4:36 PM	CMDB: Recalculate a
Updated CI	klingon	Dir	Display Label	/var/adm	dir	8/12/07 4:36 PM	CMDB: Recalculate a
Updated CI	klingon	Dir	Display Label	/usr/bin	dir	8/12/07 4:36 PM	CMDB: Recalculate a
Updated CI	klingon	Dir	Display Label	/home/aaaaaaaa	dir	8/12/07 4:36 PM	CMDB: Recalculate a
Updated CI	klingon	Dir	Display Label	/	dir	8/12/07 4:36 PM	CMDB: Recalculate a
Updated CI	klingon	Dir	Display Label	/usr/net/nls	dir	8/12/07 4:36 PM	CMDB: Recalculate a
Updated CI	klingon	Dir	Display Label	/usr/lib/uucp	dir	8/12/07 4:36 PM	CMDB: Recalculate a
Updated CI	klingon	Dir	Display Label	/home/mysql	dir	8/12/07 4:36 PM	CMDB: Recalculate a
Updated CI	klingon	Dir	Display Label	/	dir	8/12/07 4:36 PM	CMDB: Recalculate a

Relationship changes  
No data was found.

# Sharing Configuration Item Information

In environments where multiple HPOM servers are used in disaster-tolerant and failover configurations, it is vital that node data is replicated across cooperating HPOM servers. Replication of key parts of the service maps is equally important where HPOM servers participate in expert center or follow-the-sun architectures. However, maintaining a consistent set of node lists and service map objects across two or more HPOM servers can involve time-consuming manual processes. Whenever manual processes are involved, discrepancies and errors can occur.

**Figure 3 Multiple HPOM Servers Sharing UCMDB Data**



Using HPOM DMA, multiple HPOM servers can consume node lists and service object information from a single UCMDDB. UCMDDB provides the single source for this information. All HPOM servers connected to UCMDDB can see exactly the same CIs.

Figure 3 shows three HPOM servers sharing node list and service object information from a single UCMDDB.

## Identifying New Servers and Applications

Monitoring key servers and the applications that support business processes is a vital step in ensuring that the activities of IT are aligned with the business. In complex environments, tracking and ensuring that all relevant servers are adequately monitored can be a time-consuming manual process.

HPOM DMA can take the guesswork out of this activity. As new servers are installed, updated, or have new applications deployed to them, UCMDDB discovery processes detect these changes. New systems and services, and changes to existing ones, are stored in UCMDDB and are available to HPOM DMA. HPOM DMA populates the node banks and service maps within HPOM with information about systems and services that are not currently monitored.

Because HPOM DMA derives system, application and business service dependency information from the data in UCMDDB, it helps operational staff to identify which new systems are important. Using the business service dependency information in the Service Maps, you can identify new systems (or changed systems) that fulfill a role in delivering key business services and that need specific monitoring.

You can also automate the deployment of monitoring to new or updated nodes.



---

## 2 HPOM DMA Users

This chapter contains the following sections:

- [Service View Designers](#) on page 23
- [UCMDB Discovery Administrators](#) on page 24
- [Integrators](#) on page 24
- [HPOM Administrators](#) on page 25
- [HPOM Operators](#) on page 26
- [Application Support Engineers](#) on page 26

### Service View Designers

Service view designers are responsible for designing service views for HPOM Service Navigator. Service views are used by HPOM operators to fulfill their tasks. Service view designers must also regularly keep the service models up to date. They know the operational management processes of their organizations, and have a solid understanding of the application topologies. They are involved in both testing and production environments and are not expected to have programming skills.

Service view designers create design specifications for applications at the class level. If necessary, they get input on application details and application topology from application experts and HPOM operators. Service Navigator topology requirements are necessary for troubleshooting. They then implement the design specifications into TQL queries, which define the node and service CIs in UCMDB to be synchronized with HPOM. And finally, they map CI types to Service Type Definitions (STD), which are used to identify how CIs from UCMDB are to be handled when building services in HPOM on synchronization.

Service view designers are also responsible for configuring the import schedule for extracting CIs from UCMDB and importing them into HPOM. This task can be delegated to the HPOM administrator.

## UCMDB Discovery Administrators

UCMDB discovery administrators configure discovery mechanisms in UCMDB to automatically keep the CMDB up to date through discovery. They must make sure that discovery data fulfills the needs of all UCMDB users. UCMDB discovery administrators are involved in both testing and production environments. They are required to have some programming skills if new discovery scripts need to be developed. UCMDB discovery administrator should also be able to extend discovery.

## Integrators

Integrators design and develop the following:

- Management policies
- Discovery policies
- Tools and actions
- Instrumentation
- Report templates
- Graphs
- Service Type Definitions (STD)

Integrators have a very thorough knowledge of the application that they are integrating (for example, Oracle, Exchange, and HPOM components such as policies). They typically work in a separate development environment.

Typically, integrators also work with HPOM DMA to do the following:

- Create Synchronization packages.
- Write scripts to extend the synchronization process.



- Enhance services in HPOM which are not derived from UCMDB with data from UCMDB.

Integrators create synchronization packages with significant value for their partners. They deliver the knowledge of how to manage an application to ensure availability and peak performance. The main integration-specific task is to create the STDs. These can also be created automatically. For details, see [Creating Service Type Definitions Automatically](#) on page 108.

Integrators must make sure synchronization packages are updated to work with the latest releases of HPOM, operating systems, and application platforms, and achieve an acceptable balance between time pressures and the required synchronization package functionality. They must also design synchronization packages that can be used in environments of very differing size and complexity, while meeting the monitoring needs of operators and second level support. Integrators should have some “real-world” application administration knowledge.

## HPOM Administrators

HPOM administrators are responsible for installing and configuring the HPOM environment including the database and agent setup. Configuration tasks include security configuration with users, user roles, flexible management (for example, manager-to-manager configuration), and backup and database maintenance.

HPOM administrators need to be trained on the administrative aspects of HPOM and related products. They are involved in both testing and production environments.

HPOM administrators are required to guarantee the continuous operation of the management environment and ensure timely adaptation of management systems. They must keep up to date with environmental and organizational changes (for example, security requirements), and monitor expansion of the environment. HPOM administrators need to be able to work with multiple technologies.

HPOM administrators set up node groups and implement the top-level services in Service Navigator. A top-level service can be some generic service or container to give the hierarchy a structure. These include infrastructure services, applications, business services, and regions.

HPOM administrators must also configure the import schedule for extracting CIs from UCMDDB and importing them into HPOM. This task may be performed by a specialist service view designer.

## HPOM Operators

HPOM operators are responsible for the operational status of the managed environment, including messages. They work on incoming messages, execute predefined actions, and troubleshoot using predefined workflows. More complex problems may require HPOM operators to create trouble tickets.

HPOM operators need to be trained on the operational procedures of managing the IT environment with HPOM and related products. They work in production environments.

HPOM operators must resolve problems as quick as possible with the help of service trees and the message browser. They can use HPOM DMA to drill down into HP Business Availability Center (BAC) or Universal CMDB (UCMDDB) to retrieve more detailed information.

## Application Support Engineers

Application support engineers work on trouble tickets to solve problems through detailed problem analysis and changing the configuration of managed objects. More complex problems may require HPOM operators to create new trouble tickets.

Application support engineers need in-depth application knowledge to be able to troubleshoot the installation and resolve problems. They work in production environments, ensuring timely adaptation of the managed application, and guaranteeing continuous operation of the system or application. They can use HPOM DMA to drill down into BAC or UCMDDB to retrieve more detailed information.

---

# 3 Concepts of HPOM DMA

This chapter explains the HPOM DMA concepts in more detail, including:

- [Synchronizing Data](#) on page 27
- [Mapping HPOM Messages to Services](#) on page 41
- [Discovering Services](#) on page 48

## Synchronizing Data

HPOM DMA uses TQL queries to retrieve data from BAC or UCMDB, and import nodes and create service hierarchies in HPOM. [Figure 4](#) shows the synchronization process.

**Figure 4 HPOM DMA Synchronization Process**

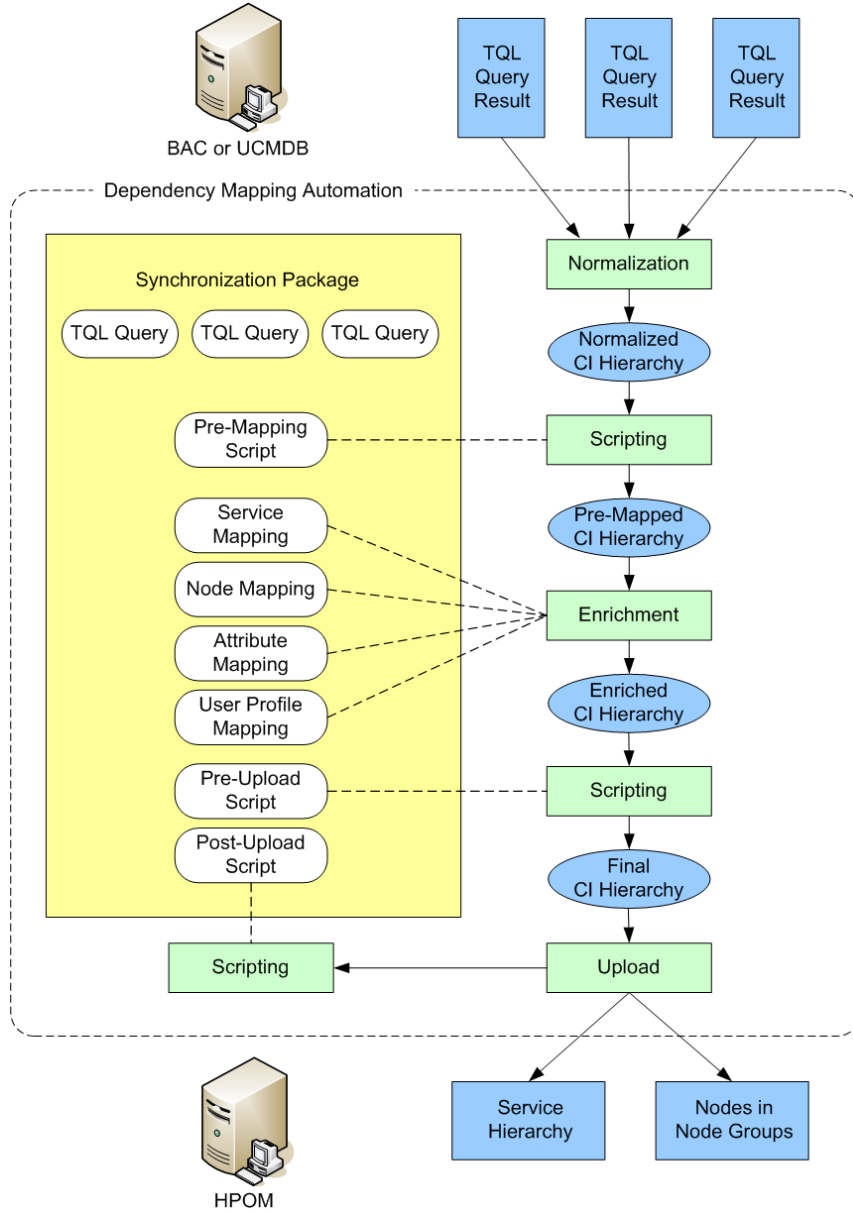
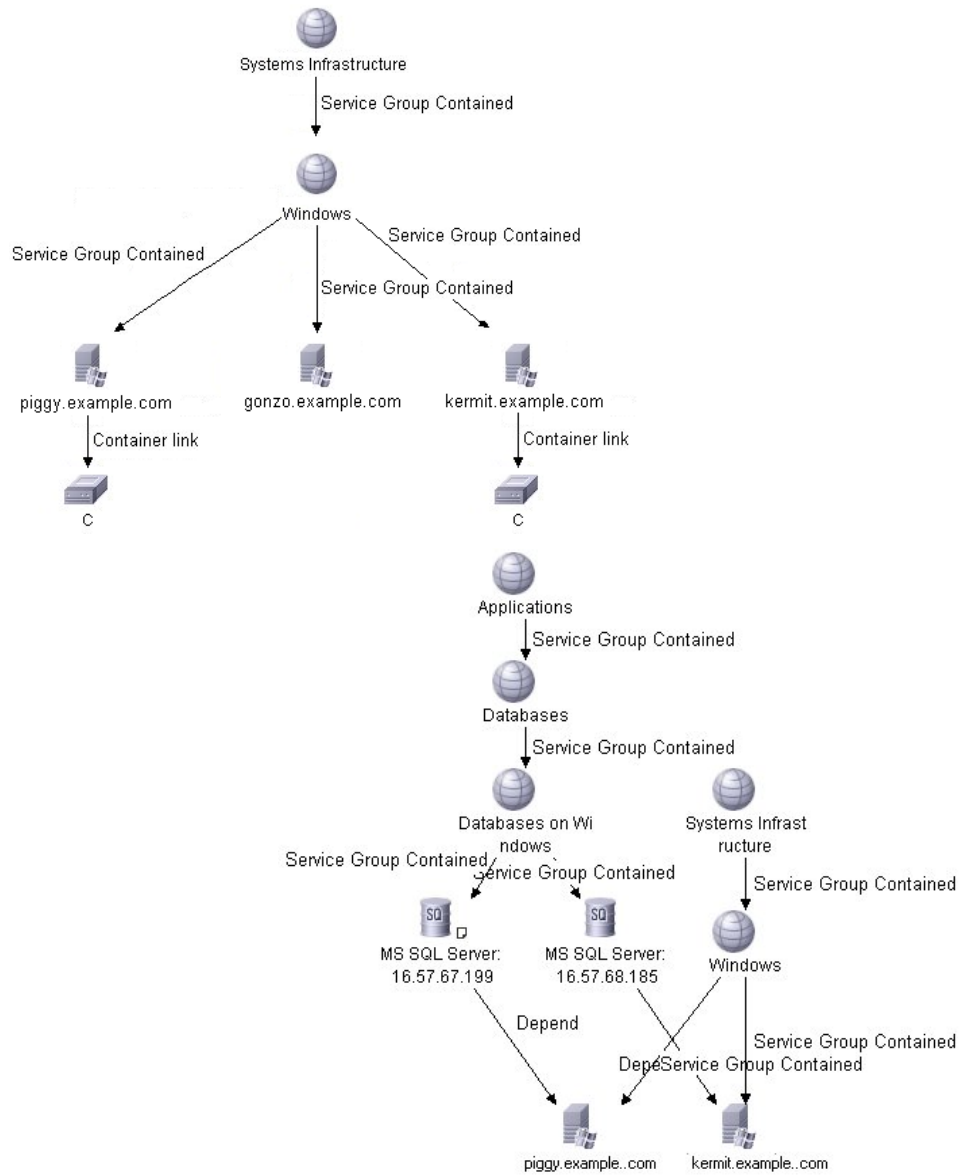


Figure 5 shows the result of two TQL queries: MS SQL and WIN OS. These are used as examples in the rest of this chapter.

**Figure 5 TQL Query Examples**



During a synchronization, the following steps are executed by HPOM DMA:

- [Configuring Active Synchronization Tasks](#)
- [Getting Data from BAC or UCMDB](#)
- [Creating CI Hierarchies](#)
- [Enriching CI Hierarchies with Mapping Rules](#)
- [Manipulating CI Hierarchies with Scripting](#)

These steps are described in the following sections.

## Configuring Active Synchronization Tasks

The active synchronization task contains the following information:

- **Root service:** The service under which the CI data is added. By default, this is CMDB.
- **The content that you want to synchronize:** The possibilities are CIs with services, and CIs with nodes or both. By default, both are selected.
- **TQL queries, mapping rules and scripts from all active synchronization packages.**

➤ Synchronization packages are containers that can have multiple TQL queries, mapping rules, and scripts. Each synchronization package has a priority that determines in which sequence the mapping rules and scripts are executed. The synchronization package concept supports easy extensibility.

In the example in [Figure 5](#) on page 29, three synchronization packages are active:

- **Databases**
  - Links to the MS SQL TQL
  - Contains Mapping rules
- **Systems**
  - Links to the Win OS TQL
  - Contains Mapping rules
- **Default**
  - No data
  - Contains mapping rules

## Getting Data from BAC or UCMDB

You retrieve data from UCMDB or BAC by getting the result of all active TQL queries. In the example shown in [Figure 5](#) on page 29, you retrieve the result of the MS SQL and the WIN OS TQL queries.

## Creating CI Hierarchies

HPOM Service Hierarchy distinguishes between two relationship types:

- Containment
- Dependency

The mapping from UCMDB relationship types to HPOM relationship types is preset:

- A containment relationship can be configured using the `<containmentrelations>` list of regular expressions. You can choose which relationship types are mapped to containment. This is specified in the `containmentrelations.xml` file. The default configuration maps all relationship types starting with `contain`.
- All other relationship types in UCMDB are mapped to `dependency`.

The configuration that specifies which CIs are added as nodes in HPOM is done using node types. Node types are specified using an XML file. By default, the node types are `unix`, `nt` and `host`.

Each CI that is not contained within another CI is treated as a top-level CI. A CI hierarchy is created for each top-level CI and all its children are contained in this hierarchy.

The example in [Figure 5](#) on page 29 shows two service hierarchies with the following top-level CIs:

- Applications
- System Infrastructure

## Enriching CI Hierarchies with Mapping Rules

You enrich the normalized CI hierarchies by creating the following mappings:

- [Applying Service Mapping](#) on page 32
- [Applying Node Mapping](#) on page 34
- [Applying Attribute Mapping](#) on page 35
- [Assigning User Roles and Profiles](#) on page 38

### Applying Service Mapping

For all CIs that are added to HPOM as service, a service mapping is necessary. In UCMDB, CIs are of a specific CI type. In HPOM, services are of a specific service type. Service mappings are a set of rules that defines how to map CI types to service types.

In the example data shown in [Figure 5](#) on page 29, there are three CI types:

- `sqlserver`
- `servicegroup`
- `nt`

In the example, HPOM DMA uses service mapping rules to assign service types to CIs as follows:

- The MS SQL: `SqlServer 6.5` checks whether a CI is of type `sqlserver` and `dbversion` is `6.5`. For CIs that meet these criteria, they are assigned the service type `ucmdb_sqlserver65`.
- To all other CIs of type `sqlserver`, the MS SQL: `SqlServer` rule assigns the service type `ucmdb_sqlserver`.
- All CIs of type `service group` are assigned the service type `folder` by the `Default: ServiceGroup` rule.
- For all other CIs, the service type `ucmdb_<CI Type>` is assigned by the `Default:Default` rule.



▶ Service type definitions (STDs) are used to identify how CIs from UCMDb are to be handled when building services in HPOM on synchronization. If an STD for an imported CI is not available in HPOM, it cannot be displayed in Service Navigator. An error message is displayed explaining that STDs are missing.

HPOM DMA can automatically create STDs to suit non-matching CIs as they are imported into HPOM. For details, see [Creating Service Type Definitions Automatically](#) on page 108.

Figure 6 shows examples of service mapping rules.

### Figure 6 Service Mapping Rules

Rule: MS SQL: SqlServer 6.5

---

```
if
    the type of the CI equals the value "sqlserver"
    and
    the value of the attribute "database_dbversion" contains the value "6.5"
then
    set the Service Type Definition name of the service to the value "ucmdb_sqlserver65"
```

Rule: MS SQL: SqlServer

---

```
if
    the type of the CI equals the value "sqlserver"
then
    set the Service Type Definition name of the service to the value "ucmdb_sqlserver"
```

Rule: Default: ServiceGroup

---

```
if
    the type of the CI equals the value "servicegroup"
then
    set the Service Type Definition name of the service to the value "folder"
```

Rule: Default: Default

---

```
if
    always
then
    set the Service Type Definition name of the service to the concatenated value of the value "ucmdb_" and the type of the CI,
```

The second rule is not actually needed. The rule `Default:Default` produces the same result. If the `ucmdb_<CI Type>` pattern meets your needs, there is no need to write new rules. New rules are needed for specific mappings only. For example, when you add version information to your service type.

The order of rules is important because only one service type can be assigned to a service. The order of rules can be viewed in the HPOM DMA console:

### **Enrichment Summary → Service Mapping**

Rule order is established using the priority of the synchronization packages.

## Applying Node Mapping

All UCMDB CIs that are added to the HPOM node bank are assigned to the node group `CMDB`. Nodes that were previously included in the synchronization information from UCMDB, but are no longer present in the synchronization are moved from the `CMDB` node group to the `CMDB_Removed` node group. This cannot be changed.

Additionally, for all CIs that are added to HPOM node bank, a node mapping can be specified. Using these node mapping rules, nodes can be added to matching node groups in HPOM.



By default, HPOM DMA imports all the nodes discovered by UCMDB to node groups `CMDB` and `CMDB_Removed`. However, the nodes which already exist in user-defined node groups in HPOM are also moved to these default node groups. Unless you define node mapping rules to place particular nodes in specified node groups, nodes from UCMDB are always placed in the `CMDB` and `CMDB_Removed` node groups.

In this way, the node group assignment process is fully automated. This is especially helpful for environments containing many thousands of nodes arranged in, possibly, hundreds of node groups. In some environments, node assignment may be changing dynamically. In such environments, handling the assignments manually is no longer advantageous.

If a node is synchronized through HPOM DMA, its node group assignments are controlled by HPOM DMA. This avoids conflicts between manual and automated changes. It is not possible to let HPOM DMA decide whether a particular manual change should be overridden. Managing nodes is clearer and easier if a node is either controlled by HPOM DMA or manually.

If you do not want HPOM DMA to change the node group of an existing node, this node must be excluded from the TQL and cannot be managed by DMA at all.

For node mapping, the order is not important because a node can be added to many node groups.

In [Figure 5](#) on page 29, the nodes `kermit.example.com` and `piggy.example.com` are placed in the node groups: MSSQL and WINOSSPI-Windows. The node `gonzo.example.com` is placed only in the node group WINOSSPI-Windows.

[Figure 7](#) shows examples of node mapping rules.

### Figure 7 Node Mapping Rules

#### -Rule: MS SQL: SQL Server Nodes

---

```
if
    the value of the attribute "host_servertype" equals the value "sqlserver"
then
    place the node into the nodegroup named after the value "MSSQL"
```

#### -Rule: WinOS: Windows Nodes

---

```
if
    the type of the CI equals the value "nt"
    and
    the result of the expression "the value of the attribute "host_os" equals the value "Linux"" is false.
then
    place the node into the nodegroup named after the value "WINOSSPI-Windows"
```

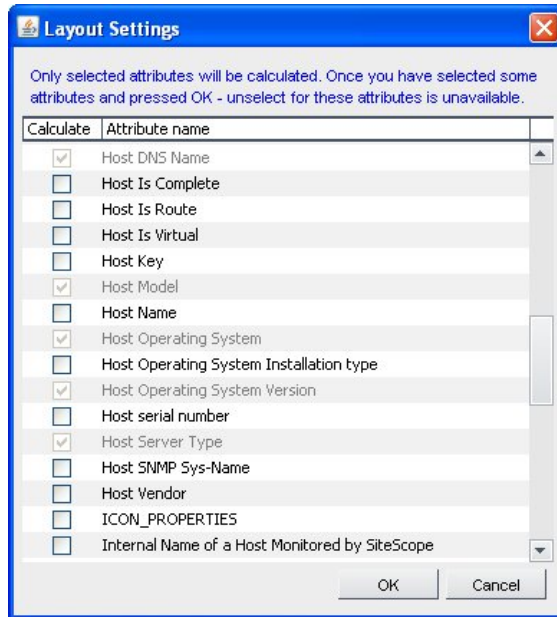
To view the rules in the HPOM DMA console, select:

**Enrichment Summary → Node Mapping**

## Applying Attribute Mapping

All attributes that are selected in the Advanced Layout Settings of the TQL query are available for HPOM. The Advanced Layout Settings are located under the Node Properties for the associated TQL query. An example is illustrated in [Figure 8](#).

**Figure 8 Advanced Layout Settings**



These UCMDB CI attributes are added to the internal CI hierarchies. Using attribute mapping, they can be changed or new attributes can be added.

Attribute mapping is useful for the following:

- Better matching of messages to services.
- Enriching HPOM messages with CI attributes
- Assigning attributes to existing service or node attributes (for example, display label, propagation and calculation rules, and node attributes).

For the examples, you do not need extra attribute mapping. The default attribute mapping maps some essential node attributes. For example, it sets specific node attributes (`ovo_osType`, `ovo_systemType`, `ovo_osVersion`) on CIs that are nodes. These attributes are required to correctly create the nodes in HPOM.

The order of rules is important if you set the same HPOM service or node attribute twice.

To view the rules in the HPOM DMA console, select:

**Enrichment Summary → Attribute Mapping**

You can manipulate it by changing the priority of the synchronization packages.

Figure 9 shows examples of attribute mapping rules.

**Figure 9 Attribute Mapping Rules**

**Rule: Default: Set node attributes for Windows NT 4.0 nodes**

if

```
the type of the CI equals the value "nt"  
and  
the value of the attribute "host_os" contains the value "Windows"  
and  
the value of the attribute "host_osversion" starts with the value "4.0"
```

then

```
assign the value "Windows_32" to the attribute "ovo_osType"  
assign the value "x86/x64 Compatible" to the attribute "ovo_systemType"  
assign the value "NT (4.0)" to the attribute "ovo_osVersion"
```

**Rule: Default: Set node attributes for Windows 2000 nodes**

if

```
the type of the CI equals the value "nt"  
and  
the value of the attribute "host_os" contains the value "Windows"  
and  
the value of the attribute "host_osversion" starts with the value "5.0"
```

then

```
assign the value "Windows_32" to the attribute "ovo_osType"  
assign the value "x86/x64 Compatible" to the attribute "ovo_systemType"  
assign the value "2000 (5.0)" to the attribute "ovo_osVersion"
```

## Assigning User Roles and Profiles

User Profile or User Role Assignment enables you to map a service to an HPOM user profile or role.

After synchronization, the service is assigned to all operators that are included in the specified HPOM user profile or role:

- **HPOM for UNIX**

User profiles are used for service assignment.

- **HPOM for Windows**

User roles are used for service assignment.

In the example, all MS SQL databases are assigned to the user profile DatabaseAdmin.



Differences between UNIX and Windows:

- **In HPOM for UNIX**

If no user profiles are assigned to a user, the user is not assigned any services or node groups.

All services are assigned to user profiles.

- **HPOM for Windows**

If no user roles are assigned to a user, the user sees all services, and node groups.

User roles can only get services assigned that are of type folder.

For details, see [Assigning User Profiles for Services on HPOM for UNIX or Linux](#) on page 109 and [Assigning User Roles for Services on HPOM for Windows](#) on page 115.

[Figure 10](#) shows examples of user profile mapping rules.

## Figure 10 User Profile Mapping Rules

### Rule: Assign MS SQL database to database admin user profile

```
if
    the type of the CI equals the value "sqlserver"
then
    assign the service to the user profile named after the value "DatabaseAdmin"
```

To view the rules in the HPOM DMA console, select:

**Enrichment Summary** → **User Mapping**

## Manipulating CI Hierarchies with Scripting

Scripting enables you to perform additional processing and customization during to the synchronization process before the mappings are applied and before and after the upload of nodes and services to HPOM.

Scripts can perform all customizations of the CI hierarchy that are not supported by enrichment, for example, grouping capabilities.

Additionally, there are use cases to trigger specific actions after the synchronization process is done. Typical use cases are:

- Start automatic policy deployment
- Send an email
- Send an `opcmsg` with details about the synchronization

One pre-mapping, one pre-upload, and one post-upload script can be associated with each synchronization package. These optional script files are located in the associated synchronization package directory. For details, see [Configuration Files](#) on page 231.

The order of execution of scripts can be arranged by changing the priority of synchronization packages.

Associating script files with synchronization packages simplifies the distribution of scripts and enables script development to be handled independently of the working environment. The execution of synchronization scripts follows the settings of the synchronization packages:

- Only scripts in active synchronization packages are executed.
- Scripts are executed in the order of the priority of the synchronization packages.



Script execution is potentially insecure. In particular, the use of `DMA.exec(...)` commands can cause damage to an installation. Therefore script access for editing is allowed on the file system level only. This ensures that only users with log-on credentials to the DMA host can edit scripts. This protects the scripts by the log-on security of the DMA host.

You can view scripts in the HPOM DMA console under **Script Summary**.



You can enable or disable synchronization package script execution from the **Content** page of the HPOM DMA console.



# Mapping HPOM Messages to Services

When HPOM receives a message, it must find out which service is impacted by the problem, and, as a result, color the service in accordance with the severity reported by the message.

The process by which HPOM DMA maps incoming messages to services is called **Smart Message Mapping** (SMM). During SMM, HPOM DMA looks for hints in a message that help to identify the service. Such hints include, for example, the service name, object, or application attribute of the message.

SMM first tries to find an exact service match by looking for a service ID that matches exactly the service name attribute of the message. The message is then sent to that service. (This ensures backward compatibility with existing SPI implementations.)

If SMM cannot find an exact match, it extracts hints from the service name, object, and application attributes of the message and compares these hints with the attributes of all services. When the best matching service is found, SMM replaces the existing service name in the message with the service ID of the best matching service and forwards the modified message to HPOM.

If SMM cannot find a matching service, it additionally considers the node attribute. If SMM finds a matching host, it forwards the message to that host. If SMM finds multiple matching services, it forward the message to the host and adds a custom message attribute to the message to If it cannot find any matches, it forwards the message unchanged (that is, SMM does not replace the service name attribute of the message). The message displays in HPOM but is not assigned to any service.

If a message does not contain a service name, SMM extracts hints from the object and application attributes, and additionally extracts the hostname from the node attribute. SMM then tries to identify a service by comparing the hints and the node name with the attributes of all services.



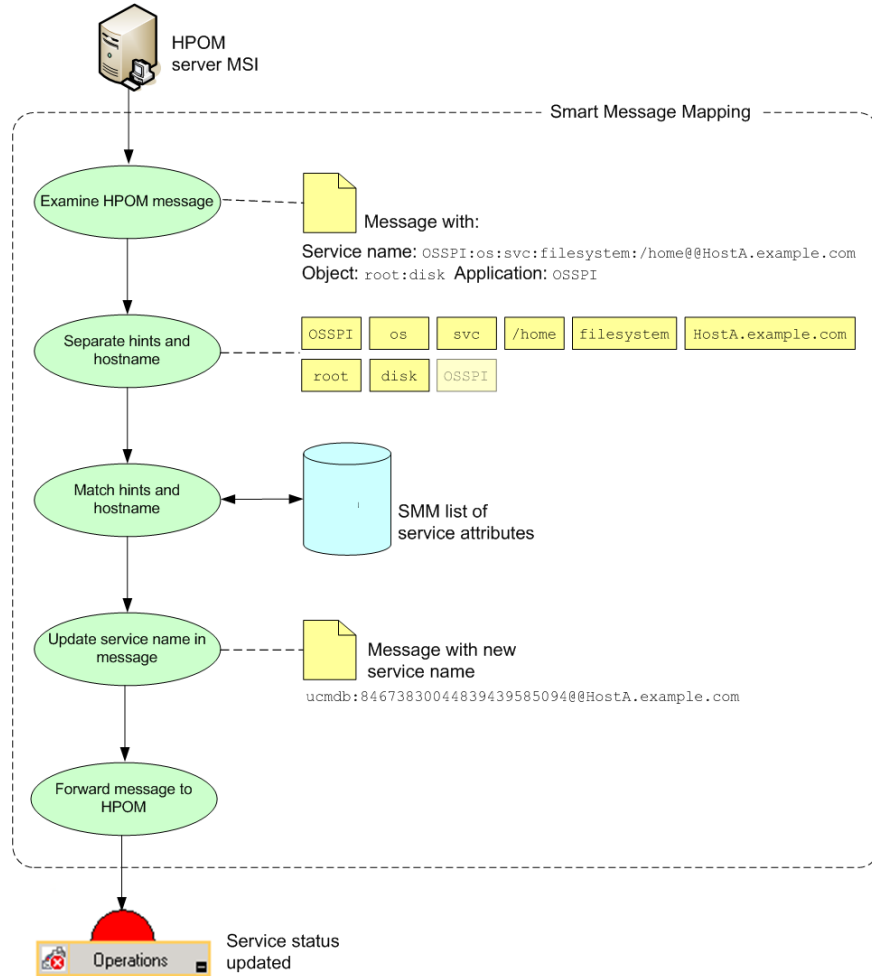
For SMM to work correctly, all hosted services must have the attribute `hosted_on` set to the fully qualified hostname. HPOM DMA sets this attribute through the following synchronization packages:

- DNS Mapping: Package containing mapping script for DNS names of hosts (pre-mapping script)
- Default: Default synchronization package (attribute mapping)

For information about virtual services, see [Mapping Messages to Virtual Services](#) on page 43.

Figure 11 on page 42 illustrates how the Smart Message Mapping process maps a message that contains a service name, object, and application attribute.

**Figure 11 Smart Message Mapping**



▶ In Figure 11, OSSPI appears twice in the list of hints. Because SMM ignores duplicate hints, the second occurrence of OSSPI is grayed out.

## Mapping Messages to Virtual Services

There are two basic types of services:

- Hosted Services

Hosted services are services that are located on a node. The node selected for service hosting is the node where the service actually resides.

- Virtual Services

Some services are abstractions, which do not actually exist on any node. Such services are virtual services, for example an email service, provided by an organization for use by users.

Virtual services do not have the `hosted_on` attribute set.

Use the following hints to send messages to virtual services:

- Service name, application, and object message attributes

To send a message to a virtual service (`mailservice`, in the following example), use a service name that does not include any hosting information, for example:

```
opcmsg a=oracle o=tablespace node=dbhost.example.com
service_id="mailservice" sev=warning msg_text="service slow"
```

- Application, object, and node message attributes

To send a message to a virtual service without using service names, use the application and object message attributes, for example:

```
opcmsg a=jee_application o=employee_portal
node=webhost.example.com sev=warning msg_text="service slow"
```

SMM will send this message to the virtual service that best matches the hints `jee_application` and `employee_portal`. However, if a service exists that matches one or more of these hints and is additionally hosted on `webhost.example.com`, SMM will send the message to that service.

## Separating Hints and Hostnames

A typical service name has the following format:

```
<some:service:id>@@<host>
```

<some:service:id> is an arbitrary string defined by the origin of the service and <host> is the fully qualified hostname of the node where the service resides.

Service names of messages addressed to virtual services do not contain any host information.

By default, SMM uses colons (:) to separate hints, and two at signs (@@) to identify the start of the hostname. (You can use regular expressions to configure SMM to recognize different separators, if a message's service name, object, and application use a different notation.)

SMM extracts hints from the following message attributes:

- Service name
- Object
- Application

In addition, SMM extracts the hostname from:

- Service name
- Node name (if service name is not set)

In the following example, SMM uses the default notation to extract hints and hostname from a message's service name, object, and application attributes:

```
Service name:  OSSPI:os:svc:filesystem:/home@@HostA.example.com
Hints:        OSSPI os svc filesystem /home
Hostname:                    HostA.example.com
Object:        root:disk
Hints:        root disk
Application:   OSSPI
Hints        OSSPI
```



By default, SMM considers the case of the hints.

For more information about configuring hint and hostname separators, case sensitivity, the update delay, and the polling interval for SMM, see [Configuring Smart Message Mapping](#) on page 134.

## Mapping HPOM Messages to Services Synchronized from UCMDB

With HPOM DMA, services are based on CIs that are uploaded from BAC or UCMDB. Service IDs are generated by the HPOM DMA synchronization process and are no longer governed by HPOM SPIs. By default, HPOM DMA service IDs have the following format:

```
ucmdb:<ci_uid>@@<host>
```

In contrast, messages generated by SPIs contain a SPI-generated service name, for example:

```
OSSPI:os:svc:filesystem:/home@@HostA.example.com
```

To direct HPOM messages generated by existing custom or SPI monitoring policies to the associated services synchronized from UCMDB, you can choose one or both of the following configuration options:

- Use Smart Message Mapping

With HPOM DMA, you can use Smart Message Mapping, which enables you to map messages to services, even if you do not know the exact service ID of the service or even if the message does not contain a service name.

For more information about Smart Message Mapping, see [Mapping HPOM Messages to Services](#) on page 41.

- Custom service ID generated by HPOM DMA

You can change the default service ID that HPOM DMA assigns to a service.

For more information, see [Customizing Service IDs](#) on page 46.

## Customizing Service IDs

When HPOM DMA synchronizes services from BAC or UCMDB, it applies the following default service ID:

```
ucmdb:<ci_uid>@@<host>
```

This service ID is different from the service name that is traditionally contained in HPOM messages. Therefore, without additional configuration, HPOM is not able to map messages generated by existing custom or SPI monitoring policies to services synchronized from UCMDB.

If you do not want to use Smart Message Mapping, you can use attribute mapping or scripting to customize the service ID that HPOM DMA assigns to services synchronized from UCMDB.

For detailed instructions, see [Customizing the ID of Services Synchronized from UCMDB](#) on page 143.

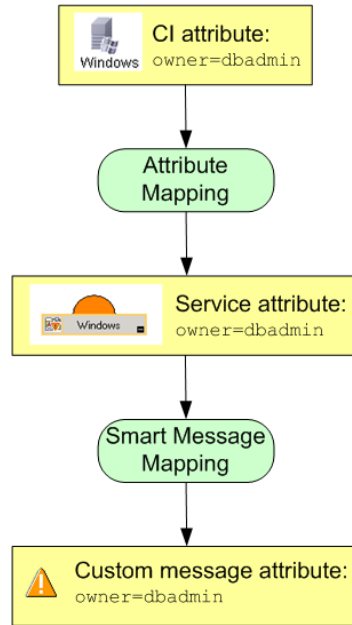
## Assigning Custom Message Attributes to Messages

In HPOM, custom message attributes (CMAs) are additional message attributes that the administrator configures for a message. CMAs may contain any information the administrator considers to be useful for evaluating or solving the problem reported by the message.

Smart Message Mapping (SMM) enables you to attach CI attributes as CMAs to HPOM messages. In HPOM, you can then look up CI information directly in the message instead of viewing the properties of services.

[Figure 12](#) on page 47 illustrates the process by which HPOM DMA assigns CMAs to messages. Before SMM can attach CI attributes to messages, the CI attributes must be mapped to service attributes using attribute mapping rules. When HPOM DMA receives a message, SMM finds the best matching service and assigns the message to that service. If SMM is configured for CMA mapping, SMM retrieves the specified service attribute and its corresponding value and copies this information into the message before forwarding the message to HPOM.

**Figure 12 Assigning CMAs to Messages**



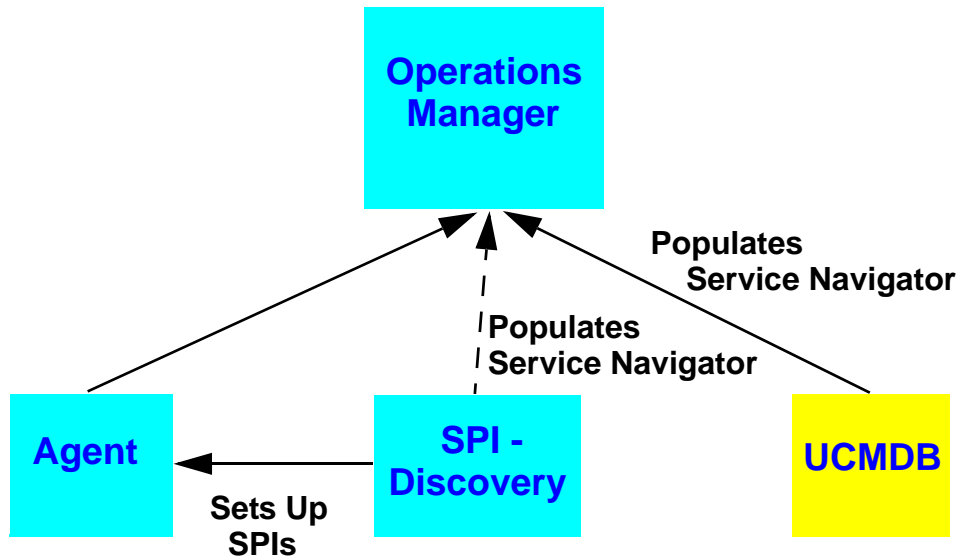
# Discovering Services

You can choose how to discover your services in Service Navigator. The two types of discovery sources are:

- SPI discovery
- UCMDB discovery

You are able to use UCMDB-based discovery as the source for displaying services in Service Navigator but continue to use SPIs for monitoring, as shown in Figure 13. If both UCMDB- and the SPI-based discoveries are activated, you see two service trees in Service Navigator. SPI-generated messages are used to identify status in the SPI-based discovery service tree. You are able to use a phased approach to switching to HPOM DMA. You initially import the services and nodes, and then you switch off the upload of the SPI discovery result. SPI monitoring continues to work as originally configured.

**Figure 13 Selecting the Discovery Source**



- - - ➔ Can be switched on or off selectively as required.



When you are satisfied that the service tree derived from UCMDB discovery is being correctly displayed, you can disable the service upload of the SPI discovery and delete the service tree generated from the SPI discovery. This avoids displaying two instances of the same service.



---

# 4 Preparing HPOM DMA

## Installation Distribution

HP Operations Manager Dependency Mapping Automation (HPOM DMA) requires the following three software components:

- HPOM for Windows, UNIX, or Linux installation
- HP Universal CMDB or HP Business Availability Center (BAC) installation
- HPOM DMA installation on the HPOM host system

You can arrange the software on your hardware as follows:

- The HPOM installation must be able to access UCMDB or BAC installations over the network. On Windows, the HPOM and UCMDB or BAC installations can be on the same host system, but this is not recommended because of performance considerations.
- HPOM DMA must be installed on the system hosting the HPOM management server system, with the exception of HPOM for UNIX installations on HP-UX 11.23 and HP-UX 11.31 PA-RISC 64-bit systems. For these installations, HPOM DMA must be installed on a proxy system running a Windows operating system.

# Product Prerequisites

This section specifies the hardware and software products you require before installing HPOM DMA.

## HP Operations Manager

For details of the product versions supported with HPOM DMA 8.20, see the support matrix at HP Software Support Online:

**<http://support.openview.hp.com/selfsolve/document/KM323488>**

Make sure one of the HP Operations Manager products listed in [Table 1](#) is installed.

**Table 1 HPOM Products**

<b>HPOM</b>	<b>OS and Version</b>	<b>Architecture</b>
HPOM 8.xx for HP-UX	<ul style="list-style-type: none"><li>• HP-UX 11.23 (11i v2 September 2003)</li><li>• HP-UX 11.23 PI (11i v2 September 2004)</li><li>• HP-UX 11.31 (11i v3)</li></ul>	Intel Itanium 64-bit systems
HPOM 8.xx for HP-UX	<ul style="list-style-type: none"><li>• HP-UX 11.23 PI (11i v2 September 2004)</li><li>• HP-UX 11.31 (11i v3) on PA-RISC</li></ul>	PA-RISC 64-bit systems (Remote access only using a proxy system running a Windows operating system.)
HPOM 9.xx for HP-UX	<ul style="list-style-type: none"><li>• HP-UX 11.31 (11i v3) on Intel Itanium</li></ul>	Intel Itanium 64-bit systems
HPOM 8.xx for Sun Solaris	<ul style="list-style-type: none"><li>• Sun Solaris 9, 10</li></ul>	Sun Microsystems

**Table 1 HPOM Products**

<b>HPOM</b>	<b>OS and Version</b>	<b>Architecture</b>
HPOM 9.xx on Linux	<ul style="list-style-type: none"> <li>Red Hat Enterprise Linux 5.2, 5.3, 5.4, 5.5, 5.6</li> </ul>	64-bit systems
HPOM 8.1x for Windows	<ul style="list-style-type: none"> <li>Windows Server 2003 SP1, SP2, or R2 (32-bit) (Standard Edition, Enterprise Edition, Datacenter Edition)</li> <li>Windows Server 2008 (32-bit)</li> </ul>	32-bit systems
HPOM 9.00 for Windows	<ul style="list-style-type: none"> <li>Windows Server 2008 R2</li> </ul>	64-bit systems

**Table 2 High-Availability Software Supported with HPOM DMA**

<b>Product</b>	<b>Version</b>	<b>Operating System</b>
HP Serviceguard	11.17	HP-UX 11.23, 11.31
Sun Microsystems Cluster	3.1	Solaris 9, Solaris 10
Veritas Cluster Server	5.0	HP-UX 11.23, 11.31 Solaris 9, Solaris 10
	5.1	Red Hat Enterprise Linux 5.2, 5.3, 5.4, 5.5, 5.6
Red Hat Cluster Suite	5	Red Hat Enterprise Linux 5.2, 5.3, 5.4, 5.5
Microsoft Cluster Server	2003 2008	Windows Server 2003 SP1, SP2, or R2 (32-bit) (Standard Edition, Enterprise Edition, Datacenter Edition) Windows Server 2008 (32-bit) Windows Server 2008 R2

## Proxy System for HPOM for UNIX on PA-RISC Systems

The proxy system hosting HPOM DMA must be running the following 32-bit operating system:

- Windows Server 2003 (Standard Edition, Enterprise Edition, Datacenter Edition) (including SP1, SP2, R2)

The following high-availability software is supported with HPOM DMA:

- Microsoft Cluster Server 2003 (including SP1, SP2, R2)

## HP Universal CMDB or HP Business Availability Center

For details of the product versions supported with HPOM DMA 8.20, see the support matrix at HP Software Support Online:

**<http://support.openview.hp.com/selfsolve/document/KM323488>**

Make sure one of the following products is installed:

Product	Version
HP Business Availability Center	7.5x or 8.0x
HP Universal CMDB	<p data-bbox="564 321 1106 355"><b>Advanced</b></p> <p data-bbox="564 361 1078 486">This edition enables discovery of all components at your site and the ability to federate with other data sources and reconcile CIs.</p> <p data-bbox="564 494 692 529"><b>Standard</b></p> <p data-bbox="564 534 1006 598">This edition enables discovery of the infrastructure and network.</p> <p data-bbox="564 607 628 642"><b>Free</b></p> <p data-bbox="564 647 1106 841">HP Universal CMDB includes the complete class model (all CI types) and all packages. (You populate UCMDB either manually or using integration.) HP Universal CMDB is provided without the discovery or federation features.</p> <p data-bbox="149 859 1085 1024">Select the Universal CMDB version that most suits your needs. To make the most of your HPOM DMA implementation, use the <b>Advanced</b> version. This version enables you to use all of the built-in features that are part of the HPOM DMA product (for example, synchronization of database-related data using the synchronization packages).</p>



The Operations Manager HTTPS Agent for Windows is assigned free ports at random during start up. This may conflict with the ports required by a UCMDB or BAC installation located on the same Windows System.

To avoid this conflict, start up UCMDB or BAC application before starting up the HTTPS Agent on the Windows System.

## HPOM Patches

The HPOM patches required for HPOM DMA are listed in the *HPOM DMA Release Notes*. You can download the latest version of the *HPOM DMA Release Notes* from the following web site:

**<http://h20230.www2.hp.com/selfsolve/manuals>**

## HPOM DNS Requirements

You must configure the HPOM host system to use a domain name server (DNS) that can resolve host names and IP addresses correctly.

To test this, execute `nslookup <hostname>` at a command prompt on the management server. The command must return a fully qualified host name and IP address.

DNS must be set up so that the HPOM host system can resolve all hosts that are synchronized from UCMDB.

## HPOM for UNIX or Linux Agents

If you want to import nodes of a particular operating system type, the agent software for that platform must be available on the HPOM for UNIX or Linux management server. If it is not included in the HPOM for UNIX or Linux media kit, download it from the HPOM for UNIX or Linux SSO web site:

**<http://support.openview.hp.com/selfsolve/patches>**



# Microsoft Visual C++ 2005 SP1 Redistributable Package

Microsoft Visual C++ 2005 SP1 Redistributable Package must be installed on every HPOM DMA for Windows system. This affects the HPOM for Windows host system as well as the proxy system for HPOM for UNIX PA-RISC system.

## Hardware Requirements for HPOM DMA

Extra hardware requirements for installing HPOM DMA on the HPOM host system:

- 700 MB free disk space (maximum)
- 1 GB Additional RAM (during synchronization)

## Temporary Disk Space Requirements During Installation

The HPOM DMA product installation requires free disk space in a temporary directory on the HPOM host system.

If the product installation cannot complete due to insufficient disk space in the temporary directory, then use an environment variable to point the temporary directory to another directory with more space available and retry the installation:

- UNIX and Linux installations

The temporary directory is `/tmp`.

By default, if `/tmp` does not exist or has insufficient disk space, the installer attempts to use `$HOME` as the temporary space.

You can define the environment variable `IATEMPDIR` to specify an alternative temporary location.

- Windows installations

The temporary directory is defined as `%TEMP%`.

## Browser Requirements for HPOM DMA

For details of the browser versions supported with HPOM DMA 8.20, see the support matrix at HP Software Support Online:

**<http://support.openview.hp.com/selfsolve/document/KM323488>**

## VMware Workstation Installations

HPOM DMA can be installed on a virtual system running in VMware Workstation. The same prerequisites must be met as for an installation on a physical system and support is only possible for problems reproducible on a physical system installation.

# Additional Prerequisites and Configurations

## Enabling HPOM DMA to Access UCMDB or BAC

HPOM DMA requires the credentials of the `admin` user account or of an integration user account to access UCMDB or BAC.



User accounts that have the `Administrator` role assigned do not provide sufficient privileges for HPOM DMA to access UCMDB or BAC.

Use the following procedure to create an integration user account in UCMDB or BAC:

- 1 Start the UCMDB or BAC console, enter the following:  
**`http://<ucmdb_server>:8080/jmx-console/`**
- 2 Log in as user with administrative privileges.
- 3 UCMDB 7 and 8: In the `MAM` section, click `service=MAM Security Services`.  
UCMDB 9: In the UCMDB section, click `service=MAM Security Services`.
- 4 Below `Create integration user`, enter, for example, the following information to create an integration user:

<code>customerID</code>	<b>1</b>
<code>name</code>	<b>myIntegUser</b>
<code>password</code>	<b>myPassword</b>
<code>dataStoreOrigin</code>	<b>hpdma</b>

- 5 Click **Invoke**.



Use the same web page to change the password of an integration user account or to delete integration user accounts.

## Installing IIS after the .NET Framework on Windows HPOM DMA Systems

HPOM DMA uses Microsoft Active Server Pages .NET (ASP .NET) to connect to the HP Operations Manager for Windows server. If you install the .NET framework on a system that already has Microsoft Internet Information Services (IIS) installed, IIS is automatically configured to handle ASP .NET requests.

However, if you install IIS after the .NET framework, you must manually register ASP .NET with IIS by executing the following command in a Command Prompt window:

```
%SystemRoot%\Microsoft.NET\Framework\v2.0.50727\  
aspnet_regiis -i
```

## Enabling Licensing on 64-bit Windows HPOM DMA Systems

Before installing HPOM DMA on the 64-bit version of HPOM for Windows, add the SYSTEM user to the licensing file `LicFile.txt` with full file access permissions:

- 1 Locate the following file in Windows Explorer:  
    `%OvShareDir%\server\OprEl\AutoPass\LicFile.txt`
- 2 Right-click the file and select **Properties**.
- 3 Open the **Security** tab.
- 4 Add the SYSTEM user to the list of users and assign full control to this user.
- 5 Click **OK** to save your changes and close the Properties dialog box.

## Setting Up Discovery Data

HPOM DMA cannot work without specific UCMDB or BAC attributes. For example, the `Host DNS Name` attribute must be included so that nodes can be created and the `hosted_on` attribute can be set. Without this, Smart Message Mapping does not work. Make sure that discovery is set up correctly.

Information on how to set up discovery can be found in the online help under:

- *UCMDB 7 and 8*  
**Help → UCMDB Help → Main Topics → Discovery**
- *UCMDB 9*  
**Help → UCMDB Help → Data Flow Management**
- *BAC*  
**Help → Documentation Library → Main Topics → Discovery**

## Enabling UI Launch from HPOM to BAC or UCMDB

To use BAC/UCMDB UI Launch from HPOM for Windows, you must install the Sun Java Plug-in, version 1.6.0 or higher, with an integration into your web browser.

To use the HPOM for UNIX or Linux Java console on Windows, you must install a Java SE Runtime Environment (JRE). It is recommended that you configure HPOM for UNIX or Linux tools to use Internet Explorer when accessing URLs.

The latest JRE can be downloaded from the following Sun Microsystems web site:

**<http://www.java.com>**



# 5 Installing HPOM DMA

The HPOM DMA installation installs the software onto the HPOM host system. This chapter guides you through all the required steps. This process should take approximately 60 minutes to complete.



Read the rest of this guide before you start the installation wizard to plan your decisions and gather the information that you need.

## Installing on Clusters

HPOM DMA is cluster aware. It has the capability to switch over automatically to an alternative cluster system (failover) under the same conditions as HPOM. HPOM DMA belongs to the same XPL High Availability (HA) resource group as HPOM.

Installing HPOM DMA on a system participating in a cluster is supported on the active node only. An attempt to install HPOM DMA on a non-active node is rejected by the installer.

HPOM DMA must be individually installed on each node participating in the cluster. For each node in the cluster, make it the active node and install HPOM DMA on that node, following the instructions given in this chapter. Proceed with the next node in the cluster until HPOM DMA is installed on all cluster nodes.

For further details on HPOM running in cluster environments, see the HPOM documentation.

For cluster-related information (for example, how to switch a system move from passive to active mode), see your clustering software documentation.

For enabling Smart Message Mapping in cluster environments, see [Configuring Smart Message Mapping in Cluster Environments](#) on page 71.

# Applications Stopped and Restarted During Installation

This section describes applications that are stopped and restarted by the HPOM DMA application installation process. The restarts are performed for install, uninstall, and repair.

## Applications Stopped and Restarted on HPOM for UNIX or Linux

HPOM DMA stops and restarts the following applications:

- Cluster monitoring on cluster systems
- Local HPOM agent
- HPOM for UNIX or Linux
- All `ovc` applications including the OV Control Daemon (`ovcd`)

The restarts are performed for install, uninstall and repair.

## Applications Stopped and Restarted on HPOM for Windows

HPOM DMA stops and restarts the following applications:

- OV Auto Discovery
- `OvTomcatB` and any `ovc` applications that requires `OvTomcatB`

# Repairing an HPOM DMA Installation

If your HPOM DMA installation is damaged, execute the installation procedure again and select the Repair option. The damaged files are replaced and HPOM DMA should be operational again. Your configuration files are not affected by the repair.



# Loading the Installation Media on UNIX or Linux

To prepare for the HPOM DMA software installation from the product media, follow these steps:

- 1 Insert the product media into an appropriate DVD-ROM drive.
- 2 Create a directory to mount the drive:

```
mkdir /<mount_point>
```

Example:

```
mkdir /dvdrom
```

- 3 Mount the DVD-ROM drive:

— HPOM for UNIX:

```
mount -r -F cdfs /dev/<dvdrom_drive_name> /<mount_point>
```

Example:

For a local DVD-ROM, you can execute:

```
mount -r -F cdfs /dev/dsk/c0t2d0 /dvdrom
```

On HP-UX systems, you can also run SAM and mount the CD-ROM to a specific path in the Disks and File Systems window.

— HPOM on Linux:

```
mount -o ro /dev/<dvdrom_drive_name> /<mount_point>
```

Example:

For a local DVD-ROM, you can execute:

```
mount -o -ro /dev/dsk/c0t2d0 /dvdrom
```

# Installing HPOM DMA

To install HP Operations Manager Dependency Mapping Automation, follow these steps:

1 If you are upgrading from HPOM DMA 8.10 to 8.20, follow the instructions in [Chapter 8, Upgrading HPOM DMA](#) on page 63.

2 Delete all shared files installed with HPOM:

- a Close all open applications.
- b Delete all files in the following directory:

```
<SharedDir>/server/conf/dma/
```

The files in this directory are installed with HPOM and must be replaced by the newer HPOM DMA 8.20 versions of the files. If you do not delete the files, the installation of HPOM DMA 8.20 will not be able to replace them.

3 Start the application installer:

- *HP-UX, Solaris, and Linux*

```
<dvd-mountpoint>/hpdma_setup.sh
```

➤ For installation on PA-RISC systems, see [Installing HPOM DMA for HPOM for UNIX on PA-RISC Systems](#).

- *Windows*

Insert the product media disk into the DVD drive of the system where HPOM for Windows is installed.

If Autorun is enabled, the installation starts automatically.

If Autorun is disabled, do one of the following:

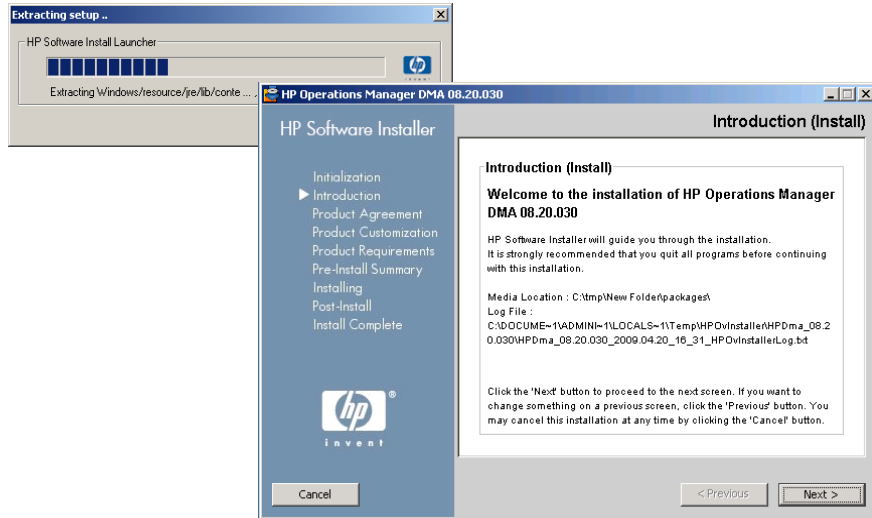
- Execute the following in a command window:

```
<dvd_drive>:\hpdma_setup.bat
```

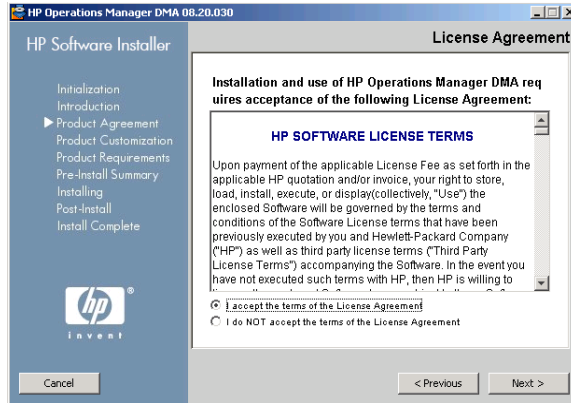
- Execute the `hpdma_setup.bat` executable file from an Explorer window.

Follow the on-screen instructions and progress through the installation process using the **Next** and **Install** buttons.

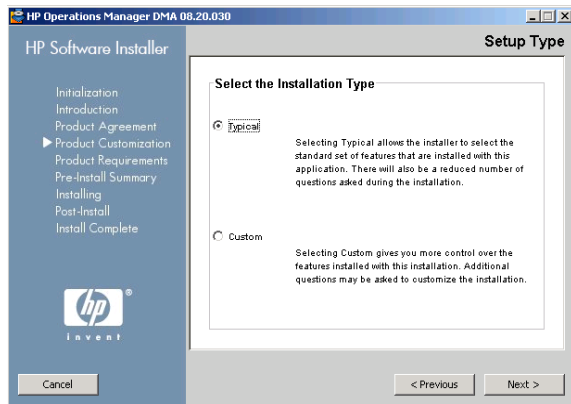
- ▶ The HPOM DMA installation location is dependent on the HPOM installation location. The HP Software Installer checks for this location. It is not possible to select an alternative for HPOM DMA.



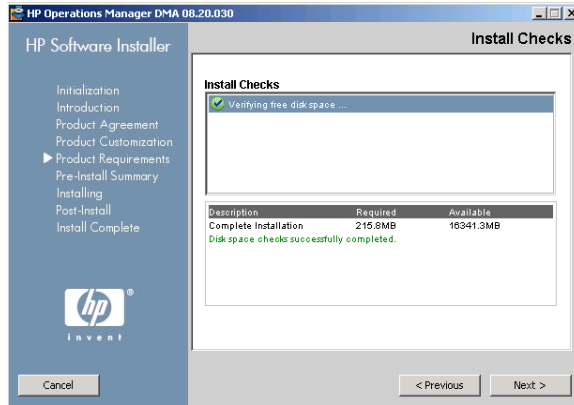
- 4 Read and accept the Licence agreement and click **Next**.



- 5 Select the **Typical** installation type and click **Next**.  
The pre-install checks, including available disk space, are executed.

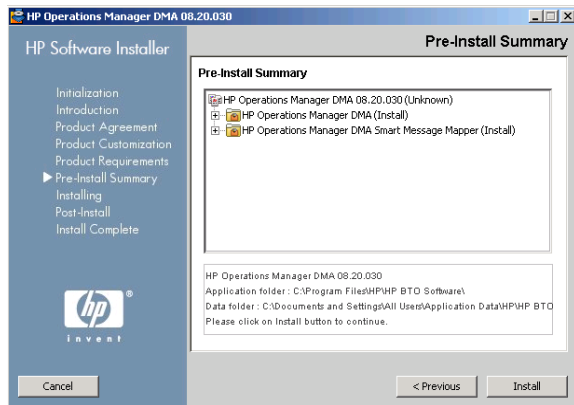


- 6 If they complete successfully, click **Next**.



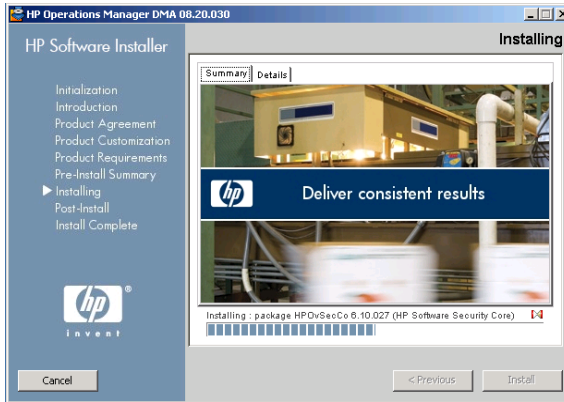
The pre-install summary lists the components to be installed or updated.

- 7 Click **Next**.



The HPOM DMA installation starts installing files onto the host system. Overall progress is displayed along with the name of the package being currently installed.

The last stage in the installation creates the HPOM DMA uninstaller.

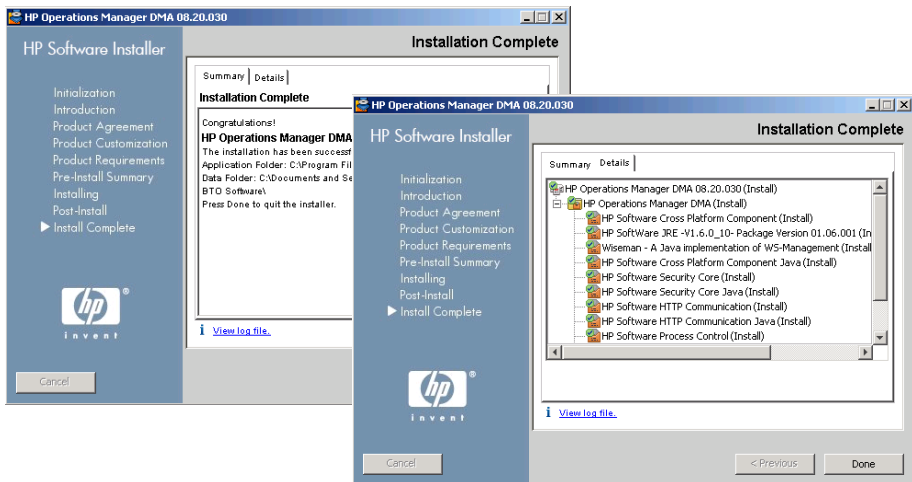


After the installation process is finished, the Installation Complete window opens showing a summary of the installation paths used.

You can also access the installation log file from the link in this window and open it in a web browser.

The installed packages can be seen from the Details tab.

- 8 Click **Done** to close the installation program.



# Configuring Smart Message Mapping in Cluster Environments

If you want to use Smart Message Mapping in cluster environments, you must make some configuration changes in the HPOM cluster configuration file.

## Configuring HPOM for UNIX Clusters Environments

To configure a cluster node for Smart Message Mapping, follow these steps:

- 1 Open the `ov-server.cntl` file for editing on the selected cluster node:

```
/etc/cmcluster/ov-server/ov-server.cntl
```

- 2 Add the following function after the existing `start_services` function:

```
function restart_dmamsg
{
    /opt/OV/bin/ovc -stop dmamsg
    /opt/OV/bin/ovc -start dmamsg
    print "dmamsg restarted" >> $0.log }

```

- 3 Search for the following code section

```
if [[ $1 = "start" ]]
then
    print "\n\t##### Node \"$(hostname)\": Starting
package at $(date) #####"
    activate_volume_group
    check_and_mount
    add_ip_address
    get_ownership_dtc
    customer_defined_run_cmds
    start_services
    Check exit value
    if (( $exit_value == 1 ))

```

- 4 Add the **restart\_dmamsg** entry as shown in the following extract:

```
if [[ $1 = "start" ]]
then
    print "\n\t##### Node \"$(hostname)\": Starting
package at $(date) #####"
    activate_volume_group
    check_and_mount
    add_ip_address
    get_ownership_dtc

```

```

        customer_defined_run_cmds
        start_services
        restart_dmamsg
    Check exit value
        if (( $exit_value == 1 ))

```

- 5 Save and close the file.
- 6 Repeat [step 1](#) to [step 5](#) for all nodes in the cluster.
- 7 Restart the cluster application.

To run Smart Message Mapping, you must:

- Enable Server-based Message Stream Interface (Server MSI).
- Start the Smart Message Mapping component.

For information on how to run Smart Message Mapping, see [Configuring Smart Message Mapping](#) on page 134.

## Configuring HPOM on Linux Cluster Environments

To configure a cluster node for Smart Message Mapping, follow these steps:

- 1 Open the `ha_start_ovserver` file for editing on the selected cluster node:

```

/opt/OV/bin/OpC/Utils/ha/ha_start_ovserver

```

- 2 Add the following lines of code at the end, just before `exit $_ret`:

```

if [ -f ${OV_BIN_DIR}/dmauser.sh ]
then
    ${OV_BIN_DIR}/ovc -restart dmamsg
fi

```

- 3 Save and close the file.
- 4 Repeat [step 1](#) and [step 2](#) for all nodes in the cluster.
- 5 Restart the cluster application.

To run Smart Message Mapping, you must:

- Enable Server-based Message Stream Interface (Server MSI).
- Start the Smart Message Mapping component.

For information on how to run Smart Message Mapping, see [Configuring Smart Message Mapping](#) on page 134.



## Starting the HPOM DMA Console

To start the HPOM DMA console, do one of the following:

- *Windows installations only.* Double-click the desktop icon.
- *Web browser.* Enter the following location:  
**`http://<Remote_HPOM_DMA_System>:8081/hpdma`**

## Further Essential Installation and Configuration Steps

To complete the HPOM DMA installation and configuration on the HPOM and UCMDB or BAC host systems, continue with the instructions described in [Configuring HPOM DMA](#) on page 91.



---

## 6 Installing HPOM DMA for HPOM for UNIX on PA-RISC Systems

HPOM DMA is not supported on HPOM host systems that run on a PA-RISC system. If you have such an HPOM installation, it is possible to install and configure HPOM DMA on an additional Windows system and remotely connect to your HPOM host system.

You must complete the following tasks:

- 1 Install the Smart Message Mapper on the PA-RISC HPOM host system.  
For detailed instructions, see [Installing on the PA-RISC HPOM Host System](#) on page 78.
- 2 Complete post-installation steps on the PA-RISC HPOM host system.  
For detailed instructions, see [Post-Installation Steps on the PA-RISC Host System](#) on page 85.
- 3 Install the HPOM DMA product software without the Smart Message Mapper on the remote HPOM DMA Windows host system.  
For detailed instructions, see [Installing on the HPOM DMA Windows Host System](#) on page 80.
- 4 Complete post-installation steps on the remote HPOM DMA Windows host system.  
For detailed instructions, see [Post-Installation Steps on the Windows Host System](#) on page 88.

This chapter guides you through all the required steps. These steps should take approximately 90 minutes to complete.



Before you start the installation wizard, read the rest of this guide to plan your decisions and gather the information that you need.

## Installing on Clusters

HPOM DMA is cluster aware. It has the capability to switch over automatically to an alternative cluster system (failover) under the same conditions as HPOM. HPOM DMA belongs to the same XPL High Availability (HA) resource group as HPOM.

For further details on HPOM running in cluster environments, see the HPOM documentation.

For cluster-related information, for example, how to switch a system move from passive to active mode, see your clustering software documentation.

## Applications Stopped and Restarted During Installation

HPOM DMA stops and restarts the following applications:

- Cluster monitoring on cluster systems
- Local HPOM agent
- HPOM for UNIX
- All `ovc` applications including the OV Control Daemon (`ovcd`)

The restarts are performed for install, uninstall and repair.

## Repairing an HPOM DMA Installation

If your HPOM DMA installation is damaged, execute the installation procedure again and select the **Repair** option. The damaged files are replaced and HPOM DMA should be operational again. Your configuration files are not affected by the repair.



The repair option does not work on HPOM DMA Windows host systems.

If you need to repair your HPOM DMA installation, follow these steps:

- 1 Back up your system data and any extensions and customizations that you have made.
- 2 Uninstall HPOM DMA using the installer application as described in [Uninstalling HPOM DMA](#) on page 203. Do *not* execute the post-uninstall cleanup steps on page [page 206](#).
- 3 Reinstall HPOM DMA.
- 4 Restore any extensions and customizations.

Alternatively, restore the system from a previous backup.

## Loading the Installation Media

To prepare for the HPOM DMA software installation from the product media, follow the steps:

- 1 Insert the product media into an appropriate DVD-ROM drive.
- 2 Create a directory to mount the drive:

```
mkdir /<mount_point>
```

Example:

```
mkdir /dvdrom
```

- 3 Mount the DVD-ROM drive:

```
mount -r -F cdfs /dev/<dvdrom_drive_name> /<mount_point>
```

Example:

For a local DVD-ROM, you can execute:

```
mount -r -F cdfs /dev/dsk/c0t2d0 /dvdrom
```

You can also run SAM and mount the CD-ROM to a specific path in the Disks and File Systems window.

## Installing on the PA-RISC HPOM Host System

To install the HPOM DMA Smart Message Mapper component on the PA-RISC HPOM for UNIX host system, follow these steps:

- 1 Enter the following command to start the installation:

```
<dvd-mountpoint>/hpdma_setup.sh
```

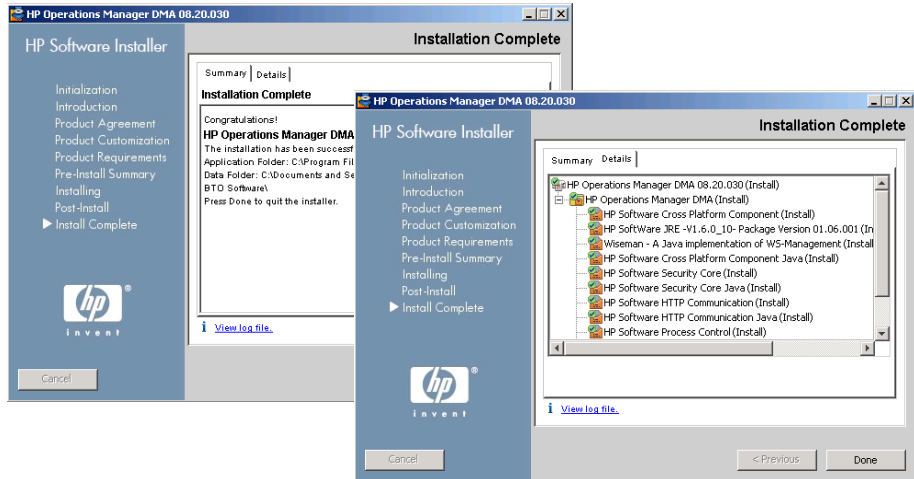
- 2 Follow the on-screen instructions and progress through the installation process using the **Next** and **Install** buttons.

After the installation process is finished, the Installation Complete window opens showing a summary of the installation paths used.

You can also access the installation log file from the link in this window and open it in a web browser.

The installed packages can be seen from the Details tab.

- 3 Click **Done** to close the installation program.



- ▶ PA-RISC HPOM for UNIX host systems do not need an HPOM DMA licence. The HPOM DMA installation on the selected Windows host system requires a valid licence. For further details, see [Chapter 10, Licensing](#).

# Installing on the HPOM DMA Windows Host System

- ▶ The system selected to be the proxy system to host HPOM DMA must not be a system where HPOM for Windows is installed.

To install HP Operations Manager Dependency Mapping Automation on the remote HPOM DMA Windows host system, follow these steps:

- ▶ The HPOM DMA installation on the selected remote HPOM DMA Windows host system requires a valid licence. For further details, see [Chapter 10, Licensing](#).

PA-RISC HPOM host systems do not need HPOM DMA licences.

- 1 Start the application installer as follows:
  - a Close all open applications.
  - b Insert the product media disk into the DVD drive of the HPOM DMA Windows host system.

If Autorun is enabled, the installation starts automatically.

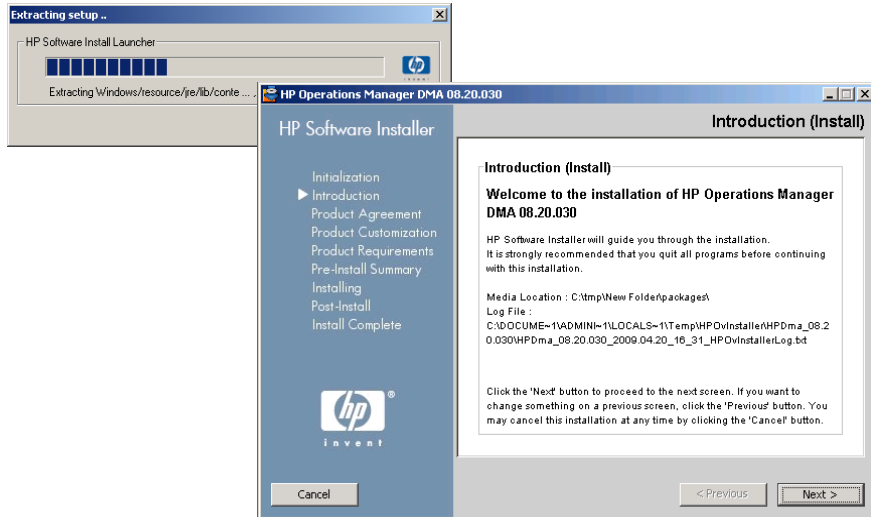
- c If Autorun is disabled, do one of the following:
  - Execute the following in a command window:

```
<dvd_drive>:\hpdma_setup.bat
```
  - Execute the `hpdma_setup.bat` executable file from an Explorer window.

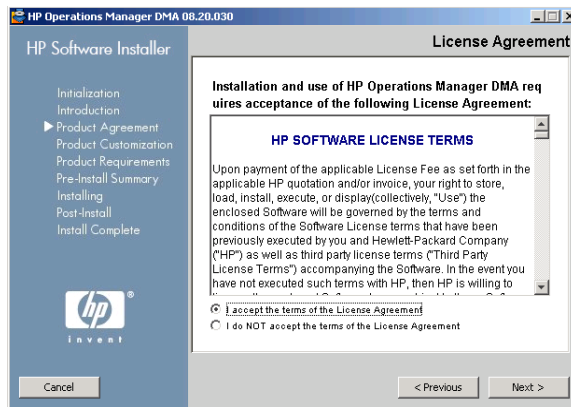
Follow the on-screen instructions and progress through the installation process using the **Next** and **Install** buttons.

- ▶ The HPOM DMA installation location is dependent on the HPOM installation location. The HP Software Installer checks for this location and it is not possible to select an alternative for HPOM DMA.

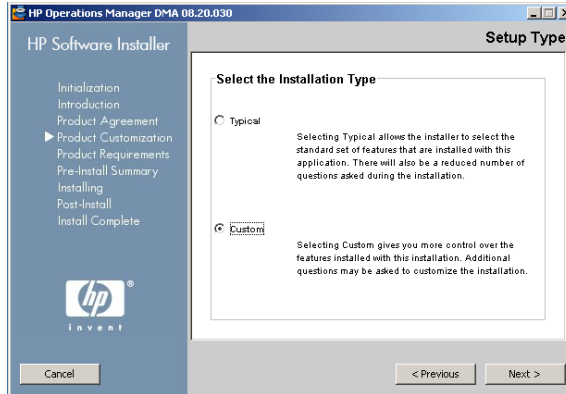




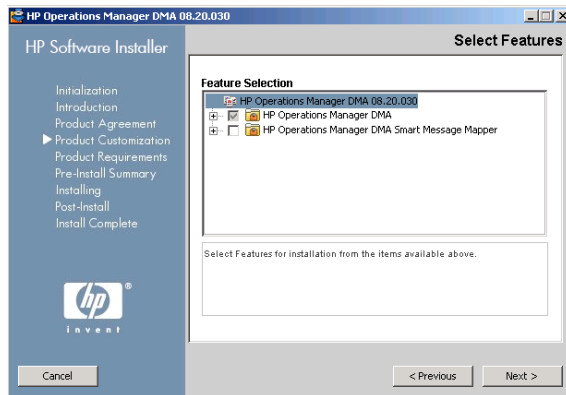
2 Read and accept the Licence agreement and click **Next**.



- 3 Select the **Custom** installation type and click **Next**.

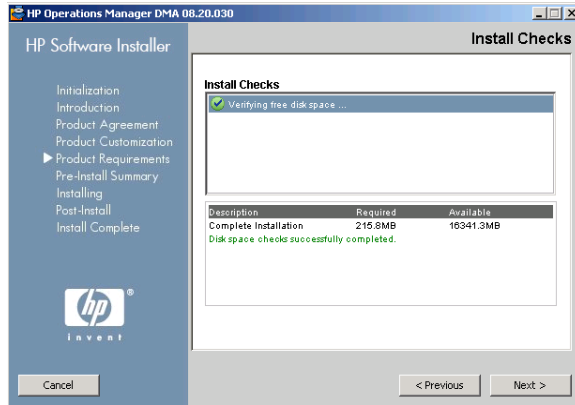


- 4 Clear the HP Operations Manager Smart Message Mapper option and click **Next**.



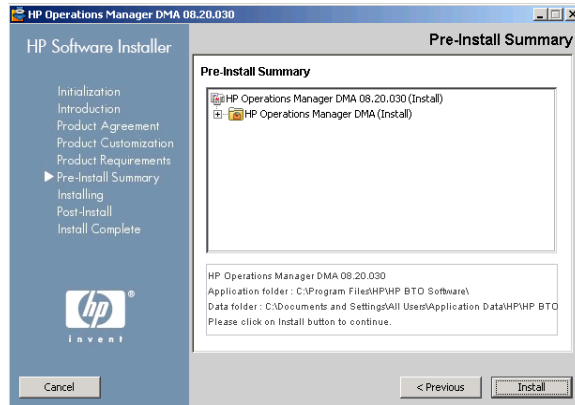
The pre-install checks, including available disk space, are executed.

- 5 If they complete successfully, click **Next**.



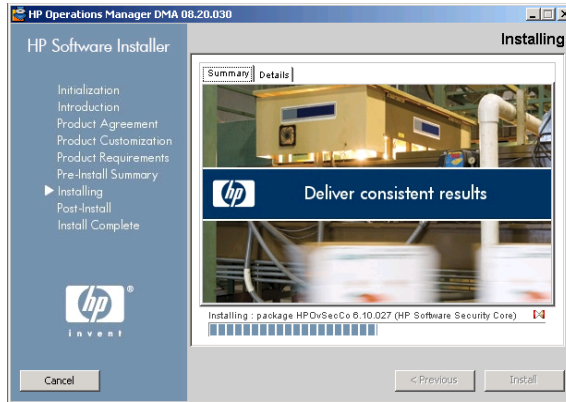
The pre-install summary lists the components to be installed or updated.

- 6 Click **Next**.



The HPOM DMA installation starts installing files onto the host system. Overall progress is displayed along with the name of the package being currently installed.

The last stage in the installation creates the HPOM DMA uninstaller.

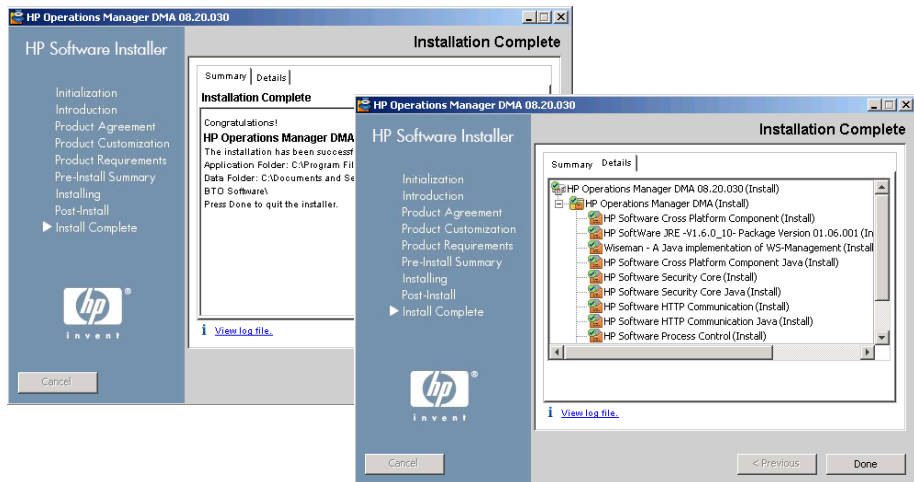


After the installation process is finished, the Installation Complete window opens showing a summary of the installation paths used.

You can also access the installation log file from the link in this window and open it in a web browser.

The installed packages can be seen from the Details tab.

- 7 Click **Done** to close the installation program.



# Post-Installation Steps on the PA-RISC Host System

To complete the post-installation steps on the PA-RISC HPOM for UNIX host system, execute the following steps:

- 1 Copy the `DefaultSyncTask.settings` file from the Windows host system to the equivalent location on the PA-RISC HPOM system:

— From:

```
<SharedDir>\server\conf\dma\DefaultSyncTask.settings
```

— To:

```
/var/opt/OV/shared/server/conf/dma/
```

The Windows copy of the file overwrites the default version on the PA-RISC HPOM system.

- 2 Copy the `<InstallDir>\misc\dma\DmaUploadsOmU.tar` file from the Windows host system to a temporary location on the PA-RISC HPOM system (for example, `/tmp`).

The `DmaUploadsOmU.tar` file contains the default root-service, calculation and propagation rules, service type definitions, and the node group and policies for HPOM DMA.

- 3 Untar the `DmaUploadsOmU.tar` file which you copied from the HPOM DMA Windows host system.

▶ `/opt/OV/misc/dma/ReadMe.txt` contains sample commands for the following tasks.

If you make the `/opt/OV/misc/dma/ReadMe.txt` file executable and run it, the post-installation steps are done for you automatically:

```
chmod 750 /opt/OV/misc/dma/ReadMe.txt
sh /opt/OV/misc/dma/ReadMe.txt
```

- 4 Load the default root-service, calculation and propagation rules for HPOM DMA into HPOM for UNIX with the command:

```
/bin/opcservice -add /opt/OV/misc/dma/
default_calcprop.xml
```

- 5 Load the service type definitions into HPOM for UNIX with the commands:

```
/opt/OV/bin/ServiceTypeDefinitionCLI -o -a /opt/OV/misc/dma/default_std.xml
```

```
/opt/OV/bin/ServiceTypeDefinitionCLI -o -a /opt/OV/misc/dma/eum_std.xml
```

- 6 Load the default node group and policies into HPOM for UNIX:

- **Node Groups**

- a Go to the `/tmp` directory:

```
cd /tmp
```

- b Untar the `defaultNodeGroup.tar` package:

```
/usr/bin/tar xf /opt/OV/misc/dma/defaultNodeGroup.tar
```

- c Upload the default node group:

```
/opt/OV/bin/OpC/opccfgupld -add -ascii /tmp/Sonata
```

- d Clean up the temporary files:

```
rm -r /tmp/Sonata
```

- **Policies**

- a Go to the `/tmp` directory:

```
cd /tmp
```

- b Untar the `OmDmaTemplates.tar` package:

```
/usr/bin/tar xf /opt/OV/misc/dma/OmDmaTemplates.tar
```

- c Upload the default policies:

```
/opt/OV/bin/OpC/opccfgupld -add -ascii /tmp/OmDmaTemplates
```

- d Clean up the temporary files:

```
rm -r /tmp/OmDmaTemplates
```

- 7 HPOM DMA delivers policies for self monitoring. To find out how to assign and deploy the OM DMA policy group, see [Assigning the OM DMA Policy Group](#) on page 108 and [Deploying the OM DMA Policy Group](#) on page 108.

However, the HPOM DMA synchronization log does not run on the HPOM management server, but on the HPOM DMA Windows host system, and specific deployment is needed for this policy.

To deploy the HPOM DMA Synchronization Log policy.

- a Change specified log file in the HPOM DMA Synchronization Log policy:

- From:

- `/var/opt/OV/shared/server/log/dma/sync.*.en`

- To:

- `C:\Documents and Settings\All Users\Application Data\HP\HP BTO Software\shared\server\log\dma\sync.*.en`

- b Install an HPOM agent on the HPOM DMA Windows host system.
- c Assign and deploy the HPOM DMA Synchronization Log policy to this new managed node.

# Post-Installation Steps on the Windows Host System

After installing HPOM DMA on a Windows host system, follow these steps.



For details of the directories used by HPOM DMA, see [Installation Locations](#) on page 229.

- 1 Remove the contents of the directory:

```
<SharedDir>\server\conf\dma\sync-packages
```

- 2 Copy the contents of the directory:

```
<InstallDir>\newconfig\DataDir\conf\dma\sync-packages\unix
```

To the directory:

```
<SharedDir>\server\conf\dma\sync-packages
```

This is the directory from which you deleted the original files in [step 1](#).

- 3 Start the HPOM DMA console by double-clicking the desktop icon or by entering the following address into a web browser:

**http://<Remote\_HPOM\_DMA\_System>:8081/hpdma**

- 4 In the Connection page of the HPOM DMA console, specify the connection for the HPOM management server:

- non-SSL HTTP connections

```
http://<HPOM_PA-RISC_host>:8081/ConfigurationItem/
```

In this URL, depending on your setup, *<HPOM\_PA-RISC\_host>* can be localhost, the short hostname, or the fully qualified domain name of the HPOM on PA-RISC host system.

- SSL HTTP connections

```
https://<HPOM_PA-RISC_host>:8444/ConfigurationItem/
```

In this URL, *<HPOM\_PA-RISC\_host>* must correspond to the HPOM PA-RISC host system as listed in the server certificate.

*<HPOM\_PA-RISC\_host>* usually takes the form of the fully qualified domain name.



The following entry in the HPOM DMA synchronization log file indicates that `<HPOM_PA-RISC_host>` is specified incorrectly:

```
Apr 24, 2009 1:07:18 PM;  
675230;12;com.hp.ov.om.dma.sync.test.connection.HttpRequest;  
getResponseCode;com.hp.ov.om.dma.common;WARNING;  
Error while opening a connection to 'https://mycompany/omws/  
ConfigurationItem/v1/service/Root_Services'.  
HTTPS hostname wrong: should be <mycompany>
```

The log file entry indicates that the web services client is configured to connect to the HPOM PA-RISC host system `mycompany` using the short hostname. However the connection is not successful, probably because the HPOM PA-RISC host system is listed in the server certificate with its fully qualified domain name. Change the URL in the Connection page to

`https://mycompany.com:8444/ConfigurationItem/`.

## Starting the HPOM DMA Console

To start the HPOM DMA console, do one of the following:

- Double-click the desktop icon.
- In a web browser, enter the following location:

**`http://<Remote_HPOM_DMA_System>:8081/hpdma`**

## Further Essential Installation and Configuration Steps

To complete the HPOM DMA installation and configuration on the HPOM and UCMDB or BAC host systems, continue with the instructions described in [Configuring HPOM DMA](#) on page 91.



---

# 7 Configuring HPOM DMA

To configure your installation, you need to make the following changes on the UCMDB or BAC system, the HPOM system and in the HPOM DMA console:

- **Change the HPOM DMA Console Default Password**

It is recommended that you immediately add at least one user with password and delete the default user to aid security.

For detailed instructions, see [Managing Users and Passwords](#) on page 93.

- **Update Your UCMDB or BAC Installation**

- Upload and deploy the HPOM DMA packages to the UCMDB or BAC system.

- Review the TQL queries in UCMDB or BAC, adapt them to your environment, and apply the enrichment rules.

For detailed instructions, see [Configuring UCMDB or BAC](#) on page 96.

- **Complete Assignments in HPOM**

- Assign the CMDB Service and Groups to an HPOM user.

- Assign and deploy the OM DMA policy or policy group to the HPOM management server (optional).

For detailed instructions, see [Configuring HPOM for UNIX or Linux](#) on page 107.

- **Specify Configurations in HPOM DMA**

Specify the web service endpoint connections between the UCMDB and the HPOM systems. Also specify the content for HPOM DMA synchronization.

For detailed instructions, see [Configuring HPOM DMA](#) on page 117.



Customizing synchronization using scripting (see the *HPOM DMA Extensibility Guide*) requires the HPOM DMA installation to be on the same system as the HPOM management server because the synchronization package `Script: Trigger Policy Distribution` is expected to run locally on the HPOM management server.

The remote HPOM DMA installation required to support HPOM on PA-RISC systems does not allow the script to be run as expected. If you want to use this feature for PA-RISC installations, you must run the script remotely on the HPOM management server system, for example, by using `ssh`.

# Managing Users and Passwords

The HPOM DMA console installation includes a default user:

- User: admin
- Password: admin

It is recommended that you immediately add at least one user with password and delete the default user to aid security.

Users are managed using the `dmauser` command-line tool available in the following location:

- *UNIX and Linux*  
`<InstallDir>/bin/dmauser.sh`
- *Windows 32-bit*  
`<InstallDir>\bin\dmauser.bat`
- *Windows 64-bit*  
`<InstallDir>\bin\win64\dmauser.bat`

## Adding a User

The `dmauser` command adds the specified user and its password to the local users store.

To add a new user, execute the following command:

- *UNIX and Linux*  
`<InstallDir>/bin/dmauser.sh -a <user name> <password>`
- *Windows 32-bit*  
`<InstallDir>/bin/dmauser -a <user name> <password>`
- *Windows 64-bit*  
`<InstallDir>/bin/win64/dmauser -a <user name> <password>`

## Changing a Password

The `dmauser` command changes the password of an existing user in the local users store.

To change the password of an existing user, execute the following command:

- *UNIX and Linux*  
`<InstallDir>/bin/dmauser.sh -a <user name> <password>`
- *Windows 32-bit*  
`<InstallDir>/bin/dmauser -a <user name> <password>`
- *Windows 64-bit*  
`<InstallDir>/bin/win64/dmauser -a <user name> <password>`

## Deleting a User

To delete an existing user from the local users store, execute the following command with the user name to be deleted:

- *UNIX and Linux*  
`<InstallDir>/bin/dmauser.sh -d <user name>`
- *Windows 32-bit*  
`<InstallDir>/bin/dmauser -d <user name>`
- *Windows 64-bit*  
`<InstallDir>/bin/win64/dmauser -d <user name>`

## Listing Users

To list all existing users in the local users store, execute the following command:

- *UNIX and Linux*  
`<InstallDir>/bin/dmauser.sh -l`
- *Windows 32-bit*  
`<InstallDir>/bin/dmauser -l`

- *Windows 64-bit*  
`<InstallDir>/bin/win64/dmauser -l`

## dmauser Usage

```
dmauser(.sh) -a <user name> <password> | -d <user name> |  
-h | -l | -version
```

-a, -add <user name> <password>	Adds a user to the local users store. If the user already exists, its password is replaced.
-d, -delete <user name>	Deletes the specified user from the local users store.
-l, -list	Displays all users stored in the local users store.
-h, -help	Displays usage information.
-version	Displays the version number of the dmauser tool.

# Configuring UCMDB or BAC

HPOM DMA delivers basic synchronization for operating systems and databases.

To use synchronization tools, follow these steps:

- **HPOM DMA Packages**

Upload and deploy the HPOM DMA packages to the UCMDB or BAC system.

For detailed instructions, see [Deploying HPOM DMA Packages to UCMDB or BAC](#) on page 97 or see the HPOM DMA online help.

- **TQL Queries**

Review the TQL queries in UCMDB or BAC and adapt them to your environment.

For detailed instructions, see [Reviewing the HPOM DMA Packages](#) on page 98 and [Adapting HPOM DMA TQL Queries](#) on page 102.

If you want to restrict service synchronization to nodes managed by a selected HPOM management server, you must configure the TQL queries to match your HPOM management server. For detailed instructions, see [Restricting Service Synchronization to Managed Nodes](#) on page 149.

- **Enrichment Rules**

Apply the enrichment rules.

For detailed instructions, see [Apply Enrichment Rules](#) on page 105.



## Deploying HPOM DMA Packages to UCMDB or BAC

To upload and deploy HPOM DMA packages to your UCMDB or BAC installation, follow these steps:

- 1 Copy the HPOM DMA packages into a temporary directory on the BAC or UCMDB system.

The HPOM DMA packages reside in the following directory on the HPOM DMA system:

*Version 7.5x*

*<InstallDir>/misc/dma/ucmdb/7*

*Version 8.0x*

*<InstallDir>/misc/dma/ucmdb/8*

*Version 9.0x*

*<InstallDir>/misc/dma/ucmdb/9*

- 2 Open the Package Manager:

- *UCMDB 7 and 8*

Select **Admin** → **Settings** → **Package Manager**.

- *UCMDB 9*

Select **Administration** → **Package Manager**.

- *BAC*

Select **Admin** → **Universal CMDB** → **Settings** → **Package Manager**.

- 3 Click **Deploy Packages to Server (from local disk)**.
- 4 In the Deploy Packages to Server dialog box, click **Add**.
- 5 Browse to the temporary directory on the BAC or UCMDB system where you stored the HPOM DMA packages.
- 6 Select the `hpdmacore.zip` file and click **Open**.  
This package must be deployed before any of the other HPOM DMA packages.
- 7 In the Deploy Packages to Server dialog box, click **OK**.

8 Deploy any of the following packages that you want to use:

- `hpdmaos.zip`  
Used for operating systems.
- `hpdmadb.zip`  
Used for databases.
- `hpdmasamples.zip`  
Used for the My Company Sample synchronization package.
- `hpdmaEUM.zip`  
*HP BAC only:* Used for End User Monitors

For each required package, repeat [step 3](#) to [step 7](#).

## Reviewing the HPOM DMA Packages

HPOM DMA uses TQL queries to extract node and service information from UCMDB. This information is then used to populate HPOM nodes and services.

For operating systems, the following TQL queries and corresponding views included in the `hpdmaos.zip` are delivered:

- UNIX Operating System (Operations)
- Windows Operating System (Operations)

For databases, the `hpdmadb.zip` package includes the following TQL queries and corresponding views:

- Oracle (Operations)
- MS SQL Server (Operations)
- Informix (Operations)
- Sybase (Operations)

An example of how to customize Service Navigator views in HPOM is available in the `hpdmasamples.zip` package. The TQL queries and corresponding views included are:

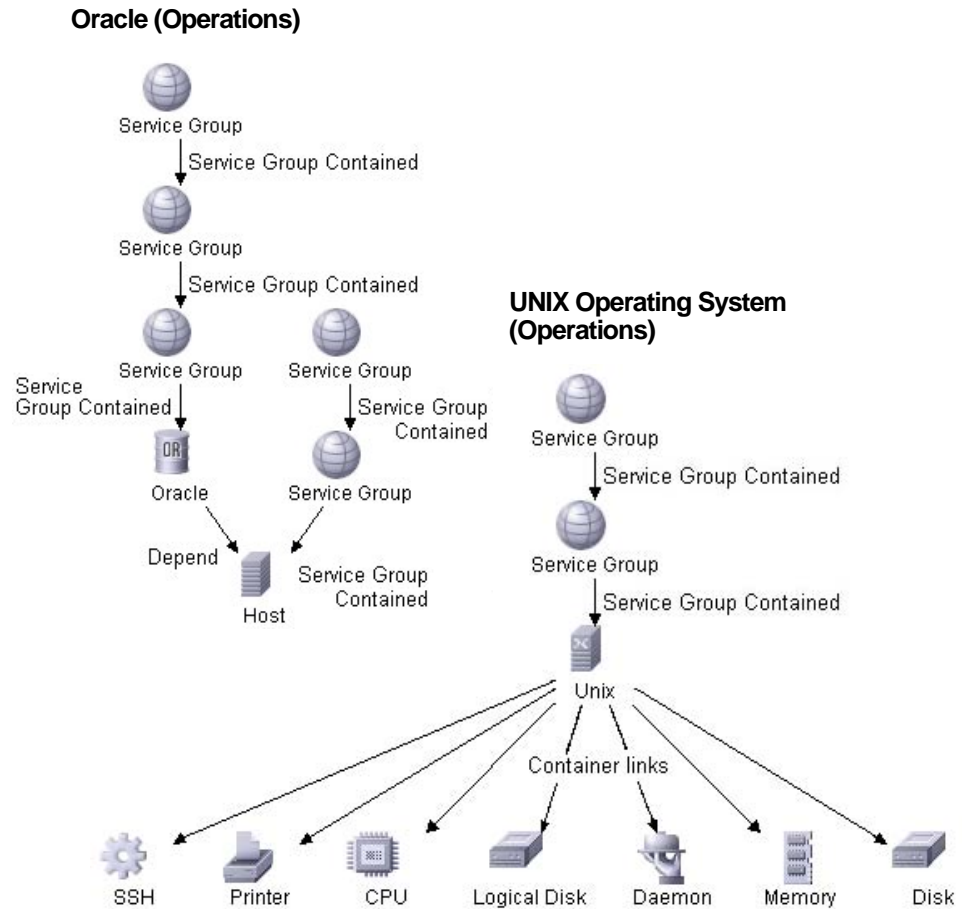
- My Company US (Operations)
- My Company EMEA (Operations)
- My Company ASIAPAC (Operations)

For displaying of End User Management views from BAC in HPOM, the TQL queries and corresponding views included in the `hpdmaEUM.zip` package are:

- End User Monitors (Operations)

Some examples of TQL queries are shown in [Figure 14](#).

**Figure 14 Examples of TQL Queries**



The predefined TQL queries are created to support HPOM service views. The relationships and the relationship types are important for correct status propagation within HPOM.

The correct status propagation within HPOM is achieved by the following:

- HPOM DMA introduces a new CI Type Service Group that is used as the top-level service above the discovered CIs. CIs are arranged under these service groups and linked using the Service Group Contained relationship.

The predefined package delivers the following service groups:

- Applications
  - Databases
    - Databases on UNIX
    - Databases on Windows
- End User Monitors
- Organizations
  - My Company
    - My Company ASIAPAC
    - My Company EMEA
    - My Company US
- Systems Infrastructure
  - UNIX
  - Windows
- **HPOM DMA then enriches the UCDMB or BAC system to assign the discovered CIs to the appropriate server groups. For that the following enrichment rules are used:**
  - DatabaseDependency
  - EUM
  - My Company ASIAPAC Databases
  - My Company ASIAPAC Unix Nodes
  - My Company ASIAPAC Windows Nodes
  - My Company EMEA Databases
  - My Company EMEA Unix Nodes
  - My Company EMEA Windows Nodes
  - My Company US Databases
  - My Company US Unix Nodes
  - My Company US Windows Nodes
  - NodeServerType

- Unix Databases
- Windows Databases
- Unix Nodes
- Windows Nodes
- UCMDB by default includes a host contains databases relationship. For proper status propagation, HPOM DMA introduces a database depends on host relationship. This is done by the enrichment rule Database Dependency.
- UCMDB includes the following relationships:
  - depends on relationship between Business Process Group and Business Process Step
  - monitored by relationship between Business Process Step and BPM Transaction from location

With HPOM DMA, the EUM enrichment rule adds an EUM contained relation for proper status propagation.

Additionally, the End User Monitors service group is added as the top level for End User Monitors CIs.

- HPOM DMA introduces an enrichment rule Node Server Type. With that rule, the host server type is set to the installed database type, for example, oracle. This is used for mapping hosts to node groups in HPOM.
- All other enrichment rules are used to assign the required CIs to appropriate service groups.

## Adapting HPOM DMA TQL Queries

HPOM DMA populates your HPOM node banks and service tree. If you are using BAC or UCMDB 7.5x or 8.0x, it is necessary that you adapt the node filters to suit to your specific environment. (The following adaption is not required for UCMDB 9.0x.)

To adapt HPOM DMA node filters, follow these steps:

- 1 Open the View Manager:
  - *UCMDB*
    - Admin → Modeling → View Manager**

- *BAC*

**Admin → Universal CMDB → Modeling → View Manager**

- 2 Expand the **hpdma** view from the Views list.

The TQL queries in the Database and Operating System groups include filters in the node types that you must adapt to your environment.

- 3 For each TQL query in the Database and Operating System groups, select the node type (Host, UNIX, or Windows).
- 4 From the shortcut menu, open **Node Properties**.
- 5 Change the filter to your environment.

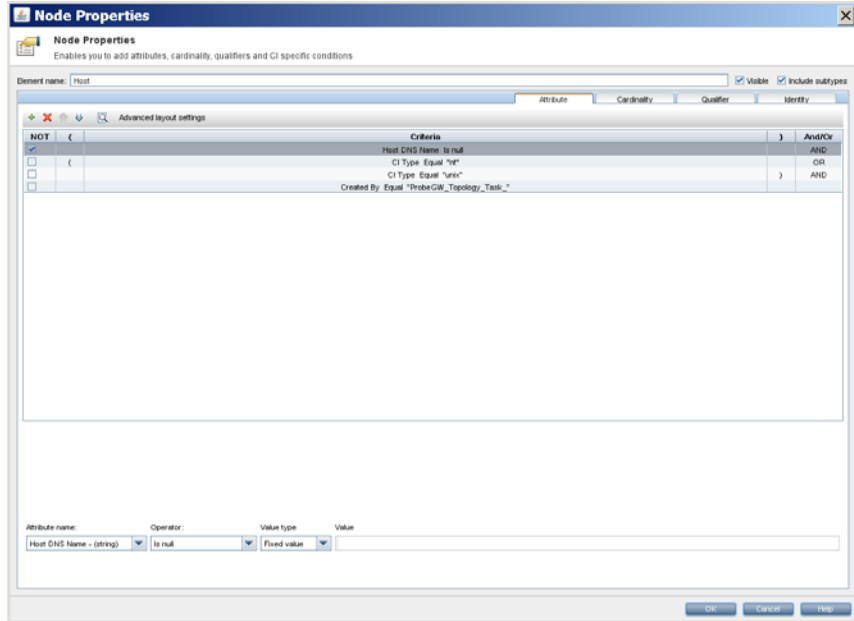
By default, only nodes that include running UCMDB probes are selected. This is specified with the following node condition:

```
Created By Equal "ProbeGW_Topology_Task_"
```

You can delete this condition and add new conditions to match your environment. For example, restrict on domain names and specify domains to limit your search.

Setting filters for TQL queries in the Node Properties window is shown in [Figure 15](#).

**Figure 15 Setting Node Conditions for TQL Queries**



Do not remove the HOST DNS Name is null filter, as this is required for HPOM DMA.



For adapting My Company synchronization package TQL queries, see the *HPOM DMA Extensibility Guide*.



## Apply Enrichment Rules

Apply each enrichment rule in the `hpdma` group.

- ▶ UCMDB enrichment rules only add the selected CI and relations to UCMDB. If you change the enrichment rule, for example, change the list of nodes that should be added to a service group, then the already existing CIs in the group are not automatically removed.

Before you change an enrichment rule, you should remove the already existing CIs.

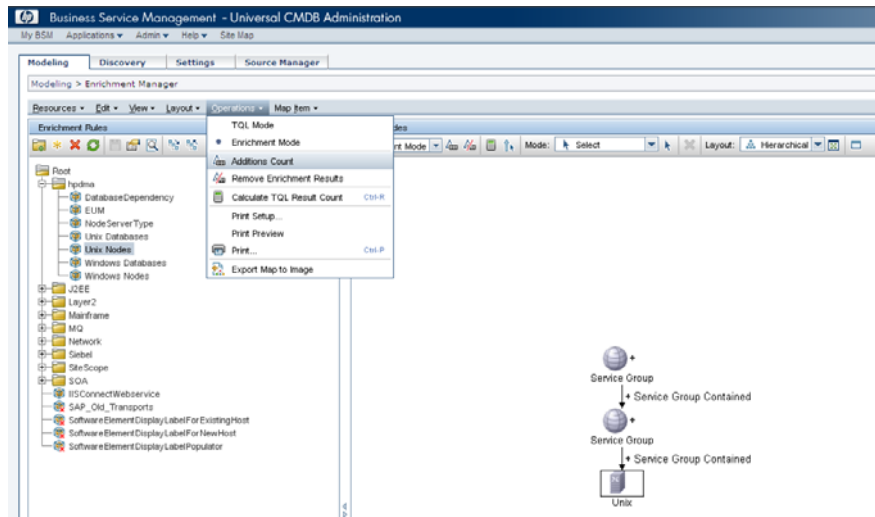
If you want to remove all currently existing assignment, select the enrichment rule in the CMDB Enrichment Manager and click **Remove Enrichment Results**.

This might also remove CIs and relations that have been added by other enrichment rules.

To apply enrichment rules, follow these steps:

- 1 Open the Enrichment Manager:
  - *UCMDB 7 and 8*  
**Admin** → **Modeling** → **Enrichment Manager**
  - *UCMDB 9*  
**Modeling** → **Enrichment Manager**
  - *BAC*  
**Admin** → **Universal CMDB** → **Modeling** → **Enrichment Manager**
- 2 Expand the **hpdma** group from the Enrichment Rules list.
- 3 Apply each enrichment rule by selecting **Operations** → **Additions Count** as shown in [Figure 16](#).

**Figure 16 Applying Enrichment Rules**



You must execute each enrichment rule whenever you discover new instances.



To make executing enrichment rules easier, you can add a schedule to regularly apply enrichment rules.

- *UCMDB 7 and 8*

Select **Admin** → **Settings** → **Scheduler**.

- *UCMDB 9*

Select **Administration** → **Scheduler**.

- *BAC*

Select **Admin** → **Universal CMDB** → **Settings** → **Scheduler**.

# Configuring HPOM for UNIX or Linux

This section contains the instructions how to do the following essential assignments on the HPOM for UNIX or Linux management server:

- [Assigning the CMDB Service Group to an HPOM User](#) on page 107.
- [Assigning the CMDB Node Groups to an HPOM User](#) on page 108.

This section also contains the instructions how to do the following optional assignments on the HPOM for UNIX or Linux management server:

- [Assigning the OM DMA Policy Group](#) on page 108.
- [Creating Service Type Definitions Automatically](#) on page 108.
- [Assigning User Profiles for Services on HPOM for UNIX or Linux](#) on page 109.
- [Automating Policy Distribution](#) on page 111.
- [Configuring HPOM Agent Types](#) on page 111.

## Assigning the CMDB Service Group to an HPOM User

To assign the `ROOT_DMA_Service` service group to an HPOM user, execute the following command:

```
opcservice -assign <HPOM_User_Name> ROOT_DMA_Service
```

Example:

```
opcservice -assign opc_adm ROOT_DMA_Service
```



User profile mapping enables you to map a service to an HPOM user profile. After synchronization, the service is assigned to all operators that are included in any specified HPOM user profile. If you use the User Profile Mapping feature, assigning the `ROOT_DMA_Service` service group to a user may not be appropriate. See the *HPOM DMA Extensibility Guide* for further details.

## Assigning the CMDB Node Groups to an HPOM User

Use the HPOM administrator console to assign the following CMDB node groups to an HPOM user:

- CMDB
- CMDB\_removed

## Assigning the OM DMA Policy Group

Use the HPOM administrator console to assign the OM DMA policy group to the agent on the HPOM management server. For details about the available policies, see [Objects Installed on HPOM](#) on page 237.

## Deploying the OM DMA Policy Group

Deploy the OM DMA policy group to the agent on the HPOM management server. For details about the available policies, see [Objects Installed on HPOM](#) on page 237.

▶ When monitoring HPOM DMA in cluster installations, policies should be enabled on the active node and disabled on all inactive nodes.

For information about policy deployment in cluster installations, see the appropriate HPOM documentation.

For HPOM installed on a cluster, policy assignments must be done on virtual nodes. For details, see the HPOM documentation on virtual nodes.

## Creating Service Type Definitions Automatically

Service type definitions (STDs) are used to identify how CIs from UCMDB are to be handled when building services in HPOM on synchronization. If an STD for an imported CI is not available in HPOM, it cannot be displayed in the

Service Navigator and an error message is displayed explaining that STDs are missing. HPOM DMA can automatically create STDs to suit non-matching CIs as they are imported into HPOM.



Automatic service type definition creation is disabled by default.

To enable automatic service type definition creation, follow these steps:

- 1 Enable automatic service type definition creation in the HPOM web service:

```
ovconfchg -ovrg server -ns  
opc.WebService.ConfigurationItem -set StdCreationEnabled  
true
```

- 2 Restart the Tomcat server:

```
ovc -restart ovtomcatB
```

## Assigning User Profiles for Services on HPOM for UNIX or Linux

User Profile Assignment enables you to map a service to an HPOM user profile. After synchronization, the service is assigned to all operators that are included in the specified HPOM user profile.

### Profile Prerequisites

Make sure that at least one user profile already exists in HPOM.

If the profile is missing or cannot be assigned to the service, the Service CI is created and a warning is logged in HPOM DMA. Additionally, an HPOM event message should be sent to the HPOM server. No error is returned by the web service when the HPOM DMA monitoring policies are deployed.



It is recommended that you do not assign user profiles to every service. Instead, assign them to a selected set of services at the top of a tree to be managed by the specified profile. Assigning a profile to every service usually results in poor performance.

## Mapping User Profiles

It is necessary to create user profile mapping (`usermapping.xml`) files for the services that you want to assign to a user. One user profile mapping file is required for each synchronization package that references services that you want to assign. To find out how to specify User Profile mapping, see the online help and the *HPOM DMA Extensibility Guide*.

## Enabling User Profile Assignment

User profile assignment for services is disabled by default. It can be enabled as follows:

- 1 Configure the HPOM for UNIX or Linux service engine to include user profiles by entering the following commands:

```
ovconfchg -ovrg server -ns opc -set  
OPCSVC_CONSIDER_PROFILES TRUE
```

- 2 Restart the service engine:

```
HPOM 8.xx: opcsv -start
```

```
HPOM 9.xx: ovc -restart SERVER
```

- 3 Create user profiles and assign operators to the profiles (see HPOM for UNIX or Linux documentation).
- 4 Create the user profiles in the service engine repository:

```
opcservice -operator <UserProfile>
```

- 5 Assign and deassign the user profiles to and from an existing service:

```
opcservice -assign <UserProfile> <ServiceName>  
opcservice -deassign <UserProfile> <ServiceName>
```

For example:

```
opcservice -assign UserProfile1 CMDB  
opcservice -deassign UserProfile1 CMDB
```

- 6 Enable user profile assignment in the HPOM web service:

```
ovconfchg -ovrg server -ns  
opc.WebService.ConfigurationItem -set  
UserProfileAssignmentEnabled true
```

- 7 Restart the Tomcat server:  
`ovc -restart ovtomcatB`
- 8 Restart Smart Message Mapping, if required:  
`ovc -start dmamsg`

## Automating Policy Distribution

The HPOM DMA Script: Trigger Policy Distribution synchronization package is deployed as part of the standard installation. It contains a post-upload script that triggers policy distribution.

If you want to configure automatic policy distribution, activate the Script: Trigger Policy Distribution synchronization package from the Content page.

## Configuring HPOM Agent Types

Attribute mapping defines the properties of a UCMDB CI, which in turn determines the node type on HPOM. It maps them to HPOM-specific values for the following properties:

- ovo\_osType
- ovo\_osVersion
- ovo\_SystemType
- ovo\_CommType

After a CI is identified as a node of a known type, it is ready for agent deployment and management using HPOM.

When nodes whose agents are not installed or available in HPOM are synchronized, warnings are written to the log files found in the following directory:

```
<SharedDir>/server/log/
```

The warnings take the following form:

```
WARNING; Machine Type for systemType: x86/x64 Compatible, osType: Windows_32, osVersion: Server 2003 (5.2), commType: HTTPS could not be evaluated and is set to OPC_MACHINE_OTHER (0)
```

In HPOM, not all agent packages must be installed. It is often the case that users have installed only the agent software to match the systems that they currently want to manage. When you want to manage additional agent types, you must install the appropriate HPOM agent packages.

After installing additional agent packages, it is necessary for you to execute the `ConfigureMachineTypes` script. This script uses the list of installed agent types from the HPOM database to select the required machine types from the `MachineTypes_template.xml` template file. The script stores this information for use at run time.

When you execute the `ConfigureMachineTypes` script, you might also see an error message of the following form, which describes the missing machine type and creates an example that can be used to update the `MachineTypes_template.xml` template:

```
No entry for Machine Type: 8 (Machine Type: SNI RM400/600 Network
Type:
```

```
IP Network OS Name: SINIX) found in the template (/var/opt/OV/
shared/server/conf/dma/MachineTypes.xml).
```

```
<?xml version="1.0" encoding="UTF-8" standalone="yes" ?>
```

```
<MachineType xmlns="http://schemas.hp.com/operations/1/
  MachineTypes" MachTypeId="8">
  <Description>Machine Type: SNI RM400/600 Network Type:
    IP Network OS Name: SINIX</Description>
  <Representations>
    <Default CommType="TO_BE_FILLED" SystemType=
      "TO_BE_FILLED" OsVersion="TO_BE_FILLED"
      OsType="TO_BE_FILLED"/>
  </Representations>
</MachineType>
```

```
Repository not updated, update the template and start again!
```

## Update HPOM DMA After Adding a New Agent Type

To update HPOM DMA after adding a new agent type to HPOM, follow these steps:

- 1 Open the template files for editing:

```
<SharedDir>/server/conf/dma/MachineTypes_template.xml
```



- 2 Add an entry in the template file to describe the machine type.

The following example shows how the entry for the missing SNI RM400/600 machine type should be specified:

```
<tns:MachineType MachTypeId="8">
  <tns:Description>Machine Type: SNI RM400/600 Network Type:
    IP Network OS Name: SINIX</tns:Description>
  <tns:Representations>
    <tns:Default CommType="DCE"
      SystemType="RM400/600" OsVersion="" OsType="SINIX"/>
  </tns:Representations>
</tns:MachineType>
```

- 3 Save and close the MachineTypes\_template.xml file.
- 4 Update the attribute mapping to set correct values for this machine type.

In HPOM DMA:

- osType is mapped to ovo\_osType
- osVersion is mapped to ovo\_osVersion
- SystemType is mapped to ovo\_SystemType
- CommType is mapped to ovo\_CommType

In the example, the attribute mapping must be updated with these values:

- ovo\_osType="SINIX"
- ovo\_osVersion=""
- ovo\_SystemType="SINIX"
- ovo\_CommType="DCE"

For further information about attribute mapping, see the *HPOM DMA Extensibility Guide*.

- 5 Execute the ConfigureMachineTypes script:

```
<InstallDir>/bin/ConfigureMachineTypes
```

For example:

```
"C:\Program Files\HP\HP BTO
Software\bin\win64\ConfigureMachineTypes"
```

The following message should be displayed if the updates have been correctly completed:

```
Repository successfully updated
```

# Configuring HPOM for Windows

This section explains how to do the following:

- [Creating Service Type Definitions Automatically](#) on page 114.
- [Assigning User Roles for Services on HPOM for Windows](#) on page 115.
- [Assigning and Deploying the OM DMA Policy Group](#) on page 116.

## Creating Service Type Definitions Automatically

Service type definitions (STDs) are used to identify how CIs from UCMDB are to be handled when building services in HPOM on synchronization. If an STD for an imported CI is not available in HPOM, it cannot be displayed in Service Navigator, and an error message is displayed explaining that STDs are missing. HPOM DMA can automatically create STDs to suit non-matching CIs as they are imported into HPOM.



Automatic service type definition creation is disabled by default.

To enable automatic service type definition creation, follow these steps:

- 1 Enable automatic service type definition creation in the HPOM web service:

```
ovconfchg -ovrg server -ns  
opc.WebService.ConfigurationItem -set StdCreationEnabled  
true
```

- 2 Restart the Tomcat server:

```
ovc -restart ovtomcatB
```



When you create your own STDs and you use the UI launch feature, you must assign the BAC Service UI Launch or UCMDB Service UI Launch tool groups to those STDs.

This is done in the HPOM for Windows console under **Tools** → **Configure** → **Service Types**.

## Assigning User Roles for Services on HPOM for Windows

User Role Assignment enables you to map a service to an HPOM user role. After synchronization, the service is assigned to all operators that are included in the specified HPOM user role.

### User Role Prerequisites

Make sure that at least one user role already exists in HPOM.

If the role is missing or cannot be assigned to the service, the Service CI is created and a warning is logged in HPOM DMA. Additionally, an HPOM event message should be sent to the HPOM server. No error is returned by the web service when the HPOM DMA monitoring policies are deployed.



It is recommended that you do not assign a user role to every service, but to a selected set of services at the top of a tree to be managed by the specified role.

### Mapping User Roles

It is necessary to create user profile mapping (`usermapping.xml`) files for the services that you want to assign to a user. One user profile mapping file is required for each synchronization package that references services that you want to assign. See the online help and the *HPOM DMA Extensibility Guide* for details on specifying User Profile mapping.

### Enabling User Role Assignment

User role assignment for services is disabled by default. It can be enabled as follows:

- 1 Create user roles and assign operators to the roles.  
For instructions, see the HPOM for Windows documentation.
- 2 Enable user role assignment in the HPOM web service:


```
ovconfchg -ovrg server -ns  
opc.WebService.ConfigurationItem -set  
UserProfileAssignmentEnabled true
```

- 3 Restart the IIS Admin Service:
  - a Select **Start** → **Administrative Tools** → **Services**.
  - b Right-click IIS Admin Service.
  - c Click **Restart**.
- 4 Restart Smart Message Mapping, if required:  
`ovc -start dmamsg`

## Assigning and Deploying the OM DMA Policy Group

Assign and deploy the OM DMA policy group to the HPOM management server.

For details about the available policies, see [Objects Installed on HPOM](#) on page 237.

-  When monitoring HPOM DMA in cluster installations, policies should be enabled on the active node and disabled on all inactive nodes.

For information about policy deployment in cluster installations, see the appropriate HPOM documentation.

For HPOM for Windows installed on a cluster, policies must be controlled by the agent Application Package Manager (APM). For details, see the HPOM for Windows online help.

# Configuring HPOM DMA

To configure HPOM DMA, complete the following tasks:

- [Specifying Web Service Endpoints](#) on page 117
- [Specifying Synchronization Content](#) on page 117
- [Synchronizing Nodes and Services](#) on page 118

## Specifying Web Service Endpoints

The web service endpoints for UCMDB and HPOM must be specified for correct connectivity. This is set from the Connections page in the HPOM DMA console. For detailed instructions, see the HPOM DMA online help.



The user to be specified in the Connection page of the HPOM DMA console must have sufficient rights on the HPOM for Windows management server.

To find out which users are HPOM for Windows administrators, check the `HP-OVE-ADMINS` group on the system where the HPOM for Windows management server is installed:

**My Computer** → **Manage** → **Local Users and Groups** → **Groups** → **HP-OVE-ADMINS** → **Properties**

Use one of these user to synchronize HPOM for Windows using HPOM DMA.

In HPOM for Windows version 8.1x, the local administrator account is no longer automatically added to the `HP-OVE-ADMINS` group.

## Specifying Synchronization Content

Before attempting to import node and service information from UCMDB or BAC into HPOM, you must specify some basic settings:

- HPOM root service for services imported from UCMDB or BAC
- Services and nodes CIs to be synchronized
- Synchronization packages that you wish to activate

For detailed instructions, see the HPOM DMA online help.

## Synchronizing Nodes and Services

After specifying the content of the HPOM DMA synchronization, you can do the following:

- Manually synchronize nodes or services in HPOM with their associated values in UCMDB.
- Set up a schedule to automatically trigger synchronizations. For detailed instructions, see the HPOM DMA online help.



Before synchronizing nodes or services for the first time after the installation of HPOM DMA, make sure that the enrichment rules have been applied. For more information, see [Apply Enrichment Rules](#) on page 105.

---

# 8 Upgrading HPOM DMA

The HP Operations Manager Dependency Mapping Automation upgrade installs the HPOM DMA version 8.20 software onto the HPOM host system. This chapter guides you through all the required steps. This process should take approximately 60 minutes to complete.

## Upgrading on Cluster Nodes

Upgrading HPOM DMA on a system participating in a cluster is supported on the active node only. An attempt to upgrade HPOM DMA on a non-active node is rejected by the installer.

HPOM DMA must be individually upgraded on each node participating in the cluster. For each node in the cluster, make it the active node and upgrade HPOM DMA on that node, following the instructions given in this chapter. Proceed with the next node in the cluster until HPOM DMA is upgraded on all cluster nodes.

# Upgrading HPOM DMA 8.10 to 8.20

To upgrade HPOM DMA from version 8.10 to version 8.20, you must follow these steps:

- 1 Read the rest of this guide before you start the installation wizard to plan your decisions and gather the information that you need.
- 2 Back up the HPOM DMA configuration.  
Follow the instructions in [Backing Up an HPOM DMA Configuration](#) on page 197.
- 3 Make sure your system meets the prerequisites required by HPOM DMA 8.20.  
Follow the instructions in [Chapter 4, Preparing HPOM DMA](#).
- 4 Install HPOM DMA using the DMA Application Installer.  
Follow the instructions in [Chapter 5, Installing HPOM DMA](#). The existing installation is updated.
- 5 Set up an integration user account in UCMDB or BAC.  
HPOM DMA requires the credentials of the `admin` user account or of an integration user account to access UCMDB or BAC. To set up an integration user account, follow the instructions in [Enabling HPOM DMA to Access UCMDB or BAC](#) on page 59.
- 6 Update the connection settings to UCMDB or BAC.  
In HPOM DMA 8.20, the connection settings require the fully qualified domain name of the system where the UCMDB is installed, the port number, and the user name and password of the integration user account set up in [step 5](#). For more information about specifying the web service endpoint connections, see the HPOM DMA online help.
- 7 Update the connection settings to HPOM.  
HPOM DMA 8.20 web service clients by default use SSL HTTP to communicate with the HPOM web services. Also by default, HPOM DMA web service clients trust all certificates issued from HPOM management servers in the environment. For more information, see [Securing](#) on page 175.



- 8 If you have deployed the HPOM DMA 8.10 discovery pattern to UCMDB or BAC 7.50, upload and deploy the updated HPOM DMA 8.20 discovery pattern to the UCMDB or BAC system.

For details, see [Updating the HPOM DMA Discovery Pattern in UCMDB or BAC](#) on page 122.

- 9 If you have modified the containment relationship mapping configuration file, open both versions of the configuration file and merge your modifications with the new HPOM DMA 8.20 configuration file.

For details, see [Updating Containment Relationship Mappings](#) on page 123.

- 10 If have installed UI Launch, perform the following configuration steps after you have upgraded to HPOM DMA 8.20:

- a On the HPOM management server, run the `dmadrilldown-toolgen` command. The following options have changed or are new:

- `<UCMDB_BAC_host>` (formerly `<URL>`)

The hostname of the BAC or UCMDB system:

```
<UCMDB_BAC_hostname>:8080
```

- `<DMA_host>` (new)

The hostname of the UI Launch Web Application system:

```
<DMA_hostname>:8081
```

For detailed instructions, see the section appropriate for the operating system of your HPOM host system: [Uploading Tools into HPOM for UNIX or Linux](#) on page 129 or [Uploading Tools into HPOM for Windows](#) on page 131.

- b In the Connection page of the HPOM DMA console, specify the application (BAC or UCMDB) and version that you want to launch. For detailed instructions, see the HPOM DMA online help.

## Updating the HPOM DMA Discovery Pattern in UCMDB or BAC

In the HPOM 8.20 discovery package `hpom.zip`, the CI type OM Agent has been replaced with the new CI type HP Operations Agent.

To update the HPOM DMA discovery pattern in UCMDB or BAC version 7.50, perform the following steps:

- 1 Deploy the HPOM DMA discovery pattern (`hpom.zip`) to the UCMDB or BAC version 7.50 system. After you have successfully deployed `hpom.zip`, restart the discovery probe.

For detailed instructions, see [Installing the BAC or UCMDB Discovery Pattern for HPOM](#) on page 150.

- 2 Exit the BAC or UCMDB web UI and log in again.
- 3 Modify all TQL queries. Replace OM Agent with HP Operations Agent.

For detailed instructions, see [Modifying the TQL Queries to Specify the HPOM Management Server](#) on page 153.

- 4 *Optional.* Delete all old OM Agent CIs:
  - a Set up a view showing all CIs of type OM Agent.
  - b Load the view in the IT Universe Manager.
  - c In the view, select all CIs of type OM Agent and delete them.

If you do not delete the CIs of type OM Agent, the UCMDB aging process will delete them.

## Updating Containment Relationship Mappings

If you have modified the HPOM DMA 8.10 containment relationship mapping configuration file, open the old and the new version of the configuration file and merge the changes in the new HPOM DMA 8.20 configuration file into your customized runtime version of the file:

- 1 Open both versions of the containment relationship mapping configuration file:
  - Customized runtime version (HPOM DMA 8.10)  
`<SharedDir>/server/conf/dma/containmentrelations.xml`
  - HP-delivered default version (HPOM DMA 8.20)  
`<InstallDir>/newconfig/DataDir/conf/dma/containmentrelations.xml`
- 2 Merge the changes in the new HPOM DMA 8.20 configuration file into your customized runtime version of the file.



---

## 9 Additional Features for HPOM DMA

HPOM DMA incorporates some additional features that make working with HPOM DMA, HPOM, UCMDB or BAC much more effective. It is not essential that you install and configure them. If you decide to use any or all of them, you may choose to set them up independently, and at any time.

The following lists HPOM DMA additional features:

- **Install and Configure the UI Launch**

When operators receive status change messages, they can open BAC or UCMDB from the HPOM console and drill down directly to the problem area using one of the following UI Launch tools:

- Show Correlated CI Map
- Show Change Report
- Show Neighborhood Map
- Show Triage Report (BAC only)
- Show End User Monitors (BAC only)
- Show Service Impact (BAC only)

To set up UI Launch for HPOM operators, you must complete some integration steps to set up the required tools.

For detailed instructions, see [Installing and Configuring the UI Launch](#) on page 127.

- **Configure Smart Message Mapping**

To run Smart Message Mapping, you must first enable the Server-based Message Stream Interface.

For detailed instructions, see [Configuring Smart Message Mapping](#) on page 134.

- **Customize Service IDs**

You can customize the service ID that HPOM DMA assigns to services synchronized from UCMDB using attribute mapping or scripting.

For detailed instructions, see [Customizing the ID of Services Synchronized from UCMDB](#) on page 143.

- **Select the Discovery Source**

You can choose how to discover your services in Service Navigator. The two types of discovery sources are:

- SPI discovery
- UCMDB discovery

If you want to use the UCMDB-based discovery, you must disable the service upload of the SPI discovery to avoid displaying two instances of the same service. It is recommended that you do not switch off the SPI discovery as some SPIs still need it for monitoring. Service upload is disabled by adding a filter entry corresponding to the SPI discovery that needs to be switched off.

For detailed instructions, see [Selecting the Discovery Source](#) on page 146.

- **Restrict Service Synchronization to Nodes Managed by a Selected HPOM Management Server**

HPOM DMA synchronizes services in UCMDB with the services monitored by HPOM. UCMDB typically maintains information about many more services than is actually managed by HPOM. HPOM DMA enables you to limit the synchronized information to those services that are of interest to a particular HPOM management server.

For detailed instructions, see [Restricting Service Synchronization to Managed Nodes](#) on page 149.

- **Business Process Monitoring Integration**

HPOM users can retrieve status alerts of business processes being monitored by BAC using Business Process Monitoring (BPM). To do this, you must complete the associated integration steps to set up BPM alert forwarding. You can also synchronize End User Management (EUM) views from BAC into HPOM by installing the BAC package for EUM Synchronization with HPOM DMA.

For detailed instructions, see [Integrating Business Process Monitoring](#) on page 159.

# Installing and Configuring the UI Launch

If you want to install and configure UI Launch, follow these steps:

- *For Show Change Report UI Launch:* Create and configure a Profile Database (Microsoft SQL Server) or a User Schema (Oracle). For detailed instructions, see [Configure a Profile Database or User Schema](#) on page 127.
- Upload the tools into HPOM. For detailed instructions, see the section appropriate for the operating system of your HPOM host system: [Uploading Tools into HPOM for UNIX or Linux](#) on page 129 or [Uploading Tools into HPOM for Windows](#) on page 131.
- Configure the UI Launch Web Application. For detailed instructions, see [Configuring the UI Launch Web Application](#) on page 133.

## Configure a Profile Database or User Schema

To launch the Show Change Report, a Profile Database (Microsoft SQL Server) or a User Schema (Oracle) must be configured.

This task describes how to configure one or more Profile Databases on a Microsoft SQL Server or Profile User Schemas on your Oracle Server.

### Prerequisites

Before you begin, make sure that you have the following connection parameters to the database server:

**1 Server Name**

Name of the machine on which the database application is installed.

**2 Database User Name and Password**

User name and password of a user with administrative rights on the database server.

**3 Server Port:**

- Microsoft SQL Server's TCP/IP port (default: 1433)
- Oracle listener port (default: 1521)

Additional prerequisite information for Oracle installations:

1 **SID**

Oracle instance name that uniquely identifies the instance of the Oracle database being used, if different from the default value, `orcl`.

2 **Default Tablespace**

Name of the dedicated default tablespace you created for profile user schemas. If you do not require a dedicated default tablespace, specify an alternative tablespace. The default Oracle tablespace is called `users`.

3 **Temporary Tablespace**

Name of the dedicated temporary tablespace you created for profile user schemas. If you do not require a dedicated temporary tablespace, specify an alternate tablespace. The default Oracle temporary tablespace is called `temp`.

If required, consult with your organization's database administrator to obtain this information.

## Add a Database

1 Access the Database Management page, located at:

**Admin** → **Platform** → **Setup and Maintenance** → **Manage Profile Databases**

2 Select **MS SQL** or **Oracle**, as appropriate, from the shortcut menu, and click **Add**.

3 In the Profile Database Properties page, enter the parameters of your database. For details, see the BAC or UCMDB documentation.



## Uploading Tools into HPOM for UNIX or Linux

The UCMDB or BAC UI Launch tools must be uploaded by running the `dmadrilldown-toolgen.sh` command located in the `<InstallDir>/bin` or `<InstallDir>\bin\win64` directories.

### dmadrilldown-toolgen.sh Command Parameters

```
dmadrilldown-toolgen.sh <tools_tar_file> <input_file>  
<output_file> <customer_id> <system_type> <UCMDB_BAC_host>  
<DMA_host> <user_name> <user_password>
```

`tools_tar_file` Path to the UCMDB or BAC launch tools tar file. Specify the file appropriate for your product installation:

`dma-BACTools`

`dma-UCMDBTools`

`input_file` Path to the UCMDB or BAC launch tools files. Select the file appropriate for your product installation:

`/opt/OV/misc/dma/drilldown/  
dma-BACapplications.dat.src`

`/opt/OV/misc/dma/drilldown/  
dma-UCMDBapplications.dat.src`

`output_file` A temporary file used to upload the UCMDB or BAC launch tools. The following files are used in examples in this section:

`/opt/OV/misc/dma/drilldown/  
dma-BACapplications.dat`

`/opt/OV/misc/dma/drilldown/  
dma-UCMDBapplications.dat`

`customer_id` Typically 1.

`system_type` BAC or UCMDB, depending on your product installation.

`UCMDB_BAC_host` The hostname of the BAC or UCMDB system:

`<UCMDB_BAC_hostname>:8080`

DMA_host	The hostname of the UI Launch Web Application system: <DMA_hostname>:8081
user_name	User name used to log on to the BAC or UCMDB system (optional).
user_password	Password used to log on to the BAC or UCMDB system (in conjunction with user_name).

Uploading the UCMDB or BAC launch tools requires you to execute the appropriate command for your product, specifying the host name and, if desired, the user name and password. If the user name and password are not specified, UI launches are accompanied by a log-on page where the appropriate credentials must be entered before the UI launch is allowed.

To upload the UCMDB or BAC launch tools, execute the appropriate command for your product:

- *UCMDB*

```
dmadrilldown-toolgen.sh dma-UCMDBTools
/opt/OV/misc/dma/drilldown/dma-UCMDBapplications.dat.src
/opt/OV/misc/dma/drilldown/dma-UCMDBapplications.dat 1
UCMDB <UCMDB_hostname>:8080 <DMA_hostname>:8081
<user_name> <user_password>
```

Example:

```
dmadrilldown-toolgen.sh dma-UCMDBTools
/opt/OV/misc/dma/drilldown/dma-UCMDBapplications.dat.src /
opt/OV/misc/dma/drilldown/dma-UCMDBapplications.dat 1 UCMDB
myUCMDBsystem.example.com:8080 myDMAsystem.example.com:8081
UCMDBuser MyPassWord
```

- *BAC*

```
dmadrilldown-toolgen.sh dma-BACTools
/opt/OV/misc/dma/drilldown/dma-BACapplications.dat.src
/opt/OV/misc/dma/drilldown/dma-BACapplications.dat 1 BAC
<BAC_hostname>:8080 <DMA_hostname>:8081 <user_name>
<user_password>
```

### Example:

```
dmadrilldown-toolgen.sh dma-BACTools
/opt/OV/misc/dma/drilldown/dma-BACapplications.dat.src
/opt/OV/misc/dma/drilldown/dma-BACapplications.dat 1 BAC
myBACsystem.example.com:8080 myDMAsystem.example.com:8081
BACuser MyPassWord
```

## Assigning Tool Groups

To be able to cross launch into BAC or UCMDB, you must assign an appropriate tool group to the operator:

- Universal CMDB
- Business Availability Center

## Uploading Tools into HPOM for Windows

The UCMDB or BAC UI launch tools must be uploaded by running the `dmadrilldown-toolgen.bat` command located in the `<InstallDir>\bin` or `<InstallDir>\bin\win64` directories.

### dmadrilldown-toolgen.bat Command Parameters

```
dmadrilldown-toolgen.bat <input_file> <output_file>  
<customer_id> <system_type> <UCMDB_BAC_host> <DMA_host>  
<user_name> <user_password>
```



The following examples assume that you are entering the commands from the `<InstallDir>\bin` or `<InstallDir>\bin\win64` directories.

<code>input_file</code>	Relative path to the UCMDB or BAC launch tools files. Select the file appropriate for your product installation: <pre>..\misc\dma\moffiles\en\dma-BACTools.mof.src ..\misc\dma\moffiles\en\dma-UCMDBTools.mof.src</pre>
<code>output_file</code>	A temporary file used to upload the UCMDB or BAC launch tools. The following files are used in this section: <pre>..\misc\dma\drilldown\moffiles\en\dma-BACTools.mof ..\misc\dma\drilldown\moffiles\en\dma-UCMDBTools.mof</pre>
<code>customer_id</code>	Typically 1.
<code>system_type</code>	BAC or UCMDB, depending on your product installation.
<code>UCMDB_BAC_host</code>	The hostname of the BAC or UCMDB system: <pre>&lt;UCMDB_BAC_hostname&gt;:8080</pre>
<code>DMA_host</code>	The hostname of the UI Launch Web Application system: <pre>&lt;DMA_hostname&gt;:8081</pre>
<code>user_name</code>	User name used to log on to the BAC or UCMDB system (optional).
<code>user_password</code>	Password used to log on to the BAC or UCMDB system (in conjunction with <code>user_name</code> ).

Uploading the UCMDB or BAC launch tools requires you to execute the appropriate command for your product, specifying the host name and, if desired, the user name and password. If the user name and password are not specified, UI launches are accompanied by a log-on page where the appropriate credentials must be entered before the UI launch is allowed.

To upload the UCMDB or BAC launch tools, execute the appropriate command for your product:

- *UCMDB*

```
dmadrilldown-toolgen.bat
"..\misc\dma\drilldown\moffiles\en\dma-UCMDBTools.mof.src"
"..\misc\dma\drilldown\moffiles\en\dma-UCMDBTools.mof" "1"
"UCMDB" "<UCMDB_hostname>:8080" "<DMA_hostname>:8081"
<user_name> <user_password>
```

Example:

```
dmadrilldown-toolgen.bat
"..\misc\dma\drilldown\moffiles\en\dma-UCMDBTools.mof.src"
"..\misc\dma\drilldown\moffiles\en\dma-UCMDBTools.mof" "1"
"UCMDB" "myUCMDBsystem.example.com:8080"
"myDMAsystem.example.com:8081" UCMDBuser MyPassWord
```

- *BAC*

```
dmadrilldown-toolgen.bat
"..\misc\dma\drilldown\moffiles\en\dma-BACTools.mof.src"
"..\misc\dma\drilldown\moffiles\en\dma-BACTools.mof" "1"
"BAC" "<BAC_hostname>:8080" "<DMA_hostname>:8081"
<user_name> <user_password>
```

Example:

```
dmadrilldown-toolgen.bat
"..\misc\dma\drilldown\moffiles\en\dma-BACTools.mof.src"
"..\misc\dma\drilldown\moffiles\en\dma-BACTools.mof" "1"
"BAC" "myBACsystem.example.com:8080"
"myDMAsystem.example.com:8081" BACuser MyPassWord
```

## Configuring the UI Launch Web Application

In the Connection page of the HPOM DMA console, specify the application (UCMDB or BAC) and version that you want to launch. For detailed instructions, see the HPOM DMA online help.

# Configuring Smart Message Mapping

To run Smart Message Mapping, you must:

- Enable the Server-based Message Stream Interface (Server MSI).
- Start the Smart Message Mapping component.



If you want to use Smart Message Mapping in cluster environments, you must make some configuration changes in the `ov-server.cntl` file. For further details, see [Configuring Smart Message Mapping in Cluster Environments](#) on page 71.

You can customize the following aspects of Smart Message Mapping:

- Hint separator
- Hostname separator
- Case sensitivity
- Update delay
- Polling interval
- Custom message attributes

## Enabling Server MSI on UNIX or Linux

When you enable the Server-based MSI on HPOM for UNIX or Linux, make sure to set the following options:

- Enable output
- Send *all* messages to server MSI
- *Divert* messages

To enable the Server MSI, use the following methods:

- **HPOM 8.xx for UNIX**  
Use the Configure Management Server window.
- **HPOM 9.xx for UNIX or Linux**  
Use the `opcsrvconfig(1M)` command-line tool.

## Enabling Server MSI on Windows

To enable the Server MSI, follow these steps:

- 1 In the HPOM shortcut menu, select **Configure** → **Server**.
- 2 In the Configure Server dialog box, open the **Namespace** drop-down menu and select **Server-based Message Stream Interface**.
- 3 Set `Enable server-based MSI` to **True**.
- 4 Set `Global Streaming Mode` for the server-based MSI to **Divert**.

## Starting and Stopping Smart Message Mapping

To start Smart Message Mapping, execute the command:

```
ovc -start dmamsg
```

To stop Smart Message Mapping, execute the command:

```
ovc -stop dmamsg
```

## Customizing Smart Message Mapping

You can configure the following aspects of Smart Message Mapping:

- **Hint separators**  
Configure the separators the Smart Message Mapper uses to extract hints from an incoming message. For instructions, see [Configuring the Hint Separator](#) on page 137.
- **Hostname separators**  
Configure the separators the Smart Message Mapper uses to extract hostnames from an incoming message. For instructions, see [Configuring the Hostname Separator](#) on page 138.
- **Case sensitivity**  
You can specify whether case sensitivity is required when matching CI attributes against fields in a message. For instructions, see [Configuring Case Sensitivity](#) on page 138.

- Update delay

You can set a minimum delay before service changes are processed. For instructions, see [Configuring the Update Delay](#) on page 139.

- Polling interval

You can configure how often the Smart Message Mappers polls for service changes, see [Configuring the Polling Interval](#) on page 139.

- Custom message attributes

You can attach CI attributes as custom message attributes to messages. For instructions, see [Assigning Custom Message Attributes to Messages](#) on page 140.

You can customize Smart Message Mapping using the Smart Message Mapper page in the HPOM DMA console (see [Figure 17](#) on page 137), or using an `ovconfchg` command of the following format:

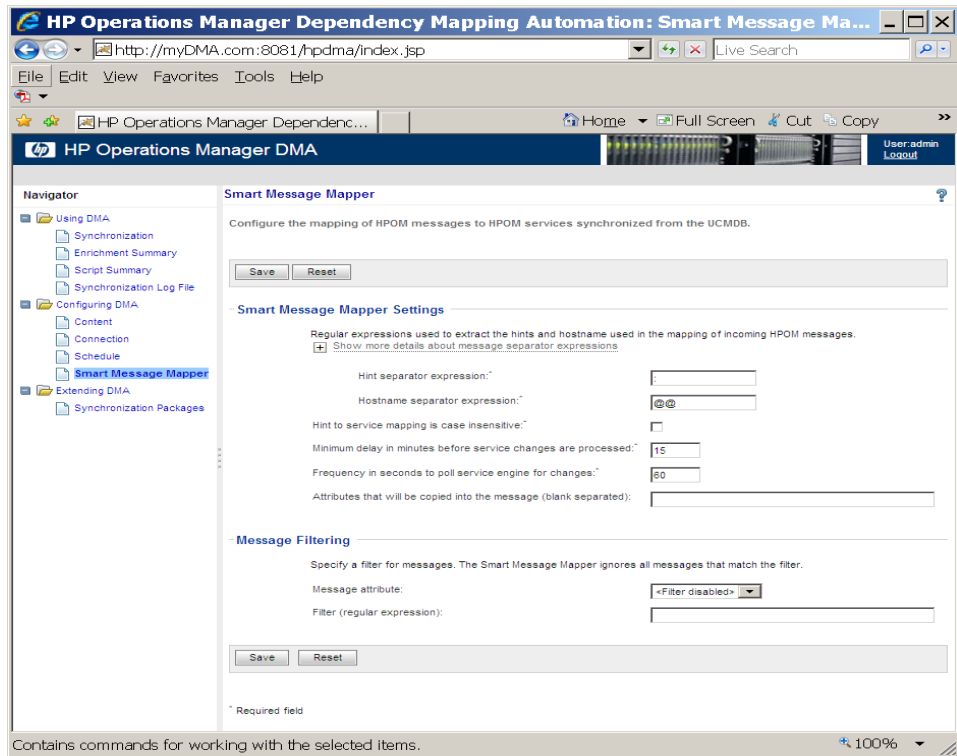
```
ovconfchg -ovrg server -ns dma.SmartMessageMapper -set  
<parameter> <value>
```



On PA-RISC systems, Smart Message Mapping cannot be configured using the HPOM DMA console. Use the `ovconfchg` command instead.



**Figure 17 Smart Message Mapper**



## Configuring the Hint Separator

The hint separator is used as the indicator for the Smart Message Mapper to divide an incoming message into the required hints. The default hint separator is a colon (:).

It is possible that messages from different sources are configured to use different separators. One source may use a colon (:) and another source uses a number sign (#). This is why you can specify multiple separators, for example, [#\$%].

Smart Message Mapping uses regular expressions as defined by the Java Pattern API to separate hints and hostnames. For more information about the regular expression syntax of the Java Pattern API, see the Java documentation.

To configure hint separators using the command line, enter the following command. Replace *<regular\_expression>* with the hint separators you want to use.

```
ovconfchg -ovrg server -ns dma.SmartMessageMapper -set  
ServiceSeparator "<regular_expression>"
```

▶ Do not select the same character to be used for hint separation and hostname separation.

## Configuring the Hostname Separator

The hostname separator is used as the indicator for Smart Message Mapping to identify the start of the hostname in an incoming message. The default hostname separator is two at signs (@@).

It is possible that messages from different sources are configured to use different separators. One source may use two at signs (@@) and another source uses a number sign (#).

Smart Message Mapping uses regular expressions as defined by the Java Pattern API to separate hints and hostnames. For more information about the regular expression syntax of the Java Pattern API, see the Java documentation.

To configure hostname separators using the command line, enter the following command. Replace *<regular\_expression>* with the hostname separators you want to use.

```
ovconfchg -ovrg server -ns dma.SmartMessageMapper -set  
HostnameSeparator "<regular_expression>"
```

▶ Do not select the same character to be used for hint separation and hostname separation.

## Configuring Case Sensitivity

The Smart Message Mapper is by default configured to consider the case of the text in incoming messages.

However, case sensitivity is not always an advantage. For example, DNS servers are not case sensitive, and CI attributes input using a mixture of cases may be referring to the same attribute. `MyWindowsHost.Example.COM` is viewed by the network as the same system as `mywindowshost.example.com`.

Use the following command to set case insensitivity (ignore case):

```
ovconfchg -ovrg server -ns dma.SmartMessageMapper -set IgnoreCase true
```

If set to false, Smart Message Mapping is case sensitive.

- ▶ Changing the case sensitivity option may not take effect immediately. The Smart Message Mapper must first reprocess all services. This may take several minutes depending on the number of services.

## Configuring the Update Delay

The Smart Message Mapping update delay stops the Smart Message Mapper from updating too often when there are multiple service changes in HPOM within a short period of time. The default delay is set to 15 minutes.

- ▶ Any changes that appear in HPOM during the update delay are not recognized by the Smart Message Mapper.

To configure the update delay using the command line, enter the following command:

```
ovconfchg -ovrg server -ns dma.SmartMessageMapper -set MinimumServiceUpdate <minutes>
```

## Configuring the Polling Interval

The polling interval determines how often the Smart Message Mapper checks the service engine for new, modified, or deleted services. After a change has been detected, the Smart Message Mapper schedules an update of its cache. The schedule is determined by the update delay setting.

The default polling interval is set to 60 seconds. The minimum interval is one second.

To configure the polling interval using the command line, enter the following command:

```
ovconfchg -ovrg server -ns dma.SmartMessageMapper -set PollingInterval <seconds>
```

## Assigning Custom Message Attributes to Messages

Smart Message Mapping enables you to attach CI attributes as custom message attributes (CMAs) to HPOM messages. In HPOM, you can then look up CI information directly in the message instead of viewing the properties of services.

Before Smart Message Mapping can attach CI attributes to messages, the CI attributes must be mapped to service attributes using attribute mapping rules. For more information about attribute mapping, see [Applying Attribute Mapping](#) on page 35.

To assign service attributes to messages using the command line, enter the following command:

```
ovconfchg -ovrg server -ns dma.SmartMessageMapper -set  
CustomMessageAttributes "<attribute> <attribute> ..."
```

Multiple service attributes must be separated by white space.

Smart Message Mapping retrieves the specified service attributes and the corresponding values, and copies this information into the message before forwarding the message to HPOM.

## Changing the Order of MSI Processes

The Message Stream Interface (MSI) API is used to register applications to receive messages on HPOM management servers. Messages are intercepted before they are added to the HPOM database and before they are displayed in the HPOM message browsers.

It might be necessary to change the order of MSI processes. For example, if an MSI process requires the original service IDs, you must assign a later order number to the Smart Message Mapping process.


For further information on changing the order of MSI processes, see the HP Operations Manager documentation.

## Setting the Order in HPOM for UNIX or Linux

To set the order for the Smart Message Mapper process in MSI:

- 1 Open the following file in an editor:

```
/etc/opt/OV/share/conf/OpC/mgmt_sv/msiconf
```

 If this file does not exist, create it. Add all processes that you need to order.

- 2 Add the following line to the file:

```
DmaSMM <your order number>
```

In this entry, the number is an integer and signifies where in the list of processes the DmaSMM process is placed.

- 3 Save and close the file.

## Setting the Order in HPOM for Windows

To set the order for the Smart Message Mapper process in MSI:

- 1 Open the Operations Manager console and select the Server-based MSI policy group:

**Policy Management** → **Server policies grouped by type** → **Server-based MSI**

- 2 Add a new policy:

Right-click **Server-based MSI** → **New** → **Policy**

The Server-based MSI policy editor opens.

- 3 Select **New**.

The MSI Instance dialog box opens.

- 4 In the Instance Name field, specify **DmaSMM**.

- 5 Enter the required order number.

The number is an integer and signifies where in the list of processes the DmaSMM process is placed.

- 6 Select the Application type **Legacy UNIX API**.

- 7 Click **OK**.

- 8 Click **Save and Close**.

- 9 Add a name and description for this new policy.
- 10 Click **OK**.

## Smart Message Mapping Simulation

The `dmasmmsim` command-line tool can be used to simulate and verify the behavior of the Smart Message Mapper without sending an OpC message. In the same way as the actual Smart Message Mapper, the `dmasmmsim` simulation tool evaluates how a message would be mapped. It responds with the selected service, where possible, without actually sending a message or updating any services in the Service Navigator. It also shows if there is no suitable service.

The `dmasmmsim` tool is located in `<InstallDir>/support`.

The `dmasmmsim` tool is executed in a similar way to the `opcmsg` command. It requires the following mandatory parameters:

- application name: `a`
- object name: `o`
- target node: `node`

The following parameter is optional:

service identifier: `service_id`

For example, enter the following command:

```
dmasmmsim a=oracle o=tablespace node=dbhost.example.com  
service_id="openview@@dbhost.example.com"
```

The result takes the following form:

```
Found CIs: 3634  
Matching CI is: openview ( ucmdb:d3bb0fc4562258ba33a43d329efe017  
@@dbhost.example.com )
```

# Customizing the ID of Services Synchronized from UCMDB

When HPOM DMA synchronizes services from BAC or UCMDB, it applies the following default service ID:

```
ucmdb:<ci_uid>@@<hosted_on>
```

This service ID is different from the service ID that is traditionally contained in HPOM messages. Therefore, without additional configuration, HPOM is not able to map messages generated by existing custom or SPI monitoring policies to services synchronized from UCMDB.

You can customize the service ID that HPOM DMA assigns to services synchronized from UCMDB using one of the following options:

- Attribute mapping

Attribute mapping is the recommended option because it is easy to use. However, when constructing the service ID, you are limited by the number of available attributes. If you want to create a more complex service ID, use scripting.

For more information, see [Customizing the Service ID with Attribute Mapping](#) on page 144.

- Scripting

Scripting gives you the flexibility to create complex service IDs because you can use additional processing and customization functions. You can integrate the code that generates service IDs into pre-mapping or pre-upload scripts.

For more information, see [Customizing the Service ID with Scripting](#) on page 145.

## Customizing the Service ID with Attribute Mapping

The following attribute mapping example creates a service ID of the following format (the HPOM DMA default service ID):

```
ucmdb:<ci_uuid>@@<hosted_on>

<?xml version="1.0" encoding="utf-8"?>
  <Mapping>
    <Rules>
      <Rule name="Map service name with host">
        <Condition>
          <Exists>
            <Attribute>hosted_on</Attribute>
          <Exists/>
        </Condition>
        <MapTo>
          <ServiceName>
            <Value>ucmdb:</Value>
            <XPathResult>./id</XPathResult>
            <Value>@@</Value>
            <Attribute>hosted_on</Attribute>
          </ServiceName>
        </MapTo>
      </Rule>
      <Rule name="Map service name without host">
        <Condition>
          <Not>
            <Exists>
              <Attribute>hosted_on</Attribute>
            <Exists/>
          </Not>
        </Condition>
        <MapTo>
          <ServiceName>
            <Value>ucmdb:</Value>
            <XPathResult>./id</XPathResult>
          </ServiceName>
        </MapTo>
      </Rule>
    </Rules>
  </Mapping>
</?xml>
```



```
</Rules>  
</Mapping>
```

## Customizing the Service ID with Scripting

The following extract from a script creates a service ID of the following format (the default service ID):

```
ucmdb:<ci_uuid>@@<hosted_on>  
  
for (ICi ci in syncData.getConfigurationItems())  
{  
    if( ci.getAttributeValue("hosted_on"))  
        ci.setServiceName( "ucmdb:" + ci.getId() + "@@" +  
            ci.getAttributeValue("hosted_on"))  
    else  
        ci.setServiceName( "ucmdb:" + ci.getId())  
}
```

# Selecting the Discovery Source

You can choose how to discover your services in Service Navigator.

The two types of discovery sources are:

- SPI discovery
- UCMDB discovery

You may want to use the UCMDB-based discovery as the source for displaying services in Service Navigator, but continue to use SPIs for monitoring. If both the UCMDB-based discoveries and the SPI-based discoveries are activated, you see two service trees in Service Navigator. SPI-generated messages are used to identify status in the SPI-based discovery service tree.

When you are satisfied that the service tree derived from the UCMDB discovery is being correctly displayed, you can disable the service upload of the SPI discovery and delete the service tree generated from the SPI discovery. This avoids displaying two instances of the same service.



It is recommended that you do not switch off the SPI discovery as some SPIs still need it for monitoring. You can disable the service upload only. See [Disabling SPI Discovery Service Upload for HPOM for UNIX or Linux](#) on page 146 and [Disabling SPI Discovery Service Upload for HPOM for Windows](#) on page 147 for details.

To continue to identify status in the UCMDB-based discovery service tree, activate Smart Message Mapping. For detailed instructions, see [Configuring Smart Message Mapping](#) on page 134.

Service upload for a particular SPI discovery is disabled by adding a filter entry corresponding to the SPI discovery that needs to be switched off.

## Disabling SPI Discovery Service Upload for HPOM for UNIX or Linux

On HPOM for UNIX or Linux, to disable a discovery service upload to Service Navigator, an option must be added to the associated tool to stop the service upload.

To disable discovery from a SPI, follow these steps:

- 1 Modify the discovery tool and replace the command in the Tool Call field with the following, for example:

```
/opt/OV/SPISvcDisc/bin/SPI_DiscServOprInt.sh -v -f /opt/OV/lib/osspi/UnixOSSPI_Disc.conf -n "$OPC_NODES"
```

- 2 In the Parameters field, enter the parameter:  
**-u false**
- 3 Save the modified tool.
- 4 Delete the service tree generated from the SPI discovery. For details, see the HPOM for UNIX or Linux documentation.

## Disabling SPI Discovery Service Upload for HPOM for Windows

On HPOM for Windows, any discovery source that must be disabled is added to the XPL configuration under the namespace `DiscoveryServiceFilter`. This namespace contains a list of service ID patterns used to filter out any service that should not be uploaded into Service Navigator. The patterns are matched against the text at the beginning of every service ID. For example, if discovery from the OSSPI is to be disabled, messages from the OSSPI must be ignored. This is done by filtering out any messages starting with the string:

OSSPI:

The XPL configuration has the following format, where a comma-separated value list of patterns specifies the services that are filtered out:

```
[DiscoveryServiceFilter]  
Excludes=OSSPI:,DBSPI:,MySPI,MyService
```

## Disabling Discovery from a SPI from the HPOM for Windows UI

To disable discovery from a SPI with messages that start with the OSSPI: strings, follow these steps:

- 1 From the HPOM for Windows UI, start the Disable SPI Discovery tool:

Go to **Tools** → **HP Operations Manager Tools** → **Disable SPI Discovery** and double-click the tool.

The Tool Status window and the Disable SPI Discovery windows are opened.

- 2 In the Disable SPI Discovery window, add the required statements. In the example, this is:

### **OSSPI :**

▶ If you are adding statements, make sure that you add commas between the existing statements and the new ones.

3 Click **OK**.

▶ If you select **Cancel**, a confirmation window opens with two portions:

- **OK** - All filter statements are deleted.
- **No** - Original filter statements are retained.

4 Delete the OSSPI service tree generated from the SPI discovery.

## Disabling Discovery from a SPI using XPL Configuration

The XPL configuration can also be modified with the XPL configuration tools. Use the `ovconfchg` command to add the discovery filters to the configuration, as described in the following procedure.

To add the discovery filters to the configuration, follow these steps:

1 Execute the following command:

```
ovconfchg -edit
```

The configuration file opens in a text editor (for example, Notepad).

2 In the editor window, add the following statements:

```
[DiscoveryServiceFilter]  
Excludes=OSSPI:
```

3 Save the changes.

4 Delete the OSSPI service tree generated from the SPI discovery.

# Restricting Service Synchronization to Managed Nodes

HPOM DMA synchronizes services in UCMDB with the services monitored by HPOM. UCMDB typically maintains information about many more services than are actually managed by HPOM. HPOM DMA enables you to limit the synchronized information to those services that are of interest to a particular HPOM management server.

To help you do this, the Discovery Pattern package is included. To install it, follow these steps:

- 1 Modify the UCMDB or BAC Classloader.  
For detailed instructions, see [Modifying the UCMDB or BAC Classloader](#) on page 149.
- 2 Install the Discovery Pattern on the BAC or UCMDB system.  
For detailed instructions, see [Installing the BAC or UCMDB Discovery Pattern for HPOM](#) on page 150.

To restrict service synchronizations you must configure the TQL queries to match your selected HPOM management server. For detailed instructions, see [Modifying the TQL Queries to Specify the HPOM Management Server](#) on page 153.

## Modifying the UCMDB or BAC Classloader

To modify the UCMDB or BAC classloader, follow these steps:

- 1 Open the following configuration file for editing:  
`<Discovery_Probe_InstallDir>\scripts\install\conf\WrapperEnv.conf`
- 2 Find the `set COLLECTORS_PROBE_CLASSPATH` entry:  
`set COLLECTORS_PROBE_CLASSPATH=%MAM_JARS%; ...`
- 3 Add the following paths to the start of the statement:

— *Version 7.5x*

```
%lib%/collectors/probeManager/discoveryResources/  
saaj-api.jar;%lib%/collectors/probeManager/  
discoveryResources/jaxb-api.jar;
```

The statement should now be as follows:

```
set COLLECTORS_PROBE_CLASSPATH=%lib%/collectors/  
probeManager/discoveryResources/saa-j-api.jar;;%lib%/  
collectors/probeManager/discoveryResources/  
jaxb-api.jar;%MAM_JARS%; ...
```

— *Version 8.0x*

```
%lib%/collectors/probeManager/discoveryResources/  
saa-j-api.jar;%lib%/collectors/probeManager/  
discoveryResources/jaxb-api.jar;%lib%/collectors/  
probeManager/discoveryResources/serializer.jar;
```

The statement should now be as follows:

```
set.COLLECTORS_PROBE_CLASSPATH=%lib%/collectors/  
probeManager/discoveryResources/saa-j-api.jar;%lib%/  
collectors/probeManager/discoveryResources/  
jaxb-api.jar;%lib%/collectors/probeManager/  
discoveryResources/serializer.jar;%MAM_JARS%; ...
```

- 4 Save and close the configuration file.
- 5 Restart the Probe.

## Installing the BAC or UCMDB Discovery Pattern for HPOM

To install the Discovery Pattern for HPOM on the BAC or UCMDB system, follow these steps:

- 1 Copy `hpom.zip` into a temporary directory on the BAC or UCMDB system.

The file `hpom.zip` resides in the following directory on the HPOM DMA system:

*Version 7.5x*

```
<InstallDir>/misc/dma/ucmdb/7
```

*Version 8.0x*

```
<InstallDir>/misc/dma/ucmdb/8
```

*Version 9.0x*

```
<InstallDir>/misc/dma/ucmdb/9
```

- 2 Open the Package Manager:

- *UCMDB 7 and 8*  
**Admin → Settings → Package Manager**
  - *UCMDB 9*  
**Administration → Package Manager**
  - *BAC*  
**Admin → Universal CMDB → Settings → Package Manager**
- 3 Click **Deploy Packages to Server (from local disk)**.
  - 4 In the Deploy Packages to Server dialog box, click **Add**.
  - 5 Browse to the temporary directory on the BAC or UCMDB system where you stored the `hpom.zip` file.
  - 6 Select the `hpom.zip` file and click **Open**.
  - 7 In the Deploy Packages to Server dialog box, click **OK**.
  - 8 From the Discovery tab, select **Setup Discovery Probes**.
  - 9 Go to **Credentials → OM WS Protocol**
  - 10 Click **Add new connection details for selected protocol type**.  
The Add Protocol Parameter dialog box opens.
  - 11 Choose the protocol that the HPOM DMA web service uses to communicate with the HPOM management server (`http` or `https`).  
If you are using the HTTPS protocol for secured connection, you can trust all certificates issued from HPOM management servers in the environment, or selected management servers only.  
To trust selected management servers only, complete the following steps:
    - a Set **Trust all SSL certificates** to false.
    - b Get a copy of the server certificate exported on the HPOM server. See [Exporting Certificates on HPOM for UNIX or Linux Management Servers](#) on page 177 or [Exporting Certificates on HPOM for Windows Management Servers](#) on page 180 for details.
    - c Copy the server certificate file `ServerCert.cer` to the directory:  
`<Discovery_Probe_InstallDir>/certificates`

d Import the server certificate into the Java keystore file for the client:

```
<Discovery_Probe_InstallDir>/jre/bin/keytool -import
-file <Discovery_Probe_InstallDir>/certificates/
serverCert.cer -keystore <Discovery_Probe_InstallDir>/
certificates/client.keystore
```

12 Specify the port number of the web server on the HPOM management server.

The default port number is:

HPOM for	UNIX or Linux	Windows
SSL HTTP	8444	443
non-SSL HTTP	8081	80

13 Specify the user name and password of an HPOM user with administrative rights.

14 In the Add Protocol Parameter dialog box, click **OK** to save your settings.

15 Open the Run Discovery page:

- *UCMDB 7 and 8*

**Admin → Discovery → Run Discovery**

- *UCMDB 9*

**Data Flow Management → Discovery Control Panel → Rerun Discovery**

- *BAC*

**Admin → Universal CMDB → Discovery → Run Discovery**

16 Select **Application HPOM Topology → HPOM by WS**

17 Right-click **HPOM by WS**, and from the shortcut menu, select **Activate**.

18 Right-click **HPOM by WS**, and from the shortcut menu, select **Rerun Discovery**.



## Modifying the TQL Queries to Specify the HPOM Management Server

To modify a TQL query to restrict synchronization to data that relates to nodes and services managed by a particular HPOM management server, follow these steps:

- 1 Open the View Manager:
  - *UCMDB 7 and 8*  
**Admin → Modeling → View Manager**
  - *UCMDB 9*  
**Modeling → Modeling Studio → Resources: Queries**
  - *BAC*  
**Admin → Universal CMDB → Modeling → View Manager**

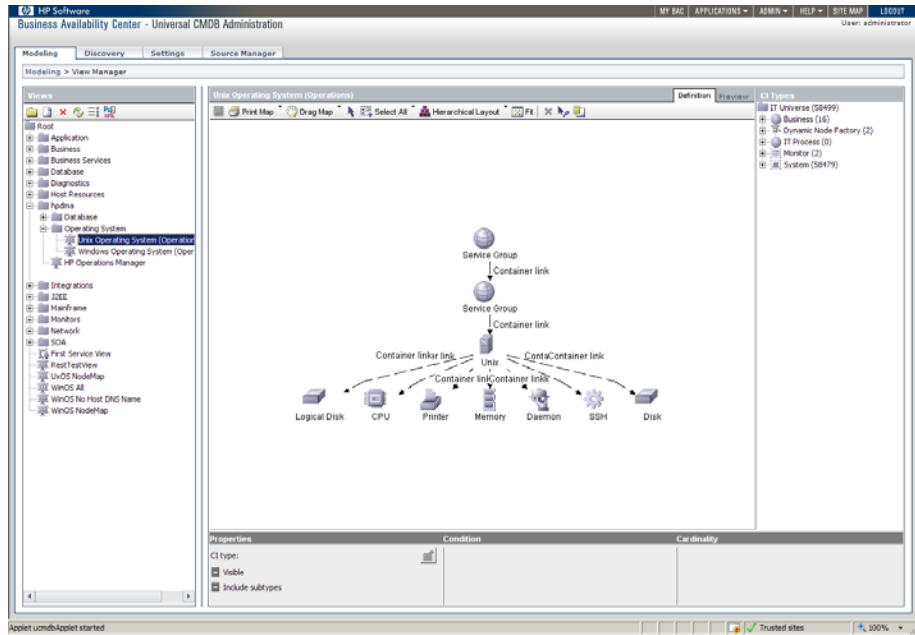
- 2 Expand the **hpdma** view from the Views list.

An example is shown in [Figure 18](#) on page 154.

The TQL queries are divided into the following groups:

- Database
- EUM
- Operating System
- Organization

Figure 18 View Manager with hpdma View Expanded



3 Select a TQL query.

4 Add HP Operations Agent and relationship:

- a From the CI Types list, navigate to HP Operations Agent:

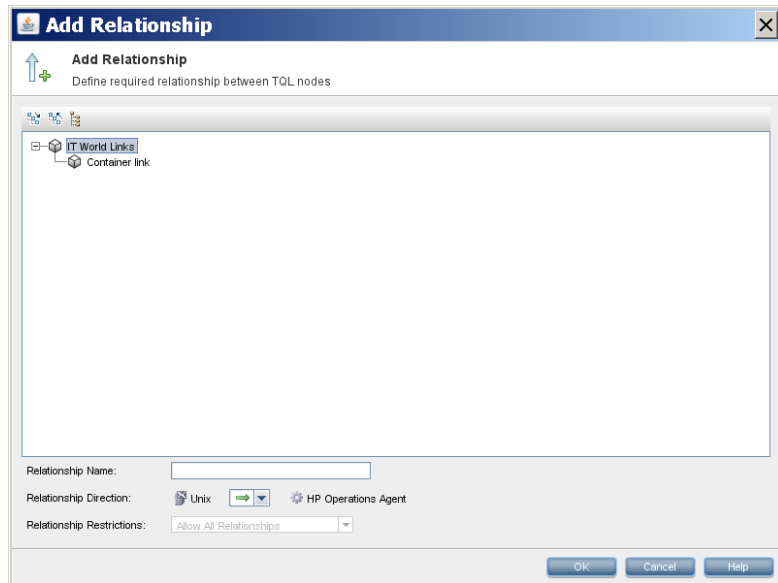
**IT Universe** → **System** → **Software Element** → **Agent** → **HP Operations Agent**

- b Drag the **HP Operations Agent** onto the TQL Query pane.

- c Create a Container link relationship from the host to the HP Operations Agent.

In the TQL Query pane, right-click the host and the **HP Operations Agent**. From the shortcut menu, select **Add Relationship**.

**Figure 19 Add HP Operations Agent Relationship**



5 Add OM Server and relationship:

- a From the CI Types list, navigate to OM Server:

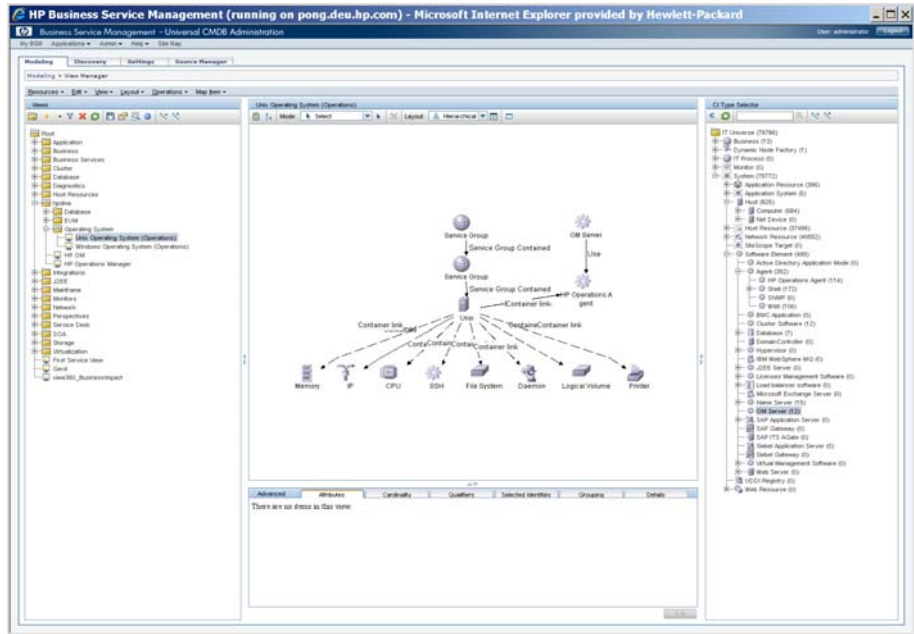
**IT Universe** → **System** → **Software Element** → **OM Server**

- b Drag the **OM Server** onto the TQL Query pane.

- c Create a Use relationship from the OM Server to the HP Operations Agent.

An example is shown in Figure 20.

Figure 20 Add HPOM Server



6 Add Host and relationship:

- a From the CI Types list, navigate to Host:

IT Universe → System → Host

- b Drag the **Host** onto the TQL Query pane.

- c Create a Container link relationship from the Host to the HPOM Server.

7 Right-click the newly added host that represents the HPOM management server and select **Node Properties**.

The Node Properties dialog box opens.

8 Click **Add an attribute condition**.

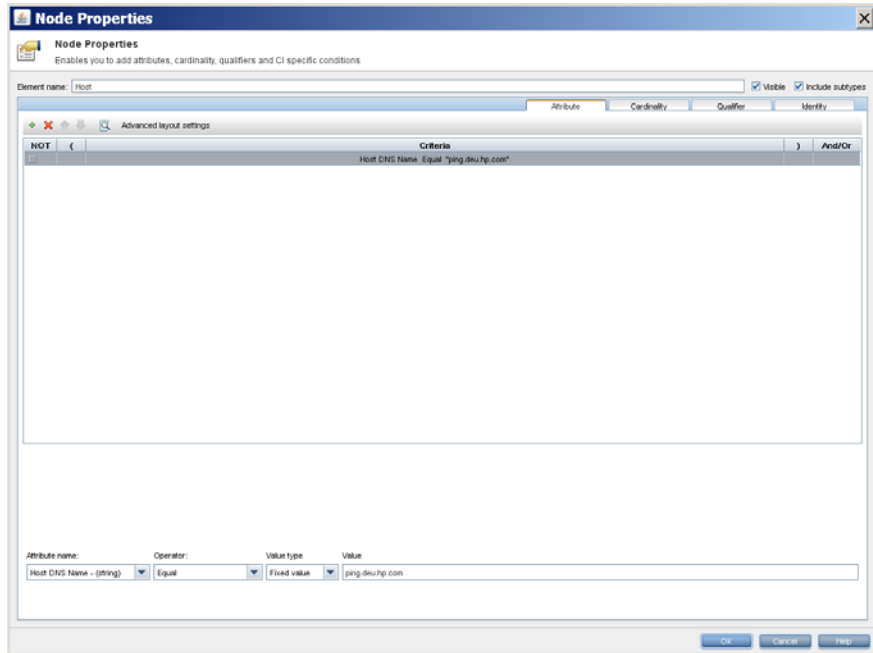
9 Select the following:

- Attribute name: **Host DNS Name - (string)**

- Operator: **Equal**
- Value: **Fixed Value** (Value cannot be changed.)

Enter the fully qualified host name of the HPOM management server system in the Value field, as shown in [Figure 21](#) on page 157.

**Figure 21 Node Properties**



- 10 Click **OK**.
- 11 Verify using the **Preview** tab.
- 12 If the preview displays the required results, for each newly added CI Type and relationship in the TQL query:
  - a Select **Node Properties**.
  - b Clear the `Visible` check box and click **OK**.



In the example, the Host and the HP Operations Agent are added CI types that must not be visible. The two Container links and the Use relationship connecting the Host and the HP Operations Agent to the system CI must also not be visible.

The TQL query is now modified to synchronize only the services being managed by the specified HPOM management server.

# Integrating Business Process Monitoring

HPOM operators can retrieve status alerts of business processes being monitored by BAC using Business Process Monitoring (BPM). When HPOM operators receive status change messages, they can open the BAC End User Monitors view from the HPOM console and drill down directly to the problem area.

To set up Business Process Monitoring for HPOM operators, complete these tasks:

- Task 1: [Forwarding BPM Alerts to HPOM](#) on page 159
- Task 2: [Setting Up CI Status Alerts](#) on page 159
- Task 3: [Setting Up Performance Limit Alerts](#) on page 161

## Forwarding BPM Alerts to HPOM

To enable operators to forward BPM alerts to HPOM, follow these steps:

- Make sure the HPOM agent is installed on the BAC server system.
- Make sure an `opcmsg` policy is created and deployed for the BAC alerts.
- Log on to the BAC UI at the following location:

**`http://<hostname>/HPBAC`**

Alerts can be set up to trigger on exceeding performance limits or when there is a change in the status of a CI. The CI Status Alerts are recommended because they can capture all status changes within the monitored business process.

## Setting Up CI Status Alerts

To set up CI Status Alerts, follow these steps in the BAC UI:

- 1 Open the CI Status Alerts tab:  
**Admin → Alerts → CI Status Alerts**
- 2 Select the End User Monitors view.
- 3 Click **New Alert**.

The Create New Alert dialog box opens.

- 4 Click **Next** and set up a new alert as follows.
- 5 Specify a name and description and use the condition **Send alert if status worsens**.
- 6 Click **Next** and select the required CIs.
- 7 Click **Next** and go to **Actions** and click **New Executable File**.
- 8 In the Create New Executable File dialog box, enter an `opcmsg` command.

Example:

```
opcmsg service="BPM" a="<<Alert Name>>" o="<<CI Name>>"  
msg_t="<<Current Status>>: <<KPI Name>> = <<KPI Value>>"  
-option KPIName="<<KPI Name>>" -option KPIValue="<<KPI  
Value>>" -option PreviousStatus="<<Previous Status>>"  
-option CurrentStatus="<<Current Status>>" -option  
TriggerTime="<<Trigger Time>>"
```



The example assumes that there is a service with the name BPM in the service tree. This is a manually added service. If you plan to synchronize the End User Monitors view, you should change the service parameter to `<CI_name>`.

- 9 Click **OK**.
  - 10 Click **Finish**.
- The alert summary page opens.
- 11 Click **OK** to apply the CI status alert. It is then available in the alert list.  
BPM alerts are now available in the HPOM console.
  - 12 To see a report of generated alerts, open the CI Status Alert Reports tab:

**Applications → Alerts → CI Status Alert Reports**

For further information about CI Status Alerts in Business Process Monitoring, see the BAC online help from the Help menu.



## Setting Up Performance Limit Alerts

To set up alerts on performance limits, follow these steps in the BAC UI:

- 1 Open the Event Based Alerts Configuration page:  
**Admin → Alerts → Event Based Alerts → Event Based Alerts Configuration**
- 2 Select a business process profile from the **Profile:** drop-down list.
- 3 Click **New Alert**.  
The Create Alert Wizard opens.
- 4 Select a trigger type from the Trigger Criteria tab. For example, Transaction response time or Average transaction response time.
- 5 Select the **Filters** tab and specify any required restrictions.
- 6 Select the **Actions** tab and click **Run executable file**.  
The Run Executable File dialog box opens.
- 7 In the Run Executable File dialog box, select **User defined** from the drop-down menu and enter the name of the file you want to execute.  
The file should contain an `opcmsg` command.

Example:

```
opcmsg service="BPM" a="<<Profile Name>>"  
o="<<Transaction Name>>" msg_text="<<Severity>>: <<Actual  
Details>>, BPM location: <<Location Name>>" -option  
AlertName="<<Alert Name>>" -option  
AlertPurpose="<<AlertPurpose>>" -option ID="<<ID>>"  
-option LocationName="<<Location Name>>" -option  
Severity="<<Severity>>" -option TriggerCause="<<Trigger  
Cause>>" -option UserMessage="<<User Message>>"
```



The example assumes that there is a service with the name BPM in the service tree. This is a manually added service. If you plan to synchronize the End User Monitors view, you should change the service parameter to `<CI_name>`.

- 8 Click **OK** to close the Run Executable File dialog box.

- 9 Select the **Settings** tab and set severity and notification frequency.
- 10 Click **Finish**.
- 11 To see a report of generated alerts, open the Event-Based Alerts Reports tab:

**Applications** → **Alerts** → **Event-Based Alerts Reports**

BPM alerts are now available in the Performance Limit Alerts in Business Process Monitoring, see the BAC online help from the Help menu.

## Synchronizing EUM Views

You can also synchronize End User Management (EUM) views from BAC into HPOM.

To synchronize EUM views, complete these tasks:

- Task 1: [Installing the BAC Package for EUM Synchronization with HPOM DMA](#) on page 162
- Task 2: [Activating the End User Monitors Synchronization Package](#) on page 164

The following are automatically installed:

- An additional Synchronization Package for HPOM DMA
- Additional Service Type Definitions and Compositions for the EUM CI types are automatically uploaded into HPOM during the HPOM DMA installation



End User Monitors are only available in BAC and not in the standalone UCMDB product. Do not deploy to a UCMDB installation.

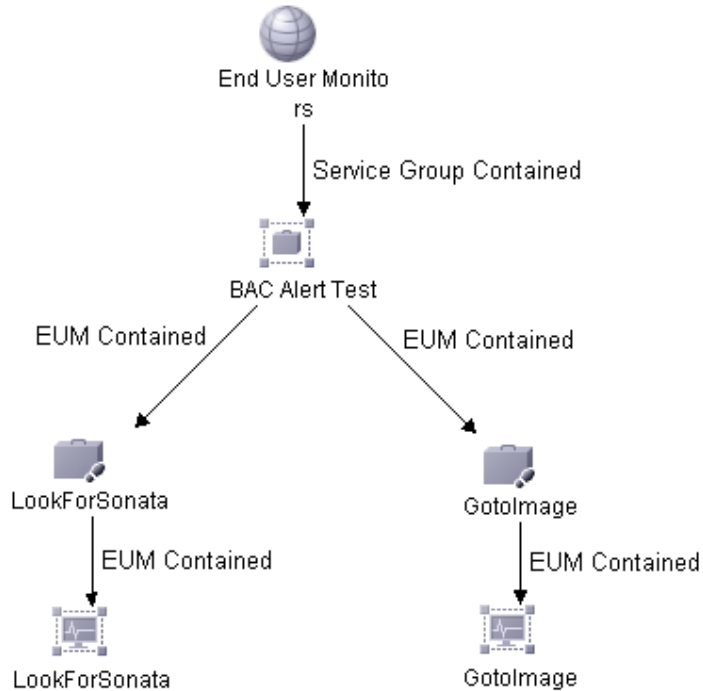
## Installing the BAC Package for EUM Synchronization with HPOM DMA

The `hpdmaEUM.zip` package contains:

- EUM contained UCMDB containment relationship type
- UCMDB enrichment rule used to prepare the EUM tree for synchronization
- End User Monitors (Operations) view TQL, which can be queried by HPOM DMA using the UCMDB web service interface

Figure 22 shows an example of an EUM View in BAC selected by the End User Monitors (Operations) view TQL.

**Figure 22 EUM View in BAC Selected by End User Monitors (Operations) View TQL**



To upload and deploy the BAC package to your BAC installation, follow these steps:

- 1 Copy the `hpdmaEUM.zip` file into a temporary directory on the BAC system.

The `hpdmaEUM.zip` file resides in the following directory on the HPOM DMA system:

*Version 7.5x*

`<InstallDir>/misc/dma/ucmdb/7`

*Version 8.0x*

<InstallDir>/misc/dma/ucmdb/8

- 2 Open the Package Manager in BAC:  
**Admin → Settings → Package Manager**
- 3 Click **Deploy Packages to Server (from local disk)**.
- 4 In the Deploy Packages to Server dialog box, click **Add**.
- 5 Browse to the temporary directory on the BAC system where you stored the hpdmaEUM.zip file.
- 6 Select the hpdmaEUM.zip file and click **Open**.
- 7 In the Deploy Packages to Server dialog box, click **OK**.

## Activating the End User Monitors Synchronization Package

The synchronization package for the EUM synchronization is automatically installed during HPOM DMA installation as a standard synchronization package.

To activate the End User Monitors Synchronization Package:

- 1 Open the Synchronization configuration page and check the **End User Monitors (BAC only): Out of the box synchronization package for BAC End User Monitors**.
- 2 Click **Save**.
- 3 Start a new synchronization from the Synchronization page.  
On completion, the EUM view is synchronized into HPOM.

---

# 10 Licensing

This chapter describes how to install and configure OVkey licenses for HPOM DMA.

## OVkey Licenses

HPOM DMA uses the HP AutoPass licensing security technology for the management of OVkey licenses. All OVkey license passwords are stored in a license file, maintained by AutoPass.

Because the OVkey licensing technology does not require a license server, the product may be used behind firewalls and in clustered environments.

When installing and setting up OVKey licenses in your HPOM DMA environment, keep the following points in mind:

- Licenses are linked to the IP address of the HPOM DMA host system and not its target ID.
- Each HPOM DMA installation has one central location for license administration.



The HPOM DMA installation on the selected Windows host system requires a valid licence. PA-RISC HPOM for UNIX host systems do not need an HPOM DMA licence.

## Types of Licenses

You can obtain the following types of licenses:

- **Instant-On License**

This license is installed with HPOM DMA and enables you to use HPOM DMA for evaluation purposes. You can use HPOM DMA for a period of 60 days. You can extend its validity once for a further 60 days by submitting a request to the HP Password Delivery Service.

- **Permanent License**

A permanent license allows you unlimited use of HPOM DMA for the associated installation.

See [Requesting a Product License](#) on page 171 for more details about requesting licenses.

- **Evaluation License**

An extended temporary license allows you an extra 60 days evaluation period for HPOM DMA.

If the permanent license key is not yet available, or if more evaluation time is needed, an evaluation extension license key can be requested at no cost through the local password center. These requests should be made by Telephone, although email and fax requests are also accepted. Evaluation extension license keys may be requested once only, and they are valid only for the system specified in the request. Some products do not have extension keys available. Hewlett-Packard reserves the right to restrict the availability of extension license keys at any time.



Evaluation extension requests cannot be made through the web. If the request is urgent and the local regional password center is closed, the password center that is open in another region can be contacted.

Have the following information available before requesting an Evaluation Extension:

- Software product number
- IP address or host name of the system where the evaluation software is installed.
- Contact information (company, name, address, phone, and email).

Evaluation extension keys are sent out through email and are valid for 60 days. See the product documentation for information on license key installation.

## Checking Licenses

HPOM DMA checks licenses during startup and when scheduled, once every 24 hours.

If your Instant-On license has not expired, you are informed of the days remaining before the license expires.

If your Instant-On license has expired, you receive a message in a message browser once every 24 hours.

## Installing Licenses on 64-bit Windows HPOM DMA Systems

If after installing HPOM DMA on 64-bit Windows systems, the Synchronization page indicates an invalid license status although a valid license is installed, complete the following steps:

- 1 Add the SYSTEM user to the licensing file `LicFile.txt` with full file access permissions:
  - a Locate the following file in Windows Explorer:  
`%OvShareDir%\server\OprEl\AutoPass\LicFile.txt`
  - b Right-click the file and select **Properties**.
  - c Open the **Security** tab.
  - d Add the SYSTEM user to the list of users and assign full control to this user.
  - e Click **OK** to save your changes and close the Properties dialog box.
- 2 Install the instant-on license manually:
  - a Open a command prompt and type:  
`cd "%OvInstallDir%OprEl\AutoPass\utilities"`

**b** Install the license. Type one of the following commands:

– 32-bit management servers:

```
APIOInstaller.exe -pdf  
"%OvInstallDir%misc\dma\pd_files\DMASync_pdf.txt"  
-idr "%OvInstallDir%OprEl\AutoPass"  
-ddr "%OvShareDir%server\OprEl\AutoPass"
```

– 64-bit management servers:

```
APIOInstaller64.exe -pdf  
"%OvInstallDir%misc\dma\pd_files\DMASync_pdf.txt"  
-idr "%OvInstallDir%OprEl\AutoPass"  
-ddr "%OvShareDir%server\OprEl\AutoPass"
```



# Setting Up OVkey Licenses

To set up and activate an HPOM DMA product license, follow these steps:

- 1 Obtain the required information from your host system.  
See [Getting the Required Information](#) on page 169 for details.
- 2 Complete the HP Software License Request Form by doing one of the following:
  - Edit the request-form file for a licence, then email, fax, or mail the file to HP.
  - Fill out an online form at the HP Internet License Request Center.  
See [Requesting a Product License](#) on page 171 for details.
- 3 Receive a license from the HP Password Delivery Center.  
See [Receiving License Passwords](#) on page 173 for details.
- 4 Install and verify the HPOM DMA Product License.  
See [Installing Product Licenses](#) on page 173, and [Verifying Product Licenses](#) on page 174 for details.

## Getting the Required Information

You can get the information specified in [Table 3](#) on page 170 from documents included with your product.

**Table 3 Information Required to Get Licenses**

<b>Information Required</b>	<b>Where to Find It</b>
HP Order Number (permanent passwords only)	License-to-Use Entitlement Certificate Local system administrator or HP Sales Representative.
IP address of the HPOM DMA <sup>a</sup> host system	On the HPOM DMA host system, execute the following command in a Command Prompt window: <ul style="list-style-type: none"><li>• <i>UNIX and Linux</i> <code>/usr/bin/nslookup &lt;hostname&gt;</code></li><li>• <i>Windows</i> <code>ipconfig /all</code></li></ul>
Hostname <sup>b</sup>	On the HPOM DMA host system, execute the following command in a Command Prompt window: <code>hostname</code>
Operating System Version	On the HPOM DMA host system: <ul style="list-style-type: none"><li>• <i>UNIX and Linux</i> Execute the following command in a Command Prompt window: <code>uname -a</code></li><li>• <i>Windows</i> Go to <b>Start</b> → <b>Control Panel</b> → <b>System</b> → <b>General</b></li></ul>
Number of Licenses (permanent passwords only)	HP Purchase Order

- a. If you are operating in a clustered environment, the IP address of the HPOM DMA cluster package and all local IP addresses of the participating nodes are required.
- b. If you are operating in a clustered environment, the fully qualified host name of the HPOM DMA cluster package and all fully qualified host names of the participating nodes are required.

## Requesting a Product License

You may request a license in one of two ways:

- **Internet**

If you have access to the Internet, you can use the HP Internet Password Delivery Service.

- **Mail, Phone or Fax**

If you do not have access to the Internet, you can complete and submit a license request form.



AutoPass stores the passwords at a location that is typically not shared in HA environments, and it also uses the local IP address and not the virtual IP address, make sure that you request license passwords for all cluster nodes in an HA environment with its physical IP address and install these passwords on the according cluster nodes.

### Requesting by Internet

If you can access the Internet, you can get license passwords by visiting the home page of the HP Password Delivery Service at the following location:

**<http://www.webware.hp.com/>**

You can use this site to do the following:

- **Generate Passwords**

Generate new product passwords, assuming you have already purchased a product and have an HP order number.

- **Move Licenses**

Move licenses from one machine to another.

- **Migrate Licenses**

Migrate licenses from an older version of a product to a new version using a migration password.

- **Contact a Password Delivery Center**

Locations, contact details, and availability of the HP Password Delivery Centers.

- **Passwording FAQs**

Information about licensing and passwords.

## Requesting by Mail, Phone or Fax

If you do not have access to the Internet, you can request a license by mail or fax using the licence request template on the back of the entitlement certificate. Enter the requested information, and mail or fax it to the nearest HP Password Delivery Center using the information in [Table 4](#).

**Table 4 HP Password Delivery Centers**

<b>Your Location</b>	<b>Password Center Location</b>	<b>Email Address</b>	<b>Phone/Fax Number</b>	<b>Service Hours (Mon-Fri Local Time)</b>
North/South America	USA	americas_password@cnd.hp.com	+1 (801) 431-1597 +1 (800) 326-0411 <i>+1 (801) 431-3654</i>	06:00-18:00 (MST) <sup>a</sup>
Asia/Pacific	Japan	asia_password@cnd.hp.com	Japanese: +81 (3) 3227-5264 English: +81-(3)-3227-5672 <i>+81 (3) 3227-5238</i>	09:00-17:00 (JST) <sup>b</sup>
Europe and Africa	Netherlands	europe_password@cnd.hp.com	+31 (55) 543 4642 <i>+31 (55) 543 4645</i>	09:00-18:00 (CET) <sup>c</sup>

- a. Mountain Standard Time (U.S.A.)
- b. Japanese Standard Time
- c. Central European Time

For further information, see the HP License Key Delivery Service web site:

**<https://webware.hp.com/>**

## Receiving License Passwords

You should receive your license password in one of two time frames:

- **Immediately (Internet)**

If you order a password on the HP License Center Internet site, you receive a license password immediately.

- **Within 48 hours (mail, fax)**

If you order a password by mail, fax, or phone, you receive a license password within 48 hours of receipt from one of the Password Delivery Centers listed in [Table 4](#) on page 172.

You receive your password in one of three ways:

- **Email**

If you provide an email address on your request form, you receive your password by email.

- **Fax**

If you do not specify an email address, you receive your password by fax.

- **Phone**

If you do not specify either a fax number or an email address, you receive your password by phone.

## Installing Product Licenses



The HPOM DMA installation on the selected Windows host system requires a valid licence. Remote HPOM host systems do not need an HPOM DMA licence.

To install the HPOM DMA product license using AutoPass, follow these steps:

- 1 Start AutoPass using the script or batch file appropriate for your operating system:

- *UNIX and Linux*

```
<InstallDir>/bin/startDmaLicenseUI.sh
```

- *Windows 32-bit*  
`<InstallDir>\bin\startDmaLicenseUI.bat`
  - *Windows 64-bit*  
`<InstallDir>\bin\win64\startDmaLicenseUI.bat`
- 2 From the AutoPass menu, select **Install/Restore Licences**.
  - 3 In the File path dialog box, click **Browse**.
  - 4 In the Browse dialog box, select **All Files** and browse to the license file to be installed and click **Install**.

## Verifying Product Licenses

You can verify licenses using the AutoPass License Report tool. It provides information on the installed passwords.

To verify the HPOM DMA product license, follow these steps:

- 1 Start AutoPass using the script or batch file appropriate for your operating system:
  - *UNIX and Linux*  
`<InstallDir>/bin/startDmaLicenseUI.sh`
  - *Windows 32-bit*  
`<InstallDir>\bin\startDmaLicenseUI.bat`
  - *Windows 64-bit*  
`<InstallDir>\bin\win64\startDmaLicenseUI.bat`
- 2 From the AutoPass menu, select **Licences Report**.
- 3 Verify that the license you have installed is listed.

---

# 11 Securing

The following features are available to make working with HPOM DMA more secure:

- Configure secure web service communication between HPOM DMA and HPOM with SSL configuration.
- Restrict IIS access to a single port by linking Tomcat and IIS using the JK Connector.
- Grant access to users' LDAP authentication.

# Configuring Secure Communication between HPOM DMA and HPOM

HPOM DMA web service clients by default use SSL HTTP to communicate with the HPOM web services. Also by default, HPOM DMA web service clients trust *all* certificates issued from HPOM management servers in the environment.

You can change the following aspects of the default setup:

- Continue to use SSL HTTP but configure HPOM DMA to trust selected management servers only.

Perform the following high-level steps:

- a Manually export certificates on each HPOM management server with which you want to communicate.

For instructions, see [Exporting Certificates on HPOM for UNIX or Linux Management Servers](#) on page 177 or [Exporting Certificates on HPOM for Windows Management Servers](#) on page 180.

- b Manually import the certificates on the HPOM DMA client systems and update the *connection* settings in the HPOM DMA console.

For instructions, see [Importing Certificates in HPOM DMA](#) on page 183.

- c Manually import the certificates on the UCMDDB or BAC systems and update the *discovery* settings in UCMDDB or BAC.

For instructions, see [Restricting Service Synchronization to Managed Nodes](#) on page 149.

- Configure HPOM DMA, HPOM, and UCMDDB or BAC to use HTTP.

Perform the following steps:

- a Configure the web server on the HPOM management server to use non-SSL HTTP.

For instructions, see [Configuring Tomcat for non-SSL HTTP](#) on page 179 or [Configuring IIS for non-SSL HTTP](#) on page 182.



- b In the Connection page in the HPOM DMA console (or in the `DefaultSyncTask.settings` file), change the URL to use the HTTP protocol and port of the server as follows:

- *UNIX and Linux*

`http://<HPOM_host>:8081/ConfigurationItem/`

- *Windows*

`http://<HPOM_host>:80/omws/ConfigurationItem.svc`

In this URL, depending on your setup, `<HPOM_host>` can be `localhost`, the short hostname, or the fully qualified domain name of the HPOM host system.

- c In the Connection page, test the connection, and then click **Save**.

- d Update the *discovery* settings in UCMDB or BAC to use HTTP.

For instructions, see [Restricting Service Synchronization to Managed Nodes](#) on page 149.

## Exporting Certificates on HPOM for UNIX or Linux Management Servers

To export server certificates for use by clients, follow these steps:

- 1 Go to the directory containing the Tomcat keystore file:

```
cd <DataDir>/certificates/tomcat/b
```

- 2 List the certificates contained in the keystore using the Java keystore tool (`keytool`):

```
<InstallDir>/nonOV/jre/b/bin/keytool -list -keystore  
tomcat.keystore
```

- 3 Enter the keystore password. If the password is not known just press return when prompted.

The following output is displayed:

```
***** WARNING WARNING WARNING *****  
* The integrity of the information stored in your keystore *  
* has NOT been verified! In order to verify its integrity, *  
* you must provide your keystore password. *  
***** WARNING WARNING WARNING *****
```

```
Keystore type: jks
Keystore provider: SUN
```

Your keystore contains 1 entry

```
ovtomcatb, Feb 25, 2009, keyEntry,
Certificate fingerprint (MD5):
96:C6:07:A8:11:02:9E:D4:99:CB:BF:07:39:22:00:69
```

- 4 Export the Tomcat server certificate using `keytool`, and specify the alias name obtained from the listing, for example, `ovtomcatb`:

```
<InstallDir>/nonOV/jre/b/bin/keytool -keystore
tomcat.keystore -export -alias ovtomcatb -file /tmp/
server.cer
```

- 5 Enter the keystore password. If the password is not known just press return when prompted.

The following output is displayed:

```
Certificate stored in file <server.cer>
```

The certificate is saved to the specified file in a format that can be imported into a Java keystore file for use by the HPOM DMA Gateway and Smart Message Mapper client applications.

- 6 Specify the location of the keystore file in the HPOM configuration settings:

```
ovconfchg -ovrg server -ns wsman.client -set ssl.keystore
"location of <client.keystore> file"
```

```
ovconfchg -ovrg server -ns wsman.client -set ssl.keystore
/var/opt/OV/shared/server/certificates/dma/
client.keystore
```

- 7 Restart the Tomcat server using the commands:

```
ovc -stop ovtomcatB
ovc -start ovtomcatB
```

To configure the client to use SSL, see [Importing Certificates in HPOM DMA](#) on page 183.

## Securing Clustered Systems with SSL

To provide SSL communication through the virtual IP address of a cluster, you must use an SSL certificate for Tomcat that is issued for the virtual IP of that cluster. For example, if your cluster consists of the hosts `hostA` and `hostB`, and is accessible externally using a virtual IP `hostV`, a certificate must be issued for `hostV`.

Also make sure that the URL of the HPOM management server web service uses the virtual IP of the cluster (for example, **`http://hostV:80/...`**) and not `localhost`.

## Configuring Tomcat for non-SSL HTTP

To configure Tomcat to run a non-SSL HTTP connector, follow these steps:

- 1 Open the following file for editing:

```
<InstallDir>/nonOV/tomcat/b/conf/server.xml.ovtemplate
```

- 2 Uncomment the connector port specification from the following section:

```
<!-- Define a non-SSL HTTP/1.1 Connector on port 8081 -->
<!--@ENABLESTANDALONEHTTP@
<Connector port="@STANDALONESERVERPORTFORHTTP@"
maxHttpHeaderSize="8192"
maxThreads="150"
minSpareThreads="25"
maxSpareThreads="75"
enableLookups="false"
redirectPort="@STANDALONESERVERPORTFORHTTPS@"
acceptCount="100"
connectionTimeout="20000"
disableUploadTimeout="true" />
@END_ENABLESTANDALONEHTTP-->
```

It should appear as follows:

```
<!-- Define a non-SSL HTTP/1.1 Connector on port 8081 -->
@ENABLESTANDALONEHTTP@
<Connector port="@STANDALONESERVERPORTFORHTTP@" maxHttpHeaderSize="8192"
maxThreads="150"
minSpareThreads="25"
maxSpareThreads="75"
enableLookups="false"
redirectPort="@STANDALONESERVERPORTFORHTTPS@"
acceptCount="100"
```

```
connectionTimeout="20000"  
disableUploadTimeout="true" />  
@END_ENABLESTANDALONEHTTP@
```

- 3 Save and close the file.
- 4 Upload the changes to the template with the command:  
**<InstallDir>/nonOV/tomcat/b/bin/ovtomcatbctl -configure**
- 5 Restart the Tomcat server using the commands:  
**ovc -stop ovtomcatB**  
**ovc -start ovtomcatB**

## Exporting Certificates on HPOM for Windows Management Servers

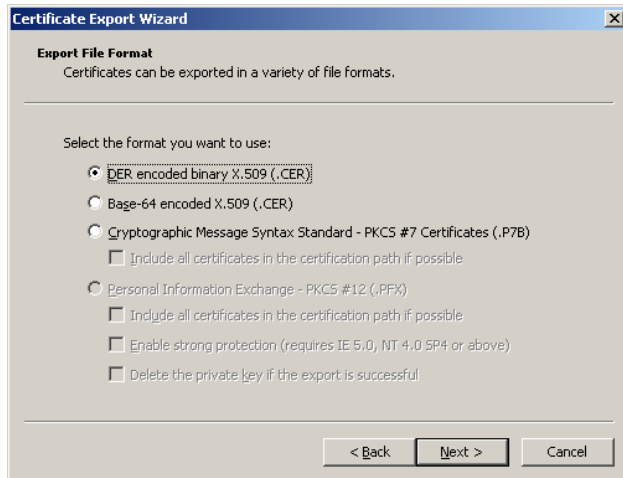
To export server certificates for use by web service clients, follow these steps from the Internet Information Services (IIS) Manager control panel:

- 1 Navigate to the `omws` entry in the Default Web Site folder:  
**<hostname> → Web Sites → Default Web Site → omws**
- 2 Open the Directory Security tab in the Properties dialog box:  
Right-click **Default Web Site**, select **Properties**, and open the **Directory Security** tab.
- 3 From the Secure Communications section, click **View Certificate**.  
The Certificate dialog box opens.
- 4 Select the **Details** tab.
- 5 Click **Copy to File**.
- 6 Click **Next**.

- 7 Select **No**, do not export the private key and click **Next**.



- 8 Select the format **DER encoded binary X.509 (.CER)** and click **Next**.



- 9 Enter a file name to hold the certificate:  
Example:  
C:\OMWServerCertificate.cer and click **Next**.
- 10 Click **Finish** and then **OK**.

The certificate is saved to the specified file in a format that can be imported into a Java keystore file for use by the HPOM DMA gateway and Smart Message Mapper client applications.

To configure the client to use SSL, see [Importing Certificates in HPOM DMA](#) on page 183.

## Configuring IIS for non-SSL HTTP

To switch IIS to use a non-SSL HTTP connection, create a server certificate and configure the web services to use non-SSL HTTP:

- 1 Open the Internet Information Services (IIS) Manager control panel:

**Start** → **Control Panel** → **Administrative Tools** → **Internet Information Services (IIS) Manager**

- 2 Navigate to the Default Web Site:

**<hostname>** → **Web Sites** → **Default Web Site**

- 3 Open the Directory Security tab in the Properties dialog box:

Right-click **Default Web Site**, select **Properties**, and open the **Directory Security** tab.

- 4 Install a server certificate (or select an existing certificate):

- a From the Secure Communications section, click **Server Certificate**.

- b Follow the steps of the Web Server Certificate Wizard.

Alternatively, you can use tools like `SelfSSL` from the IIS Resource kit to install a self-signed server certificate.

- 5 Open the file for editing from the following location:

`<InstallDir>\www\webapps\omws\web.config`

- 6 In the bindings section, change each instance of the XML element name `httpsTransport` to `httpTransport`.

- 7 Save the file.

- 8 Restart the Default Web Site in IIS:

Right-click **<hostname>** → **All Tasks** → **Restart IIS**

## Importing Certificates in HPOM DMA

To import certificates in HPOM DMA:

- 1 In the Connection page in the HPOM DMA console (or in the `DefaultSyncTask.settings` file), change the URL to use the HTTPS protocol and the SSL port of the HPOM host as follows:

- *UNIX and Linux*

```
https://<HPOM_host>:8444/ConfigurationItem/
```

- *Windows*

```
https://<HPOM_host>:443/omws/ConfigurationItem.svc
```

In the URL, `<HPOM_host>` must correspond to the HPOM host system as listed in the server certificate. `<HPOM_host>` usually takes the form of the fully qualified domain name.

The following entry in the HPOM DMA synchronization log file indicates that `<HPOM_host>` is specified incorrectly:

```
Apr 24, 2009 1:07:18 PM;
675230;12;com.hp.ov.om.dma.sync.test.connection.HttpRequest;
getResponseCode;com.hp.ov.om.dma.common;WARNING;
Error while opening a connection to 'https://example/omws/
ConfigurationItem.svc/v1/service/Root_Services'.
HTTPS hostname wrong: should be <example>
```

The log file entry indicates that the web services client is configured to connect to the HPOM host system `example` using the short hostname. However the connection is not successful, probably because the HPOM host system is listed in the server certificate with its fully qualified domain name. Change the URL in the Connection page to `https://example.hp.com:443/omws/ConfigurationItem.svc`.

- 2 In the Connection page, clear **Trust all SSL certificates** and click **Save**.
- 3 *Optional*. Check if the client keystore already exists:

```
<InstallDir>/nonOV/jre/b/bin/keytool -list -keystore
<SharedDir>/server/certificates/dma/client.keystore
```

The default location is:

```
<SharedDir>/server/certificates/dma/client.keystore
```

- 4 Check if the location of the keystore file is already defined in HPOM:

```
ovconfget -ovrg server wsman.client ssl.keystore
```

If the location is already defined and you want to store the client keystore file in the same location, continue with [step 6](#).

If the location is not yet defined or if you want to use a different location, continue with [step 5](#).

- 5 Specify the location of the client keystore file in the HPOM configuration settings:

```
ovconfchg -ovrg server -ns wsman.client -set ssl.keystore  
"<location of client.keystore file>"
```

For example:

```
ovconfchg -ovrg server -ns wsman.client -set ssl.keystore  
"<SharedDir>/server/certificates/dma/client.keystore"
```

- 6 Get a copy of the server certificate exported on the HPOM server. See [Exporting Certificates on HPOM for UNIX or Linux Management Servers](#) on page 177 or [Exporting Certificates on HPOM for Windows Management Servers](#) on page 180 for details.

- 7 Copy the server certificate file `ServerCert.cer` to the directory:

```
<SharedDir>/server/certificates/dma
```

If this directory does not exist, create it.

- 8 Import the server certificate into the Java keystore file for the client:

```
<InstallDir>/nonOV/jre/b/bin/keytool -import -file  
<SharedDir>/server/certificates/dma/serverCert.cer  
-keystore <SharedDir>/server/certificates/dma/  
client.keystore
```

- 9 Select and enter a password for the keystore.

- 10 When asked to trust this keystore, enter **yes**.



- 11 Stop and restart the Tomcat server and all other processes dependent on the Tomcat server using the commands:

```
ovc -stop ovtomcatB
```

```
ovc -start
```



If you want to use an SSL connection to LDAP or UCMDB, you also need to import their respective certificates into the client keystore. In this case, follow the import instructions in [step 8](#) on page 184, using the certificates of your LDAP server or UCMDB server as appropriate.

- 12 Test the connection from the Connections page of the HPOM DMA console. If the connection test is successful, the configuration is complete and correct.

# Restricting IIS Access to a Single Port

The JK Connector can be used to provide a single port of entry for IIS and Tomcat services using port redirection for HPOM DMA Configuration web pages.

## Setting Up a Distributed System

To set up a distributed system consisting of an outward facing IIS web server and an internal HPOM DMA installation hosted on Tomcat, complete the following procedure:

- 1 Download the `isapi_redirect.msi` connector installer package from:

**<http://archive.apache.org/dist/tomcat/tomcat-connectors/jk/binaries/win32/jk-1.2.15/>**



You must use the JK Connector. The JK2 Connector is obsolete.

- 2 Extract the package and execute the installer. Further information can be found at:

**<http://tomcat.apache.org/connectors-doc/miscellaneous/faq.html>**

The installer creates a folder structure containing a few files, sets some registry entries, creates an IIS virtual directory, and adds the `isapi_redirect.dll` to the IIS web site ISAPI filters tab.

- 3 Add a Web Service Extension as follows. This must be done manually because the installer works for IIS 5 and 6, but Web Service Extension applies only to IIS 6.

- a Open the Internet Information Services console:

**Start → Administrative Tools → Internet Information Services (IIS) Manager**

- b In the tree on the left, expand the web server that is running on the local computer and click **Web Service Extensions**.

In general this tree lead is called `<nodename>` (local computer).

- c In the right hand pane, click **Add a new Web Service Extension**.

- d For the Extension Name, enter **Jakarta Tomcat** and click **Add**.

- e Browse and select:  
`<drive>:\Program Files\Apache Software Foundation\Jakarta Isapi Redirector\bin\isapi_redirect.dll`
- f Click **OK**.
- g Select the Set Extension status to Allowed check box.
- h Click **OK**.

The installer looks for a Tomcat listener on localhost.

- 4 Add the HPOM DMA context. The following assumes a default HPOM DMA install, with your application in:

**`http://<your-host>:8081/hpdma/`**

## Adding the HPOM DMA Context

To add the HPOM DMA context, follow these steps:

- 1 On the IIS web server, open the following file in an editor:

`C:\Program Files\Apache Software Foundation\Jakarta Isapi Redirector\conf\uriworkermap.properties`

In the # [URL]=[Worker name] section, add this line:

**`/dma/*=w1b`**

- 2 Save the file.
- 3 Restart the IIS Admin services from:  
**Start → Administrative Tools → Services**
- 4 Test the connector with HPOM DMA using the following URL:

**`http://<your-host>:8081/hpdma`**



Omit the port 8081. The default port 80 is then used.

If you want to block remote access to port 8081 on Tomcat completely, complete the procedure described in [Restricting Access to Localhost](#) on page 188.

## Restricting Access to Localhost

It is often desirable to restrict access to Tomcat's web application to specified host names or IP addresses only. Only clients at those specified sites are then served content. Tomcat incorporates two valves that you can configure and use for this purpose:

- RemoteHostValve
- RemoteAddrValve

These valves enable you to filter requests by host name or by IP address, and to allow or deny hosts that match. If you run HPOM DMA, you may want to allow access to it only from the localhost. This can be achieved by using the following statement:

```
<Context path="/path/to/secret_files" ... >
  <Valve className="org.apache.catalina.valves.RemoteAddrValve?"
    allow="127.0.0.1" deny=""/>
</Context >
```

If no `allow` attribute pattern is specified, all requests that match the `deny` attribute patterns are rejected, and all others are allowed. Similarly, if no `deny` attribute pattern is specified, requests that match the `allow` attribute patterns are allowed, and all others are denied.

## Change the Tomcat Server AJP Port

If the Tomcat server AJP port used for the HPOM DMA installation has been changed, for example, if a port conflict occurs, an alternative port must be specified.

To specify an alternative port, follow these steps:

- 1 Open the following file for editing:

```
<InstallDir>\nonOV\tomcat\b\server.xml.ovtemplate
```

- 2 Find the section that defines the AJP 1.3 Connector:

```
<!-- Define an AJP 1.3 Connector on port 8010 -->
<!--
<Connector port="8010"
  redirectPort="8444"
  enableLookups="false" debug="0" protocol="AJP/1.3" />
-->
```

- 3 Remove the comment marks around the port specification lines and make a note of the connector port value:

```
<!-- Define an AJP 1.3 Connector on port 8010 -->  
  
<Connector port="8010"  
    redirectPort="8444"  
    enableLookups="false" debug="0" protocol="AJP/1.3" />
```

- 4 Edit the file:

```
<drive>:\Program Files\Apache Software Foundation\Jakarta  
Isapi Redirector\conf\workers.properties.minimal
```

- 5 Change the following line:

— From:

```
worker.ajp13w.port=8009
```

— To:

```
worker.ajp13w.port=<AJPPort>
```

In the example, *<AJPPort>* is the port value (8010) you noted in step 3.

- 6 Save the file.
- 7 Restart the IIS Admin services from:

**Start → Administrative Tools → Services**

# LDAP Authentication

HPOM DMA supports authentication using LDAP. Consult your LDAP administrator to gather the configuration values required by HPOM DMA. The values are:

- **Host name or IP address of the LDAP server**  
`ldap.server.address=<DNS_or_IP_Address_LDAP_Server>`
- **Port on LDAP server**  
`ldap.server.port=<Network_Port_LDAP_Server>`
- **Protocol prefix for LDAP connection**  
`ldap.server.protocol=<Protocol_ldap_or_ldaps>`
- **Root of LDAP schema**  
`ldap.schema.root=o\=<LDAP_root>`
- **Branch containing user entries in the LDAP schema**  
`ldap.schema.people=ou\=<Users_branch>`
- **Branch containing group entries in the LDAP schema**  
`ldap.schema.groups=ou\=<Groups_branch>`
- **Canonical name attribute for groups**  
`ldap.schema.group.cn.identifier=<Common_name_identifier>`
- **Distinguished name attribute for users**  
`ldap.schema.user.dn.identifier=<Distinguished_name_identifier>`
- **Allowed groups definition**  
`ldap.allowed.groups=<GROUP_Name1>;<GROUP_Name2>;...`

The LDAP configuration values are stored in the `ldap.properties` file, which is located at:

```
<SharedDir>/server/conf/dma/ldap.properties
```

An example of this file is illustrated in [Configuring LDAP Access](#) on page 193.

[Figure 23](#) on page 192 shows a typical LDAP schema.



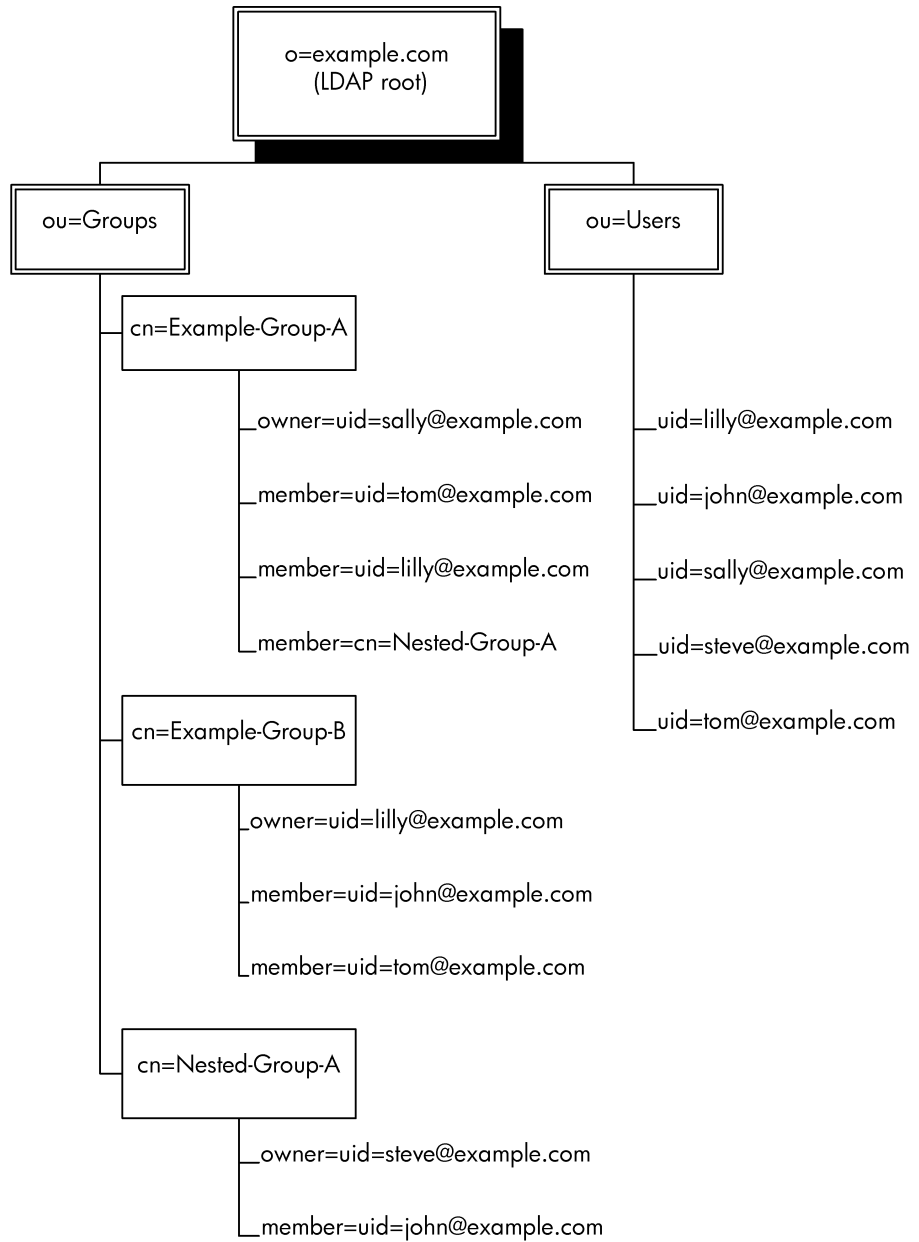
If configuring SSL protected LDAP (ldaps), download the LDAP server certificate and import it into the client.keystore and restart the Tomcat server.

To import the LDAP server certificate into the Java keystore file, execute the following command:

```
<InstallDir>/nonOV/jre/b/bin/keytool -import -file  
<Downloaded_LDAP_Server_Certificate> -keystore <DataDir>/  
certificates/dma/client.keystore
```

If the keystore file does not exist, it is generated.

**Figure 23 A Sample LDAP Schema**





## Configuring LDAP Access

To configure LDAP access, you must modify the `ldap.properties` file as follows:

- 1 Open the `<SharedDir>/server/conf/dma/ldap.properties` file for editing:

```
# Defines the host name or IP address of the LDAP server
# example: ldap.example.com
ldap.server.address=192.168.1.1
# Defines the LDAP server's port and protocol prefix
# Defaults are: 389 & ldap for non-SSL
#                 636 & ldaps for SSL
ldap.server.port=636
ldap.server.protocol=ldaps
# Defines the LDAP schema's root
# Examples: o\=com
#           o\=example.com
ldap.schema.root=o\=example.com
# Defines the LDAP schema's branch containing user entries
# Examples: ou\=example
#           or dc\=Users
ldap.schema.people=ou\=Users
# Defines the LDAP schema's branch containing group entries
# Examples: ou\=groups
#           or dc\=Groups
ldap.schema.groups=ou\=Groups
# Defines the groups' canonical name attribute
ldap.schema.group.cn.identifier=cn
# Defines the users' distinguished name attribute
# Example: uid\=\{0\}
ldap.schema.user.dn.identifier=uid\=\{0\}
# Defines the allowed LDAP groups
# Multiple groups are separated by semicolons
ldap.allowed.groups=Example-Group-A;Example-Group-B;
Example-Group-E
```

- 2 Specify the LDAP configurations that are appropriate for your implementation. The example in [Figure 23](#) is reflected in the `ldap.properties` configuration file.

- ▶ Equal signs (=) and accolades must be escaped with a backslash (\) in the `ldap.properties` file, as shown in the `ldap.properties` file example, because of character encoding in ISO 8859-1.

When specifying allowed groups definitions, do not use spaces before, after, or within group names. In the following example, the first group cannot be recognized, but the second is correctly specified:

```
ldap.allowed.groups= Example Group A;Example-Group-B;
```

- 3 Save and close the `ldap.properties` file.
- 4 Specify the location of the keystore file in the HPOM configuration settings:

```
ovconfchg -ovrg server -ns wsman.client -set ssl.keystore  
"location of <client.keystore> file"
```

— *UNIX and Linux*

```
ovconfchg -ovrg server -ns wsman.client -set  
ssl.keystore /var/opt/OV/shared/server/certificates/  
dma/client.keystore
```

— *Windows*

```
ovconfchg -ovrg server -ns wsman.client -set  
ssl.keystore "C:/ProgramData/HP/HP BTO Software/  
shared/server/certificates/dma/client.keystore"
```

- 5 Restart the Tomcat server to activate the modified LDAP settings:

```
ovc -stop ovtomcatB  
ovc -start
```

- ▶ Only group members and not group owners can be authenticated with this release.

## Logging In Using LDAP Authentication

Using LDAP, you must enter the LDAP Uid (user's distinguished name identifier), as specified in the `ldap.properties` file, as your user name. In the example, a user logon is `sally@example.com`.



# 12 Backup, Restore, and Migration

It is possible to make a copy of an existing HPOM DMA setup (tasks, synchronization packages, and connection information) from an existing HPOM DMA installation to another installation. This process can be used for simple copies as well as for backup and restore. It is also applicable to cases where individual synchronization packages need to be migrated.

- ▶ Before starting a migration, make sure that you have installed HPOM DMA on an alternative HPOM host system running the same operating system as the source system.

Backing up, restoring, and migrating HPOM DMA installations does not manage data synchronized from the UCMDB or BAC. Likewise, it does not back up information available within HPOM.

A separate license is required for the alternative HPOM host system.

## Backing Up an HPOM DMA Configuration

To back up the HPOM DMA configuration, copy the following directory and all of its contents from the source system to an alternative, secure location:

`<SharedDir>/server/conf/dma`

**Example:**

```
C:\Documents and Settings\All Users\Application Data\HP\
HP BTO Software\shared\server\conf\dma
```

# Backing Up HPOM DMA TQL Queries

Backing up HPOM DMA TQL queries requires you to create a new package containing the existing UCMDB resources (views and enrichments) being used by HPOM DMA.

To back up your TQL queries and enrichments, follow these steps:

- 1 Open the Package Manager:
  - *UCMDB 7 and 8*  
**Admin** → **Settings** → **Package Manager**
  - *UCMDB 9*  
**Administration** → **Package Manager**
  - *BAC*  
**Admin** → **Universal CMDB** → **Settings** → **Package Manager**
- 2 Create a backup package:
  - a Click **New**.  
The Create Custom Package wizard opens.
  - b Enter a name and description for the new package and click **Next**.
  - c Expand **Query** → **TQLs** → **Enrichment** and check `hpdma`.
  - d Expand **Query** → **TQLs** → **View** and check `hpdma`.
  - e Expand **Query** → **Views** and check `hpdma`.
  - f Expand **Query** → **Enrichments** and check `hpdma`.
  - g Click **Next**.
  - h A summary of the selections that you have made is displayed.
  - i Click **Finish**.

# Restoring the Default HPOM DMA Configuration

To restore the default HPOM DMA configuration:

- 1 Copy the default data from the storage directory:

```
<InstallDir>/newconfig/DataDir/conf/dma
```

**Example:**

```
C:\Program Files\HP\HP BTO  
Software\newconfig\DataDir\conf\dma
```

- 2 Place the default data into the configuration directory:

```
<SharedDir>/server/conf/dma
```

**Example:**

```
C:\Documents and Settings\All Users\Application Data\HP\  
HP BTO Software\shared\server\conf\dma
```

# Moving an HPOM DMA Configuration

To move an HPOM DMA configuration, follow these steps:

- 1 *Optional.* Back up the existing configuration.

Copy the following directory and all of its contents on the source system to an alternative location:

```
<SharedDir>/server/conf/dma
```

Example:

```
C:\Documents and Settings\All Users\Application Data\HP\
HP BTO Software\shared\server\conf\dma
```

- 2 Make sure that the following location on the target system is empty:

```
<SharedDir>/server/conf/dma
```

- 3 Copy the existing configuration to the following location on the target system:

```
<SharedDir>/server/conf/dma
```

- 4 If you do not need the original installation any longer, delete the following directory and all of its contents from the source system:

```
<SharedDir>/server/conf/dma
```

- 5 Uninstall HPOM DMA. For further information, see [Chapter 13, Uninstalling](#).

## Recreate a Synchronization Package

It is possible to recreate an existing HPOM DMA setup (tasks, synchronization packages, and connection information) from an existing HPOM DMA installation to another installation. This process can be used for simple copies as well as for backup and restore operations. It is also applicable to cases where individual synchronization packages need to be migrated.





Before starting a move, make sure that you have installed HPOM DMA on an alternative HPOM host system running the same operating system as the source system.

You cannot transfer the data from an HPOM DMA installation on an HPOM for Windows system to an HPOM DMA installation on an HPOM for UNIX or Linux system.

## Make a Copy of a Synchronization Package

To move an HPOM DMA synchronization package configuration, follow these steps:

- 1 Copy the subdirectory used for the synchronization package configuration, for example, `myspi`, and all of its contents from the source system to the target system:

```
<SharedDir>/server/conf/dma/sync-packages/
```

Example:

- *UNIX and Linux*

```
/var/opt/OV/shared/server/conf/dma/sync-packages/
```

- *Windows 32-bit*

```
C:\Documents and Settings\All Users\Application  
Data\HP\HP BTO Software\shared\server\  
conf\dma\sync-packages\
```

- *Windows 64-bit*

```
C:\ProgramData\HP\HP BTO Software\shared\server\  
conf\dma\sync-packages\
```



All subdirectory names must be unique. You may need to rename synchronization packages when copying subdirectories to the directory:

```
<SharedDir>/server/conf/dma/sync-packages/
```

- 2 Make sure that the name in the `bundle.xml` file for the relocated synchronization package is unique and preferably matches the name of the synchronization package.

Example:

```
<Name>My_Application</Name>
```

- 3 Include the relocated synchronization package to be synchronized from the Synchronization page on the target system.

# 13 Uninstalling

Uninstalling HPOM DMA consists of two procedures:

- [Uninstalling HPOM DMA](#)
- [Post-Uninstallation Cleanup](#) on page 206

## Uninstalling HPOM DMA



Applications are stopped and restarted by the HPOM DMA application installation process during installation, uninstallation, and repair. For detailed instructions, see [Applications Stopped and Restarted During Installation](#) on page 64

To delete the installed HPOM DMA components from the system:

1 Start the HP Software Installer:

- *UNIX and Linux*

Execute the following command:

```
/opt/OV/Uninstall/HPDma/setup.bin
```

- *Windows*

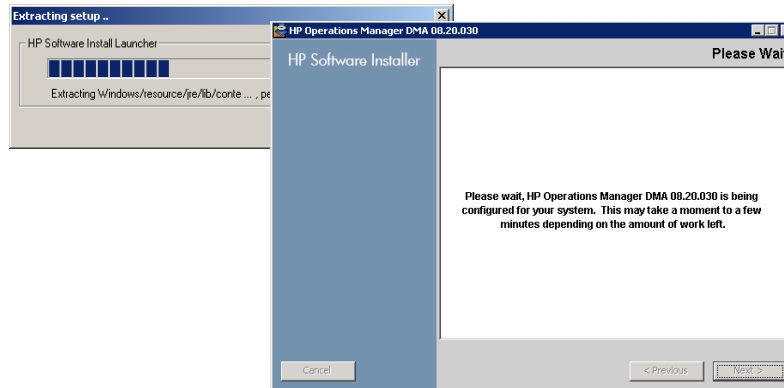
Select one of the following options:

- Select the program:

**Control Panel** → **Add or Remove Programs** → **HP Operations Manager Dependency Mapping Automation** and click **Change/Remove**.

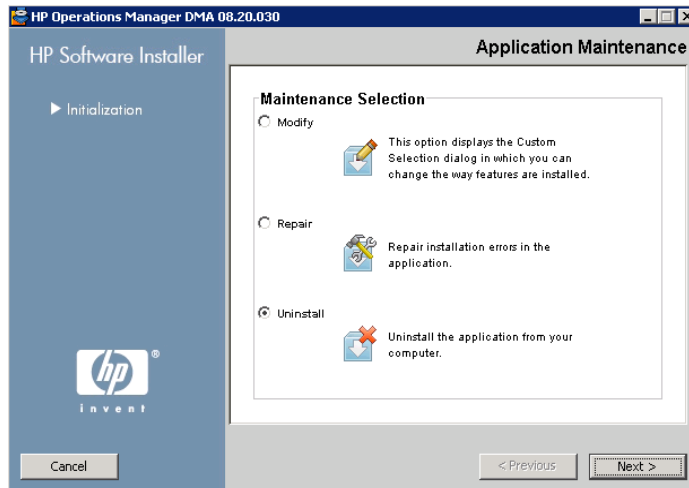
- Execute the following command:

```
<InstallDir>/Uninstall/HPDma/setup.exe
```



- 2 Select **Uninstall** and click **Next**.

Follow the on screen instructions and progress through the installation process using the **Next** and **Uninstall** buttons.



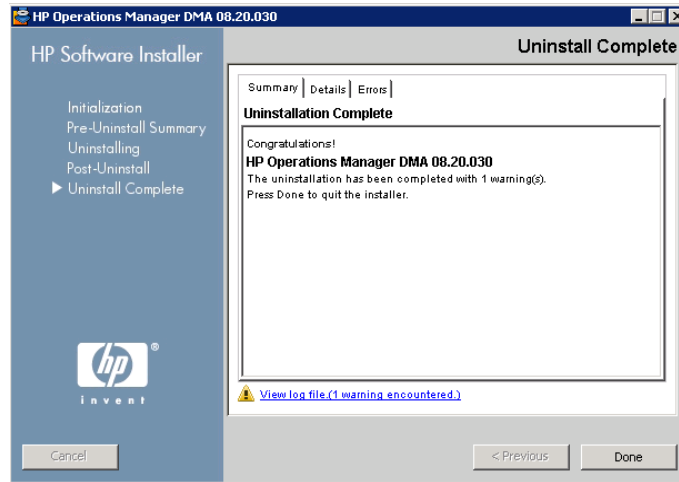
- 3 After the uninstallation process is finished, the Uninstall Complete window opens showing a summary of the uninstallation paths used.

You can also access the uninstallation log file from the link in this window and open it in a web browser.

The removed packages are listed under the **Details** tab.

If any errors occurred during the Uninstallation, they are summarized under the **Errors** tab.

- 4 Click **Done** to close the installation program.



Now go to the [Post-Uninstallation Cleanup](#) on page 206 to complete the HPOM DMA uninstallation.

# Post-Uninstallation Cleanup

If you want a completely clean system, you must remove a number of files and directories from the HPOM and UCMDB or BAC systems. Follow these instructions to complete your cleanup.



If you are sure that you no longer need any HPOM DMA personalized configurations, delete the HPOM DMA configuration files. After these files are removed, reinstalling HPOM DMA reverts to the default configuration files. If in doubt, retain these files or create a backup copy in a safe location.

## Removing the HPOM DMA Synchronization Packages and Configuration Files

Remove the following HPOM DMA directory. It contains the synchronization packages and some configuration files (for example `ldap.properties` and `users.properties`):

```
<SharedDir>/server/conf/dma
```

## Removing the HPOM DMA Data Files

Remove the following HPOM DMA directory. It contains the HPOM DMA data files:

```
<SharedDir>/server/datafiles/dma
```

## Removing Log Files



All log files not mentioned in the following sections are shared with other HP products and should not be deleted.

- **HPOM Web Service Log Files**

Remove the following log files:

- *UNIX and Linux*

```
<SharedDir>/server/log/om/ciws.<*>.<locale>
```

— *Windows*

`<SharedDir>\server\log\om\ws.trace.txt`

• **Synchronization and Smart Message Mapper Log Files**

Remove the following directory and all of its contents:

— *UNIX and Linux*

`<SharedDir>/server/log/dma`

**rm -rf <SharedDir>/server/log/dma**

`<SharedDir>/server/log/om`

**rm -rf <SharedDir>/server/log/om**

— *Windows*

`<SharedDir>\server\log\dma`

• **HPOM DMA Web Console (CWC) Log Files**



Remove only if no other application is running in the CWC web UI.

Remove the following log files:

— *UNIX and Linux*

`<DataDir>/tmp/cwc.log`

— *Windows*

`<InstallDir>/nonOV/tomcat/b/cwc.log`

• **Tomcat Server Log Files**



Remove only if no other application is using the Tomcat server.

Remove the following log files:

`<DataDir>/log/tomcat/ovtomcatb.out`

- **Installation Log Files**

Remove the following log files:

- *UNIX and Linux*

`/var/tmp/HPDma_<version>_HPOvInstaller.txt`

`/var/tmp/HPOvInstaller/HPDma_<version>/*`

- *Windows*

`<drive>:\Documents and Settings\Administrator\  
Local Settings\Temp\HPOvInstaller\HPDma_<version>`

## Cleaning Up UCMDB or BAC

To clean up your UCMDB or BAC system, follow these steps:

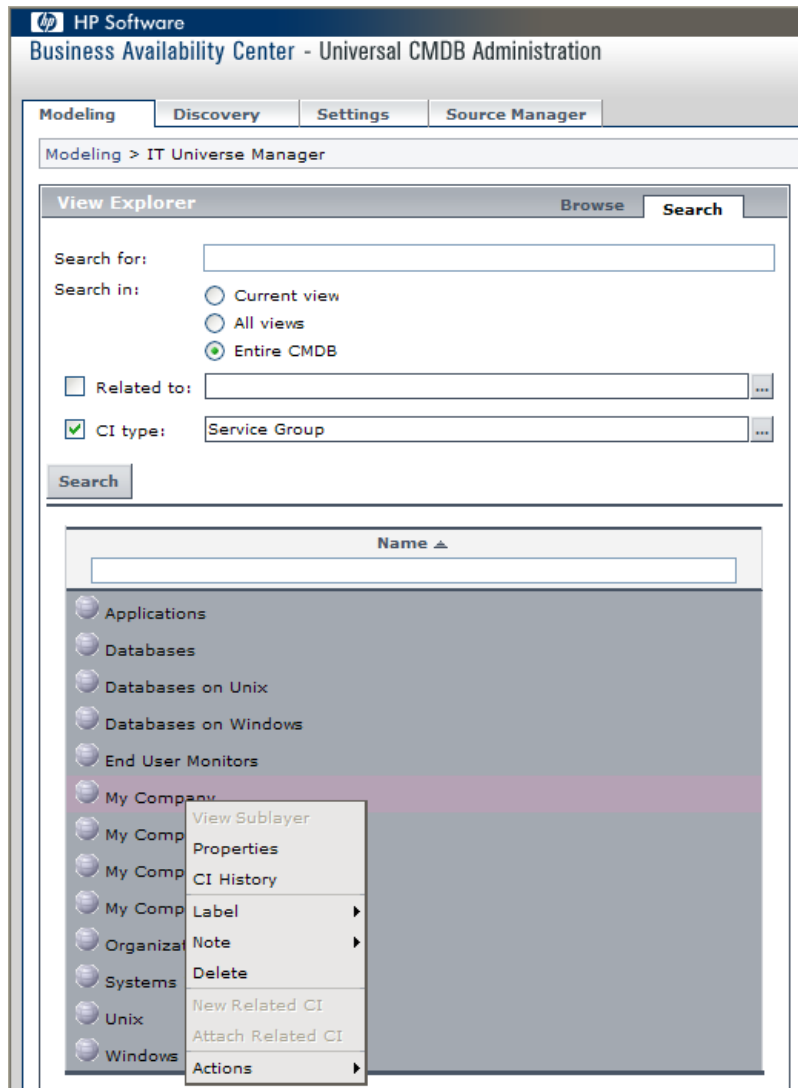
- 1 Open the Package Manager:
  - *UCMDB 7 and 8*  
**Admin → Settings → Package Manager**
  - *UCMDB 9*  
**Administration → Package Manager**
  - *BAC*  
**Admin → Universal CMDB → Settings → Package Manager**
- 2 If originally deployed, undeploy the optional synchronization packages:
  - `hpdmadb.zip` for databases
  - `hpdmaEUM.zip` for HP BAC End User Monitors
  - `hpdmaos.zip` for operating system
  - `hpdmasamples.zip` for the My Company Sample
  - `hpom.zip` for the Discovery Pattern for HPOM
- 3 Remove all instances of the CI type *Service Group* from UCMDB:
  - a Open the IT Universe Manager:
    - *UCMDB 7 and 9*  
**Admin → Settings → IT Universe Manager**



- *UCMDB 9*  
**Modeling** → **IT Universe Manager**
- *BAC*  
**Admin** → **Universal CMDB** → **IT Universe Manager**

- b Search for **CI type: Service Group**.  
Service Group is found under **Business**.
- c Select all returned items.
- d Right-click to open the shortcut menu.

- e Select **Delete**.



- 4 Delete all TQL queries, views, and enrichments that are related to the CI type Service Group. This includes any user-created TQL queries, views, and enrichments.

The `hpdmacore.zip` package can only be undeployed if all references in the TQL queries are removed.

- 5 Undeploy the `hpdmacore.zip` package.
- 6 Delete the `hpdmacore.zip` package and, if originally deployed, the any other optional package files.

## Cleaning Up HPOM for UNIX or Linux



Execute this procedure only if you no longer have HPOM DMA synchronized nodes and services in HPOM or if you have moved required nodes to alternative node groups.

To delete the nodes and services that have been imported by HPOM DMA, follow these steps:

- 1 Delete the CMDB root service and all its children.
- 2 Delete all nodes in the CMDB node group.
- 3 Delete all nodes in the CMDB\_removed node group.
- 4 Delete the HPOM the CMDB and CMDB\_removed node groups.
- 5 Delete the service type definitions.
- 6 Unassign the policy group Group OM DMA.
- 7 Undeploy the OM DMA policy group from the agent on the HPOM management server node

## Cleaning Up HPOM for Windows



Execute this procedure only if you no longer have HPOM DMA synchronized nodes and services in HPOM or if you have moved required nodes to alternative node groups.

### Deleting Imported Services

To delete the services that have been imported by HPOM DMA, follow these steps:

- 1 Open the Configure Services window:
  - a Right-click **Services** to open the shortcut menu.

**b Configure → Services**

- 2 Delete the `CMDB` service as follows:

Right-click the **CMDB** service and select **Delete** and **Yes**.

Click **OK** in the Configure Services window.

## Removing the OM DMA Policy Group

To remove the `OM DMA` policy group from the agent on the HPOM management server node, from HPOM UI, follow these steps:

- 1 Go to the `OM DMA` policy group:

**Policy management → Policy groups → OM DMA**

- 2 Right-click the **OM DMA** policy group and select **Delete** and **Yes**.

## Deleting HPOM DMA Node Groups

If you want to delete the HPOM DMA node groups, follow these steps:

- 1 Verify that any nodes that have been imported by HPOM DMA and that you want to continue to manage are moved to alternative node groups.
- 2 Delete the `CMDB` and `CMDB_removed` node groups and any nodes that are no longer required.

## Removing UI Launch Tools and Applications

If you originally installed and configured UI Launch, you can remove the following tools:

- Show Correlated CI Map
- Show Change Report
- Show Neighborhood Map
- Show Triage Report (BAC only)
- Show End User Monitors (BAC only)
- Show Service Impact (BAC only)

To remove the UI Launch tools, delete the Business Availability Center or Universal CMDB tool group in HPOM.

## Unconfiguring Smart Message Mapping

To unconfigure Smart Message Mapping, disable Server-based Message Stream Interface (Server MSI), if no other product is using MSI.

To disable Server MSI, use the following methods:

- **HPOM 8.xx for UNIX**  
Use the Configure Management Server window.
- **HPOM 9.xx for UNIX or Linux**  
Use the *opcsrvconfig(1M)* command-line tool.

## Resetting the Discovery Source to SPI Discovery

Resetting the discovery source requires you to complete one of the following tasks, appropriate for the operating system of the host system:

- [Resetting the Discovery on HPOM for UNIX or Linux](#) on page 213
- [Resetting the Discovery on HPOM for Windows Using the GUI](#) on page 214
- [Resetting the Discovery on HPOM for Windows Using XPL](#) on page 214

### Resetting the Discovery on HPOM for UNIX or Linux

To reset discovery from a SPI, follow these steps:

- 1 Modify the discovery tool and replace the command in the Tool Call field with the following, for example:  

```
/opt/OV/SPISvcDisc/bin/SPI_DiscServ.sh -v -f /opt/OV/lib/osspi/UnixOSSPI_Disc.conf -n "$OPC_NODES"
```
- 2 In the Parameters field, remove the parameter:  

```
-u false
```
- 3 Click **OK**.

- 4 Delete the service tree generated from the UCMDB discovery.

## Resetting the Discovery on HPOM for Windows Using the GUI

To reset discovery from a SPI, for example, with messages that start with the strings `OSSPI:`, follow these steps:

- 1 From the HPOM for Windows UI, go to:

**Tools** → **HP Operations Tools** → **Disable SPI Discovery**

- 2 Double-click the **Disable SPI Discovery** tool.

The Tool Status window and the Exclude Service Prefixes windows are opened.

- 3 In the Exclude Service Prefixes window, add the required statements. In the example, this is: **OSSPI:**

▶ If you are deleting statements, make sure that you delete the comma between the unwanted statements and the next one.

- 4 Click **OK**.

▶ If you select **Cancel**, a confirmation window opens with two portions.

- **OK** - All filter statements are deleted.
- **No** - Original filter statements are retained.

- 5 Delete the OSSPI service tree generated from the UCMDB discovery.

The XPL configuration can also be modified with the XPL configuration tools. For adding the filters to the configuration, use the `ovconfchg` command as described in [Resetting the Discovery on HPOM for Windows Using XPL](#).

## Resetting the Discovery on HPOM for Windows Using XPL

To enable discovery from a SPI with messages that start with the string `OSSPI:`, follow these steps:

- 1 Execute the following command:

```
ovconfchg -edit
```

The configuration file opens in an editor, for example, Notepad.

- 2 In the editor window, remove the OSSPI: from the following statement:

```
[DiscoveryServiceFilter]
```

```
Excludes=OSSPI:
```

- 3 Save the changes.
- 4 Delete the OSSPI service tree generated from the UCMDB discovery.

## Cleaning Up BPM Integration

Cleaning up the BPM Integration requires you to complete the following tasks:

- [Deleting CI Status Alerts](#) on page 215
- [Deleting Performance Limit Alerts](#) on page 215

### Deleting CI Status Alerts

To delete CI Status Alerts follow these steps in the BAC UI:

- 1 Open the CI Status Alerts tab:  
**Admin** → **Alerts** → **CI Status Alerts**
- 2 Select the End User Monitors view.
- 3 Delete the CI Alerts that you no longer need.

### Deleting Performance Limit Alerts

To delete Alerts on performance limits follow these steps in the BAC UI:

- 1 Open the Event Based Alerts Configuration page:  
**Admin** → **Alerts** → **Event Based Alerts** → **Event Based Alerts Configuration**
- 2 Select a business process profile from the **Profile:** drop-down list.
- 3 Delete the Event Based Alerts that you no longer need.





# 14 Performance and Configuration Tips

When synchronizing CI data from UCMDB or BAC to HPOM using HPOM, the following performance can be expected:

- **UNIX and Linux**

One percent change in 10,000 originally synchronized CIs (100 nodes with 100 services per node) requires approximately 3 minutes.

- **Windows**

One percent change in 10,000 originally synchronized CIs (100 nodes with 100 services per node) requires approximately 10 minutes.

The time necessary to add a new node depends on the available hardware and operating system information. If the information is provided by UCMDB, or if the node is accessible over the network, only a few seconds are needed. If the information is missing and the node is not reachable for a lookup, it can take 30 seconds depending on the network environment. When adding nodes, make sure that nodes are reachable. If nodes are shut down overnight, and information is not available from within UCMDB, reschedule adding nodes to a time when the majority of nodes are running.



Initial synchronization from UCMDB or BAC may take longer, especially on Windows installations. Initial synchronization of 10,000 CIs on the specified Windows reference system requires approximately 210 minutes.

These values have been achieved using multi-processor server systems. However, HPOM DMA requires only one processor.

- *HP-UX:*

HP ia64 Server rx2600 with 2 x Intel Itanium 2, 1300 MHz CPUs, 2 GB RAM running the HP-UX B.11.23 U operating system.

- *Windows:*

Intel Xeon Prestonia Server with 2 x 3.2 GHz CPUs, 4 GB RAM, running the Microsoft Windows Server 2003 R2 Enterprise Edition Service Pack 1 operating system.

To help minimize performance issues, you must create efficient mapping rules. See the *Mapping Basics* chapter in the *HPOM DMA Extensibility Guide* for guidance on how to write mapping rules correctly.

## Increasing Tomcat Server Memory

Synchronizing bigger hierarchies consumes a lot of memory during synchronization. If the log file contains `OutOfMemoryException` entries, increase the heap size. To prevent memory exceptions and native library errors, increase the maximum heap size of the Tomcat server:

To increase the heap size, follow these steps:

- 1 Stop the Tomcat server using the command:  

```
ovc -stop ovtomcatB
```
- 2 Change the heap size with the following command:  

```
ovtomcatbctl -setmaxheapsize <size of heap>
```
- 3 Restart the Tomcat server using the commands:  

```
ovc -start ovtomcatB
```

## Adding Missing Node Attribute

Make sure that the nodes imported from UCMDB or BAC are fully described using the following attributes:

- System type (for example, Alpha, and Itanium)
- OS type (for example, HP-UX, Solaris, and Windows)
- OS version (for example, B.11.11, and B.11.22)

This ensures that nodes can be brought under management as quickly as possible. If some of this information is missing, HPOM for Windows initiates a discovery to establish the missing values, which takes additional time.

Missing attributes are likely to be a problem of UCMDB or BAC discovery setup. Make sure those attributes are specified to be discovered by UCMDB or BAC and mapped appropriately by HPOM DMA.

## Changing XPL Configuration Parameters

Some XPL configuration parameters have an influence on performance and resource consumption. The parameters of interest are stored in the XPL Configuration under the resource group `server` and the name space `dma`.

To view the current settings, execute the command:

```
ovconfget -ovrg server dma
```

## Web Service Client

If log files show timeouts, increase the appropriate timeout setting, for example, `operation.timeout` or `enumeration.context.timeout`.

The client implementation uses the following parameters. These parameters can be changed with the command:

```
ovconfchg -ovrg server -ns wsman.client -set <parameter>  
<value>
```

### **operation.timeout**

Maximum permitted duration for one Web Service Operation (default is 5 minutes and the value is specified in milliseconds).

### **enumeration.context.timeout**

Maximum permitted duration for a complete enumeration (enumerate, pull, release). This is a suggestion from the client and could be overwritten by the server (default is 10 minutes and the value is specified in milliseconds).

### **bulkcreate.chunksize**

Maximum number of items to be sent in one chunk during a bulk create. Increasing this parameter should lead to better performance, but significantly increases memory consumption (default is 1000).

**enumeration.chunksize**

Maximum number of items to be retrieved in one chunk during an enumeration. Increasing this parameter should lead to better performance, but significantly increases memory consumption (default is 1000).

**ssl.keystore**

File name of the keystore where SSL certificates are stored. Only used for SSL default:

```
${OV_DATA}/shared/certificates/wsman/client.keystore
```

The following are examples of how to change these parameter values:

```
# ovconfchg -ovrg server -ns wsman.client -set  
operation.timeout 300000  
  
# ovconfchg -ovrg server -ns wsman.client -set  
enumeration.context.timeout 600000  
  
# ovconfchg -ovrg server -ns wsman.client -set  
bulkcreate.chunksize 1000  
  
# ovconfchg -ovrg server -ns wsman.client -set  
enumeration.chunksize 1000  
  
# ovconfchg -ovrg server -ns wsman.client -set ssl.keystore  
${OV_DATA}/shared/certificates/client.keystore
```

# Changing Non-XPL Configuration Parameters

Some non-XPL configuration parameters that have an influence on performance and resource consumption.

## HPOM for Windows Web Services

The maximum message size that the HPOM for Windows Web Service Server accepts can be configured in the file:

```
<InstallDir>\www\webapps\omws\web.config
```

The default maximum size is set to 50MB. If you want to change the maximum message size, in the `MyServiceBinding` binding, change the values of the following parameters as required:

- `maxReceivedMessageSize`
- `maxBufferSize`



The value of `maxBufferSize` must be equal to or greater than the value of `maxReceivedMessageSize`.

### Example:

```
<system.serviceModel>
  <bindings>
    <customBinding>
      <binding name="MyServiceBinding">
        <textMessageEncoding messageVersion="Soap12WSAddressingAugust2004" />
        <httpTransport authenticationScheme="Basic"
          maxReceivedMessageSize="52428800" maxBufferSize="52428800" />
      </binding>
    </customBinding>
  </bindings>
</system.serviceModel>
```

## Tomcat Server

Configurable parameters of the Tomcat server are configured using the `ovtomcatbctl` CLI. Help is available with `ovtomcatbctl -h` command.

OVTomcatB Control Script Usage is listed in [Table 5](#).

**Table 5 OVTomcatB Control Script Usage**

Option	Parameter
-adduri	<i>[-allowlinking]</i> <webapp_name> <webapp_path> <webapp_description> <webapp_workdir>
-disablehttp	—
-disablehttps	—
-checkport	<portnumber>
-configure	—
-enablehttp	—
-enablehttps	—
-getconf	—
-help	N/A
-removeuri	<webapp name>
-restart	—
-sethttpport	<portnumber>
-sethttpsport	<portnumber>
-setshutdownport	<portnumber>
-start	—
-status	—
-stop	—
-version	—
-setiniheapsize	<size of heap>
-setmaxheapsize	<size of heap>

# Changing the HPOM Web Service Credentials

After a synchronization is specified, the credentials for the HPOM Web Service interface are cached. Changing the credentials in the HPOM DMA console (Connections page) has no effect unless Tomcat is restarted.

To change the current credentials, follow these steps:

- 1 Change the credentials on the HPOM server.
- 2 Change the credentials on the HPOM DMA console.
- 3 Stop and start the Tomcat server:

```
ovc -stop ovtomcatB
ovc -start ovtomcatB
```

# Changing the Port of HPOM DMA Tomcat

After installation, the HPOM DMA console cannot be opened in a web browser. The Tomcat log file in `<DataDir>/log/tomcat/ovtomcatb.out` indicates that there is a conflict on port 8081.

There may be another program that is occupying this port. Change the other application's port and restart Tomcat, or change the port of the HPOM DMA Tomcat:

- 1 Change the port of the HPOM DMA Tomcat:

— UNIX and Linux

```
/opt/OV/nonOV/tomcat/b/bin/ovtomcatbctl -sethttpport
<New Port Number>
```

— Windows

```
<InstallDir>\nonOV\tomcat\b\bin\OvTomcatBCtrl.vbs
-sethttpport <New Port Number>
```

- 2 Stop Tomcat:

```
ovc -stop ovtomcatB
```

- 3 Start Tomcat and all processes that depend on Tomcat:

```
ovc -start
```

# Changing Log File Parameters

Logging can be controlled by adjusting the XPL parameters. Use the XPL utility **ovconfchg -edit** to set any of the following parameters. After setting the XPL configuration, you must restart the appropriate application, for example, `dmamsg` or `tomcat`.



The level parameter only affects HPOM DMA log files. It does not have any affect on the XPL system log file.

**Table 6**

<b>Parameter Name</b>	<b>Parameter Namespace</b>	<b>Default</b>	<b>Location and Name</b>
filecount	xpl.log.OvLogFileHandler	10	Specifies the maximum number of log files to maintain in the log file history.
filesize	xpl.log.OvLogFileHandler	1	Specifies the maximum number of megabytes a log file may contain before a switch-log is done.
level	xpl.log.OvLogFileHandler	INFO	Specifies the logging level of the OvLogFileHandler. Possible values are any of those supported by the Java logging facility. The levels in descending order are SEVERE, WARNING, INFO, CONFIG, FINE, FINER, and FINEST. Each level enables all logs made at its level and those above it. For example, level INFO includes all SEVERE, WARNING, and INFO logs. In addition there is a level OFF that can be used to turn off logging, and a level ALL that can be used to enable logging of all messages.



# Smart Message Mapping

Troubleshooting Smart Message Mapping includes the following guides:

- [Messages Mapped to Wrong Nodes](#) on page 225
- [No Messages are Mapped](#) on page 225

## Messages Mapped to Wrong Nodes

If messages are being mapped to the wrong node, send a test message with a dedicated service ID and node for the target service:

```
opcmsg a="app" o="obj" severity="warning"  
service_id="<key1>:<key2>:...@@<your node>" msg_t="test"
```

Make sure that the values for key1, key2, ... are attribute values of the target service.

If another service is still being colored, check if that service also has the same set of keys.

## No Messages are Mapped

Check that messages are being sent:

- 1 Disable MSI and send message to server.

Message should be visible in the message browser. If not, the problem is not related to HPOM DMA.

- 2 Check that Smart Message Mapping and HPOM web server is running.
- 3 Check that server-MSI is activated.
- 4 Restart Smart Message Mapping:

- a Open command line and execute:

```
ovc -stop dmamsg  
ovc -start dmamsg
```

- b Look into the HPOM Smart Message Mapper log files and check that Smart Message Mapping has resynchronized services:

```
Nov 28, 2007 8:45:33
AM;28;10;com.hp.ov.om.dma.smart.HpOmMessageMapper;init;co
m.hp.ov.om.dma.smart;INFO;**** OM DMA Smart Message
Mapping logging initialized ****Nov 28, 2007 8:45:33
AM;33;11;com.hp.ov.om.dma.smart.MessageRouter;sync;com.hp
.ov.om.dma.smart;INFO;Resynchronizing services.Nov 28,
2007 8:54:00
AM;2807;11;com.hp.ov.om.dma.smart.MessageRouter;sync;com.
hp.ov.om.dma.smart;INFO;Resynchronizing services done.
```

- 5 Send a test message and make sure that target node is set.
- 6 Check that services have a hosted on attribute set. Follow the steps in the Enrichment Simulator. Verify that the enriched data have the hosted on set correctly.

# Analyzing Synchronization Error Messages

The following errors can be identified by messages in the HPOM DMA log file:

- **TQL Not Found**

TQL queries are either not installed or not accessible in UCMDB.

- **Service Type Definition Missing in HPOM**

Either STDs have not been uploaded to HPOM, or a new type of object has been returned by the TQL queries in UCMDB.

- **CI could not be Saved due to Invalid Attribute Value**

Some characters, such as \, are not allowed for certain attribute types. The error message identifies the object and attribute. The character must be mapped in the attribute mapping.

- **Service or Node Already Exists**

A TQL query returns the same service or node multiple times because different discovery sources have added the same object to UCMDB (for example, `testnode.example.com` and `TESTNODE`). The query must be adapted or the data in UCMDB must be rationalized.

# Analyzing LDAP Configuration Errors

The following are common LDAP problems:

- **Unreachable LDAP Server**

The LDAP server is not reachable from the host, and the port number or the protocol prefix do not match.

Defaults (RFC): ldap + 389, ldaps + 636

- **Specify Correct Branches**

Correct branches for user accounts and groups must be specified:

- Do not use white-space characters surrounding group names.
- Multiple group names must be separated by a semicolon (;).
- HPOM DMA uses the group SONATA-USER internally for users authenticating using the local users store.

---

# A HPOM DMA Reference Information

This chapter describes the standard HPOM DMA installation. The following information is available:

- [Installation Locations](#) on page 229
- [Configuration Files](#) on page 231
- [Data Files](#) on page 234
- [Log Files](#) on page 235
- [Standard Synchronization Package Locations](#) on page 241
- [Objects Installed on HPOM](#) on page 237
- [HPOM DMA Default Synchronization Package and other standard synchronization packages](#) on page 243.

## Installation Locations

The HPOM DMA installation installs the files in the following locations:

- *UNIX and Linux*
  - **<InstallDir>**  
/opt/OV/
  - **<DataDir>**  
/var/opt/OV/
  - **<SharedDir>**  
/var/opt/OV/shared

- *Windows*

- **<InstallDir>**

Default:

C:\Program Files\HP\HP BTO Software

- **<DataDir>**

Default:

C:\Documents and Settings\All Users\Application Data\HP\HP BTO Software

- **<SharedDir>**

Default:

C:\Documents and Settings\All Users\Application Data\HP\HP BTO Software\shared

# Configuration Files

All HPOM DMA configuration files are stored in:

`<SharedDir>/server/conf/dma`

These files are used during run time and can be changed by users.

The initial configuration files are available (unchanged) for backup purposes, in:

`<InstallDir>/newconfig/DataDir/conf/dma`

**Table 7 Configuration Files and Descriptions**

Location and Name	Purpose
<b><code>&lt;SharedDir&gt;/server/conf/dma</code></b>	
DefaultSyncTask.settings	Contains the information that can be accessed through the Connection and Configuration web page.
schedule.xml	Specifies when a synchronization should be triggered. This information can be accessed from the Schedule web page.
nodetypes.xml	Defines which UCMDB CI types are imported as nodes into the HPOM node groups. For each rule that matches, the node is also added to the all node groups defined in the rule. For details, see the <i>HPOM DMA Extensibility Guide</i> .
containmentrelations.xml	Contains a list of regular expressions. All UCMDB relation type names that match this regular expression become a containment relation when the relation is synchronized into the Service Navigator using DMA. For details, see the <i>HPOM DMA Extensibility Guide</i> .

**Table 7 Configuration Files and Descriptions**

Location and Name	Purpose
users.properties	Contains the HPOM DMA console users' information written by the dmauser tool.
ldap.properties	Contains the configuration information required by LDAP authentication.
MachineTypes.xml	Contains all currently installed HPOM machine types (UNIX and Linux only).
MachineTypes_template.xml	Contains list of currently supported machine types (UNIX and Linux only).
sync-packages	Contains a subdirectory for each synchronization package. Each synchronization package contains several configuration files. For details, see the <i>HPOM DMA Extensibility Guide</i> .
<p><b>&lt;SharedDir&gt;/server/conf/dma/sync-packages/&lt;syncPackage&gt;/</b>            See <a href="#">Standard Synchronization Package Locations</a> on page 241 for a description of the files installed with HPOM DMA. Detailed information about synchronization packages is available in the <i>HPOM DMA Extensibility Guide</i>.</p>	
bundle.xml	Contains general information about this synchronization package, including name, description, priority and UCMDB TQL queries used. This file cannot be accessed through HPOM DMA web console.
nodemapping.xml	Contains the rules for the node group mapping.
servicemapping.xml	Contains the rules for the Service Type Definition mapping.
attributemapping.xml	Contains the rules for attribute enrichment.
usermapping.xml	Contains the rules for the User Profile mapping.



**Table 7 Configuration Files and Descriptions**

<b>Location and Name</b>	<b>Purpose</b>
preMapping.groovy	Contains the script to be executed before mapping.
preUpload.groovy	Contains the script to be executed before synchronization.
postUpload.groovy	Contains the script to be executed after synchronization.
<b>&lt;SharedDir&gt;/server/conf/dma/uilaunch/</b>	
BAC_7.5.properties	Contains information used by the UI Launch tools for BAC 7.5x.
BAC_8.0.properties	Contains information used by the UI Launch tools for BAC 8.0x.
UCMDB_7.5.properties	Contains information used by the UI Launch tools for UCMDB 7.5x.
UCMDB_8.0.properties	Contains information used by the UI Launch tools for UCMDB 8.0x.

# Data Files

HPOM DMA data files are stored in:

`<SharedDir>/server/datafiles/dma`

HPOM DMA creates these files during run time. They must not be changed by users.

**Table 8 Data Files and Descriptions**

Location and Name	Purpose
<b><code>&lt;SharedDir&gt;/server/datafiles/dma</code></b>	
nodemapping.properties	Maps DNS names of nodes to UCMDB or BAC IDs. The file is created and updated during node synchronization.

# Log Files

The HPOM DMA log files are listed in [Table 9](#). For information how to configure HPOM DMA log files, see [Changing Log File Parameters](#) on page 224.

**Table 9 HPOM DMA Log Files**

Logging	Platform	Location and Name
Synchronization	All	<SharedDir>/server/log/dma/ sync.<*>.<locale> Accessible from the HPOM DMA console.
Smart Message Mapper	All	<SharedDir>/server/log/dma/ msgmap.<*>.<locale>
UI Launch	All	<SharedDir>/server/log/dma/ uilaunch.<*>.<locale>
Default HPOM DMA Log File	All	<SharedDir>/server/log/ system.<#>.<locale>
HPOM for UNIX or Linux Web Service	UNIX, Linux	<SharedDir>/server/log/om/ ciws.<*>.<locale>
HPOM for Windows Web Service	Windows	<SharedDir>\server\log\om\ws.trace .txt http://<host>/omws/trace.txt
HPOM DMA Web Console (CWC)	UNIX, Linux	<DataDir>/tmp/cwc.log
	Windows	<InstallDir>/nonOV/tomcat/b/ cwc.log

**Table 9 HPOM DMA Log Files**

<b>Logging</b>	<b>Platform</b>	<b>Location and Name</b>
TomcatB	UNIX, Linux	<DataDir>/log/tomcat/ovtomcatb.out
	Windows	<DataDir>/log/tomcat/stdout.log
Installation	UNIX, Linux	/var/tmp/ HPDma_<version>_HPOvInstaller.txt /var/tmp/HPOvInstaller/ HPDma_<version>/*
	Windows	C:\Documents and Settings\ Administrator\Local Settings\ Temp\HPOvInstaller\HPDma_<version>

# Objects Installed on HPOM

HPOM DMA installs the following objects for HPOM:

- [Node Groups](#)
- [Root Service](#)
- [Propagation and Calculation Rules](#)
- [Service Type Definitions](#) on page 238
- [Policies](#) on page 239

## Node Groups

HPOM DMA includes two HPOM node groups that are automatically created during installation:

- CMDB
- CMDB\_Removed

## Root Service

HPOM DMA includes one HPOM root service that is automatically created during installation:

- CMDB

## Propagation and Calculation Rules

HPOM DMA includes the following HPOM calculation and propagation rules:

- **Calculation Rule:** `ucmdb_generic_CR` ("Most Critical")
- **Propagation Rule:** `ucmdb_generic_PR` ("Unchanged")

## Service Type Definitions

HPOM DMA includes the following HPOM Service Type Definitions and their associated GUID values:

- **Informix** (ucmdb\_informix)
- **NT** (ucmdb\_nt)
  - **Cpu** (ucmdb\_cpu)
  - **Disk** (ucmdb\_disk)
  - **Drive** (ucmdb\_drive)
  - **File system** (ucmdb\_filesystem)
  - **IP** (ucmdb\_ip)
  - **Logical Disk** (ucmdb\_logicaldisk)
  - **Logical Volume** (ucmdb\_logicalvolume)
  - **Memory** (ucmdb\_memory)
  - **Printer** (ucmdb\_printer)
  - **Service** (ucmdb\_service)
  - **SSH** (ucmdb\_ssh)
  - **Windows OS User** (ucmdb\_winosuser)
- **Oracle Windows** (ucmdb\_oracle\_nt)
- **Oracle UNIX** (ucmdb\_oracle\_unix)
- **SQLServer** (ucmdb\_)
- **SQLServer 6.5** (ucmdb\_sqlserver\_65)
- **Sybase** (ucmdb\_sqlserver)
- **Unix** (ucmdb\_unix)
  - **Cpu** (ucmdb\_cpu)
  - **Disk** (ucmdb\_disk)
  - **Drive** (ucmdb\_drive)
  - **File system** (ucmdb\_filesystem)
  - **IP** (ucmdb\_ip)

- Logical Disk (ucmdb\_logicaldisk)
- Logical Volume (ucmdb\_logicalvolume)
- Memory (ucmdb\_memory)
- Printer (ucmdb\_printer)
- SSH (ucmdb\_ssh)
- OS User (ucmdb\_osuser)
- Business Process Group (ucmdb\_bp\_group)
- Business Process Step (ucmdb\_bp\_step)
- BPM Transaction from Location (ucmdb\_bp\_tx\_from\_location)



Where appropriate, existing HPOM or SPIs tools are assigned to the HPOM DMA Service Type Definitions.

## Policies

The HPOM DMA policies are listed in [Table 10](#). For information on how to assign and deploy these policies, see [Assigning the OM DMA Policy Group](#) on page 108 or [Assigning and Deploying the OM DMA Policy Group](#) on page 116.



When monitoring HPOM DMA in cluster installations, policies should be enabled on the active node and disabled on all inactive nodes.

For information about policy deployment in cluster installations, see the appropriate HPOM documentation on virtual nodes.

**Table 10 HPOM DMA Policies**

<b>Name</b>	<b>Group</b>	<b>Description</b>
HPOM DMA Synchronization log	OM DMA	Monitors failure of the HPOM DMA synchronization from UCMDDB to HPOM.
HPOM DMA Smart Message Mapping log	OM DMA	Monitors the HPOM DMA Smart Message Mapper log file.
HPOM Web Service log	OM DMA	Monitors the HPOM Web Service log.
uCMDDB missing Node	OM DMA	Monitors whether a node in UCMDDB previously synchronized to HPOM is now missing from the current synchronization.



# Standard Synchronization Package Locations

This section describes the directory and file structure of synchronization packages in the file system. Each of these synchronization package directories must contain a `bundle.xml` file. Some synchronization packages also include `servicemapping.xml`, `nodemapping.xml`, and `attributemapping.xml` files.

```
<SharedDir>/server/conf/dma/sync-packages/default  
    attributemapping.xml  
    bundle.xml  
    servicemapping.xml  
    preMapping.groovy
```

```
<SharedDir>/server/conf/dma/sync-packages/dnsmapping  
    bundle.xml  
    preMapping.groovy
```

```
<SharedDir>/server/conf/dma/sync-packages/dmaInformix  
    bundle.xml  
    nodemapping.xml  
    servicemapping.xml
```

```
<SharedDir>/server/conf/dma/sync-packages/dmaMSSQLServer  
    bundle.xml  
    nodemapping.xml  
    servicemapping.xml
```

```
<SharedDir>/server/conf/dma/sync-packages/dmaOracle  
    bundle.xml  
    nodemapping.xml  
    servicemapping.xml
```

```
<SharedDir>/server/conf/dma/sync-packages/dmaOS  
    bundle.xml  
    nodemapping.xml (UNIX and Linux only)
```

```
<SharedDir>/server/conf/dma/sync-packages/dmaSybase  
    bundle.xml  
    nodemapping.xml
```

```
<SharedDir>/server/conf/dma/sync-packages/dmaWinOS  
    bundle.xml  
    nodemapping.xml (UNIX and Linux only)
```

```
<SharedDir>server//conf/dma/sync-packages/  
dmaScriptAutomaticPolicyDistribution  
    bundle.xml  
    postUpload.groovy (UNIX and Linux only)
```

`<SharedDir>/server/conf/dma/sync-packages/dmaEUM  
bundle.xml`

`<SharedDir>/server/conf/dma/sync-packages/dmaMyCompany  
bundle.xml`

`<SharedDir>/server/conf/dma/sync-packages/dmaGroupHostResources  
bundle.xml  
preUpload.groovy`

# HPOM DMA Default Synchronization Package

The default synchronization package is deployed as part of the standard installation. It contains the default mappings to enable synchronization of nodes and services from UCMDB or BAC into HPOM.

Priority: 10 (LOW)

The default synchronization package is the package with the lowest priority in HPOM DMA. This package is taken only if no other mappings apply.

## Service Mapping

By default, all services are assigned to the default service type definition in accordance with the following pattern: `ucmdb_<CI Type>`.

The service type definitions must exist in HPOM. For details on how to upload service type definitions, see the *HPOM DMA Extensibility Guide*.

## Attribute Mapping

This section include information on attribute mappings used for the following elements:

- [All CI Types](#) on page 243
- [SQL Server, Oracle, and Sybase Database CI Types](#) on page 244
- [Host, NT, and Unix CI Types](#) on page 244

## All CI Types

Required fields (must be selected in TQL query definition):

`display_label` (Display Label)

The default attribute mapping defines mapping for:

- `display_label`

*Example*

The display label for Oracle database is set to:

```
"my_database on mynode.example.com [oracle]"
```

### *Example*

The display label for other types is set to:

```
"c:\" [disk]
```

The display label for nodes and service groups is not changed.

- CMDBCiCaption

The UCMDB display label is not mapped, but rather manipulated for better readability and to achieve uniqueness. As a result, you also need to map the original UCMDB display label into a service attribute. This is needed for Smart Message Mapping.

## SQL Server, Oracle, and Sybase Database CI Types

Required fields (must be selected in TQL query definition):

- database\_dbtype (Type)
- database\_dbversion (Version)
- display\_label (Display Label)

## Host, NT, and Unix CI Types

Required fields (must be selected in TQL query definition)

- host\_dnsname (Host DNS Name)
- host\_os (Host Operating System)
- host\_osversion (Host Operating System Version)
- host\_model (Host Model)
- display\_label (Display Label)
- data\_description (Description)

Hints are required for Smart Message Mapping:

- Make sure that the content of attributes includes enough information, for example, caption.

- When identifying a host CI, make sure that the caption is identical to the host DNS name. This is used as a fallback by Smart Message Mapping when a message cannot be definitely mapped to a service.

The default attribute mapping defines mapping for:

- **Hosted on relationship**  
Without setting the `hosted_on` relationship, the Smart Message Mapping cannot work.
- `CmdbObjectID` and `CmdbCiType`.  
Required for UI launch tools of synchronized services. `ID` is mapped to `CmdbObjectID` and `CiType` is mapped to `CmdbCiType`.  
These attributes are also added to the service.

The following standard mappings are included:

- [AIX Attribute Mapping](#) on page 246
- [HP-UX Attribute Mapping](#) on page 246
- [Linux Attribute Mapping](#) on page 246
- [Solaris Attribute Mapping](#) on page 247
- [Windows Attribute Mapping](#) on page 247
- [Other Attribute Mapping](#) on page 248

`ovo_systemType`, `ovo_osType` and `ovo_osVersion` are required to specify the appropriate machine type in HPOM.



These are not all the possible mappings, as it is not possible to discover all combinations of HPOM for Windows requests with the standard discovery from UCMDB. If the appropriate mapping is not available, the HPOM for Windows discovery attempts to find the information.

## AIX Attribute Mapping

Table 11 summarizes the default attribute mappings for AIX nodes.

**Table 11 Attribute Mapping for AIX**

UCMDB Attributes			HPOM Attributes		
CiType	host_os	host_osversion	ovo_systemType	ovo_osType	ovo_osVersion
unix	AIX	starts with 51	Power PC Family	AIX_32	5L 5.1
unix	AIX	starts with 52	Power PC Family	AIX_32	5L 5.2
unix	AIX	starts with 53	Power PC Family	AIX_32	5L 5.3

## HP-UX Attribute Mapping

Table 12 summarizes the default attribute mappings for HP-UX nodes.

**Table 12 Attribute Mapping for HP-UX**

UCMDB Attributes				HPOM Attributes		
CiType	host_os	host_model	description	ovo_systemType	ovo_osType	ovo_osVersion
unix	HP-UX	ia64	contains B.11.22	Itanium Compatible	HP-UX_64	B.11.22
unix	HP-UX	ia64	contains B.11.23	Itanium Compatible	HP-UX_64	B.11.23
unix	HP-UX	ia64	contains B.11.31	Itanium Compatible	HP-UX_64	B.11.31
unix	HP-UX		contains B.10.20	Itanium Compatible	HP-UX_64	B.10.20
unix	HP-UX		contains B.11.00	Itanium Compatible	HP-UX_64	B.11.00
unix	HP-UX		contains B.11.11	Itanium Compatible	HP-UX_64	B.11.11
unix	HP-UX		contains B.11.23	Itanium Compatible	HP-UX_64	B.11.23
unix	HP-UX		contains B.11.31	Itanium Compatible	HP-UX_64	B.11.31

## Linux Attribute Mapping

No mapping specified.

## Solaris Attribute Mapping

Table 13 summarizes the default attribute mappings for Solaris nodes.

**Table 13 Attribute Mapping for Solaris**

UCMDB Attributes				HPOM Attributes		
CiType	host_os	host_osversion	host_model	ovo_systemType	ovo_osType	ovo_osVersion
unix	SunOS	2.6		SPARC Family	Solaris_32	2.6
unix	SunOS	5.7		SPARC Family	Solaris_32	7
unix	SunOS	5.8		SPARC Family	Solaris_32	8
unix	SunOS	5.9		SPARC Family	Solaris_32	9
unix	SunOS	5.10	sun4u	SPARC Family	Solaris_64	10
unix	SunOS	5.10	i86pc	x86/x64 Compatible	Solaris_64	10

## Windows Attribute Mapping

Table 14 summarizes the default attribute mappings for Windows nodes.

**Table 14 Attribute Mapping for Windows**

UCMDB Attributes			HPOM Attributes		
CiType	host_os	host_osversion	ovo_systemType	ovo_osType	ovo_osVersion
nt	Windows	4.0	x86/x64 Compatible	Windows_32	NT (4.0)
nt	Windows	5.0	x86/x64 Compatible	Windows_32	2000 (5.0)
nt	Windows	5.1	x86/x64 Compatible	Windows_32	XP (5.1)
nt	Windows	5.2	x86/x64 Compatible	Windows_32	2003 (5.3)
nt	Windows	6.0	x86/x64 Compatible	Windows_32	Server 2008 (6.0)

## Other Attribute Mapping

Table 15 summarizes the default attribute mappings for all nodes not specifically specified.

**Table 15 Attribute Mapping for Other Platforms**

UCMDB Attributes	HPOM Attributes		
	ovo_systemType	ovo_osType	ovo_osVersion
	n/a	n/a_0	n/a

## Pre-Mapping Script

The pre-mapping script sets the `ipAddresses` attribute for CIs of type `host`. If a `host` CI references multiple CIs of type `IP`, all IP addresses are copied into the attribute, separated by white space. In HPOM, this information is used to set the IP address of a managed node.

The `host_iscomplete` and `host_key` attributes are used to establish the MAC address for CIs. This information is needed so that the UCMDB can identify the nodes when HP Operations Manager i synchronizes them again with the UCMDB.

## Host, NT, and UX CI Types

Required fields (must be selected in TQL query definition):

- `host_iscomplete` (Host Is Complete)
- `host_key` (Host Key)

## IP CI Type

Required field (must be selected in TQL query definition):

- `ip_address` (IP Address)



# UNIX OS Synchronization Package: dmaOS

The UNIX operating system synchronization package is deployed as part of the standard installation. It contains mappings to enable synchronization of UNIX nodes from UCMDB or BAC into HPOM.

Priority: 8

TQL query used: Unix Operating System (Operations)

## Node Mapping

Table 16 specifies the node mappings for the UNIX operating system.

**Table 16 UNIX Operating System Node Mappings**

CI Type	host_os	Mapped to Node Group	
		Windows	UNIX
unix	HP-UX	—	OSSPI-HPUX
unix	Linux	—	OSSPI-Linux
unix	AIX	—	OSSPI-AIX
unix	SunOS	—	OSSPI-Solaris



On HPOM for Windows, operating system node mapping is not needed as nodes are automatically mapped to product defined node groups based on the operating system. Any specified node mapping is ignored.

# Windows OS Synchronization Package: dmaWinOS

The Windows operating system synchronization package is deployed as part of the standard installation. It contains mappings to enable synchronization of Windows nodes from UCMDB or BAC into HPOM.

Priority: 8

TQL query used: Windows Operating System (Operations)

## Node Mapping

Table 17 specifies the node mappings for the Windows operating system.

**Table 17 UNIX Operating System Node Mappings**

CI Type	host_os	Mapped to Node Group on HPOM for Windows	Mapped to Node Group on HPOM for UNIX
nt	not Linux	—	WINOSSPI-Windows



On HPOM for Windows, operating system node mapping is not needed as nodes are automatically mapped to product defined node groups based on the operating system. Any specified node mapping is ignored.

# Informix Synchronization Package: dmaInformix

The Informix database synchronization package is deployed as part of the standard installation. It contains mappings to enable synchronization of Informix nodes and services from UCMDB or BAC into HPOM.

Priority: 7

TQL query used: Informix (Operations)

## Service Mapping

Table 18 specifies the service mappings for the Informix database.

**Table 18 Informix Database Service Mappings**

CI Type	DB type	Mapped to Service Type Definition
database	informix	ucmdb_informix

## Node Mapping

Table 19 specifies the node mappings for the Informix database.

**Table 19 Informix Database Node Mappings**

Host Server Type	Mapped to Node Group on HPOM for Windows	Mapped to Node Group on HPOM for UNIX or Linux
informix	DBSPI_Informix_Nodes	Informix

# Microsoft SQL Server Synchronization Package: dmaMSSQLServer

The Microsoft SQL Server database synchronization package is deployed as part of the standard installation. It contains mappings to enable synchronization of Microsoft SQL Server nodes and services from UCMDB or BAC into HPOM.

Priority: 7

TQL query used: MS SQL Server (Operations)

## Service Mapping

Table 20 specifies the service mappings for the Microsoft SQL Server database.

**Table 20 Microsoft SQL Server Database Service Mappings**

CI Type	Database Version	Mapped to Service Type Definition
sqlserver	6.5	ucmdb_sqlserver65
sqlserver		ucmdb_sqlserver

## Node Mapping

Table 19 specifies the node mappings for the Microsoft SQL Server database.

**Table 21 Microsoft SQL Server Database Node Mappings**

Host Server Type	Mapped to Node Group on HPOM for Windows	Mapped to Node Group on HPOM for UNIX or Linux
sqlserver	DBSPI_SQL_Server_Nodes	MSSQL

# Oracle Synchronization Package: dmaOracle

The Oracle database synchronization package is deployed as part of the standard installation. It contains mappings to enable synchronization of Oracle nodes and services from UCMDB or BAC into HPOM.

Priority: 7

TQL query used: Oracle (Operations)

## Service Mapping

Table 22 specifies the service mappings for the Oracle database.

**Table 22 Oracle Database Service Mappings**

Caption from Parent	CI Type	Mapped to Service Type Definition
Databases on Windows	oracle	ucmdb_oracle_nt
Database on Unix	oracle	ucmdb_oracle_unix

## Node Mapping

Table 23 specifies the node mappings for the Informix Database.

**Table 23 Oracle Database Node Mappings**

CI Type	Host Server Type	Mapped to Node Group on HPOM for Windows	Mapped to Node Group on HPOM for UNIX or Linux
nt	oracle	DBSPI_Oracle_Windows_Nodes	Oracle (NT)
unix	oracle	DBSPI_Oracle_Unix_Nodes	Oracle (Unix)

# Sybase Synchronization Package: dmaSybase

The Sybase database synchronization package is deployed as part of the standard installation. It contains mappings to enable synchronization of Sybase services from UCMDB or BAC into HPOM.

Priority: 7

TQL query used: Sybase (Operations)

## Node Mapping

Table 24 specifies the node mappings for the Sybase database.

**Table 24 Sybase Database Node Mappings**

<b>Host Server Type</b>	<b>Mapped to Node Group on HPOM for Windows</b>	<b>Mapped to Node Group on HPOM for UNIX or Linux</b>
sybase	DBSPI_Sybase_Nodes	Sybase

# Group Multiple Host Resource Types Synchronization Package

The HPOM DMA "Script: Group Multiple Host Resource Types" synchronization package is deployed as part of the standard installation. It contains a pre-upload script that groups multiple instances of a resource type, for example disks, under an additional subgroup.

Priority: 8

TQL query used: None

- ▶ This script requires STDs that are not delivered as part of the HPOM DMA product. It is recommended that Automatic STD Creation is activated. For details, see [Creating Service Type Definitions Automatically](#) on page 108 and [page 114](#).

# Trigger Policy Distribution Synchronization Package

- ▶ UNIX and Linux only.

The HPOM DMA "Script: Trigger Policy Distribution" synchronization package is deployed as part of the standard installation. It contains a post-upload script that triggers policy distribution.

Priority: 8

TQL query used: None

## My Company Synchronization Package: dmaMyCompany

The My Company synchronization package is deployed as part of the standard installation. It contains examples of TQL queries and enrichment rules to help you configure customized Service Navigator views in HPOM.

Priority: 8

TQL query used: My Company US (Operations)  
My Company EMEA (Operations)  
My Company ASIAPAC (Operations)

## End User Management Synchronization Package: dmaEUM

The End User Management synchronization package is deployed as part of the standard installation. It contains a TQL query and service type definitions to enable the display of End User Management views from BAC in HPOM.

Priority: 9

TQL query used: End User Monitors (Operations)



# DNS Mapping Synchronization Package: dmaDnsMapping

The DNS Mapping synchronization package is deployed as part of the standard installation. It contains a pre-mapping script to set the `host_dnsname` (Host DNS Name) attribute for CIs of type host.

Discovery modules may store the fully qualified domain name in different attributes of CIs of type host or of type IP. The pre-mapping script queries these attributes to establish the fully qualified domain name and then stores this information in the `host_dnsname` (Host DNS Name) attribute.

In addition, the pre-mapping script sets the `hosted_on` attribute and stores the fully qualified domain name in the `hosted_on` attribute. The `hosted_on` attribute is required for Smart Message Mapping.

Priority: 9

TQL query used: none

# HPOM DMA Configuration Parameters in XPL

Table 25 lists the XPL configuration parameters used by HPOM DMA.

**Table 25** OV Resource Group: Server Configuration Parameters in XPL

Name Space	Name	Type	Default	Description
dma.SmartMessageMapper	CustomMessageAttributes	String		Service attributes that the Smart Message Mapper adds as custom message attributes to HPOM messages.
dma.SmartMessageMapper	HostnameSeparator	String	@@	Indicator for the Smart Message Mapper to identify the start of the hostname in an incoming message.
dma.SmartMessageMapper	IgnoreCase	Boolean	false	Indicates whether the Smart Message Mapper takes into account the case of the text used in incoming messages.
dma.SmartMessageMapper	MinimumServiceUpdate	int	15	Minimum delay (in minutes) before which the Smart Message Mapper processes service changes.
dma.SmartMessageMapper	PollingInterval	int	60	Interval (in seconds) after which the Smart Message Mapper polls for service changes.
dma.SmartMessageMapper	ServiceSeparator	String	:	Indicator for the Smart Message Mapper to divide an incoming message into the required hints.

**Table 25 OV Resource Group: Server Configuration Parameters in XPL**

Name Space	Name	Type	Default	Description
dma.UILaunch	ConfigName	String	BAC_7.5	UCMDB or BAC application and version used by the UI Launch web application. Possible values are: BAC_7.5 BAC_8.0 UCMDB_7.5 UCMDB_8.0 UCMDB_9.0
HPDmaSync	FailedServicesToLog	int	100	To reduce log output, only log the most likeliest root causes of a service synchronization failure. A value of 0 logs all errors.
opc.WebService	EnumerationExpiration	int	20	Duration for which the enumeration context is valid. Default is 20 minutes.
opc.WebService	EnumerationExpiration Maximum	int	60	Maximum duration for which the enumeration context is valid. If a client specifies a longer value, the service overrides the client's request with this value. Default is 60 minutes.
opc.WebService	EventQueueSize	int	1000	Maximum number of events that an event queue stores. When the event queue contains the maximum number of events, the service discards the oldest events from the queue as new events are added. Default is 1000 events.

**Table 25 OV Resource Group: Server Configuration Parameters in XPL**

<b>Name Space</b>	<b>Name</b>	<b>Type</b>	<b>Default</b>	<b>Description</b>
opc.WebService	MaxItemsMaximum	int	500	Maximum number of items that the service allows for a pull operation. If the client specifies a larger value, it is ignored and this value is used. Default is 500 items.
opc.WebService	SubscriptionExpiration	int	60	Duration for which the subscription context is valid. Default is 60 minutes.
opc.WebService	SubscriptionExpirationMaximum	int	1440	Duration for which the subscription context is valid. If a client specifies a longer value, the service overrides the client's request with this value. Default is 1440 minutes (one day).
opc.WebService. Configuration Item	NodeGroupCreation Enabled	Boolean	false	Indicates whether Node Group Creation for CI Nodes created within the Web Service is enabled or disabled. By default, this feature is disabled and the Node Groups are not created.
opc.WebService. Configuration Item	StdCreationEnabled	Boolean	false	Indicates whether STD Creation for CI Services created within the Web Service is enabled or disabled. By default, this feature is disabled and the STDs are not created.

**Table 25 OV Resource Group: Server Configuration Parameters in XPL**

<b>Name Space</b>	<b>Name</b>	<b>Type</b>	<b>Default</b>	<b>Description</b>
opc.WebService. Configuration Item	UserProfileAssignment Enabled	Boolean	false	Indicates whether User Profile assignment for CI Services created within the Web Service is enabled or disabled. By default, this feature is disabled and the User Profile properties within the CI created by the Web Service are ignored.
wsman.client	bulkcreate.chunksize	int	1000	The maximum number of items the client sends in a chunked Bulk Create operation. Default is 1000.
wsman.client	enumeration.chunksize	int	1000	The maximum number of items the client requests in a pull operation. Default is 1000.
wsman.client	enumeration.context. timeout	int	600000	EnumerationExpiration value in ms requested by the client. This is the duration that the enumeration context should be valid for. Default is 10 minutes.
wsman.client	operation.timeout	int	300000	Timeout for each operation requested by the client in ms. After this time the server sends a timeout fault. Default is 5 minutes.
wsman.client	ssl.keystore	String		Absolute path to the keystore file containing the SSL certificates (used by the LDAP authentication and for running DMA in secured mode).

# Open Source Software

WisemanA, JAXB and JAX-WS Open Source Software (OSS) product source code is packaged with HPOM DMA. The OSS source code is located in the following location:

```
<InstallDir>/nonOV/wiseman/a/src
```

The OSS product packages used by HPOM DMA are as follows:

- jaxb-src.zip
- jaxws-src.zip
- wiseman\_src.zip

# Index

## A

### access

- HPOM installation, 51
- remote, 187
- restriction to localhost, 188
- UCMDB/BAC
  - network, 51

### activating

- discovery source, 146
- EUM synchronization package, 164
- LDAP configuration, 194
- licenses, 169
- synchronization packages, 117
- tool group, 131

### adding

- attribute condition, 156
- relationship, 155
- user
  - HPOM DMA, 93, 94
  - integration, 59, 120

### agent types, 111

### AJP port, changing, 188

### alerts

- BPM, 159
- CI status, 159, 215
- performance limit, 161, 215

### applications

- removing, 212
- started, 64, 76
- stopped, 64, 76

### Application Support Engineer, 26

### assigning

- CMDB Node Groups, 108
- OM DMA Policy Group, 108, 116
- ROOT\_DMA\_Service Service Group, 107
- user profiles to services, 38
  - Linux, 109
  - mapping, 110, 115
  - prerequisites, 109, 115
  - UNIX, 109
  - Windows, 115
- user roles to services, 38
  - Linux, 109
  - mapping, 110, 115
  - prerequisites, 109, 115
  - UNIX, 109
  - Windows, 115

- attribute
  - completeness, 218
  - enrichment, 232
  - Host DNS Name, 61
  - mapping
    - AIX, 246
    - default, 243
    - HP-UX, 246
    - machine type, 113
    - machine types, 113
    - node types, 111
    - other platforms, 248
    - Solaris, 247
    - Windows, 247
  - name, 156
  - node, 218
  - services, 41
  - smart message mapping, 244
- attributemapping.xml, 232, 241
- authentication using LDAP, 190
- AutoPass license, 165
  - installing, 173
  - verifying, 174

## **B**

- backing up, 197
- BAC package
  - EUM synchronization, 162
- BPM integration
  - alerts, 159
  - removing, 215
  - setting up, 159
- browser, 58, 73, 88, 89
- bundle.xml, 232, 241
- Business Process Monitoring, 159

## **C**

- calculation rules, 237

- case sensitivity, configuring, 138
- certificate
  - clusters, 179
  - LDAP server, 185, 191
  - server, 182
  - UCMDB server, 185
- chunk size
  - WS Man Client, 219
- CI status alerts
  - deleting, 215
  - setting, 159
- classloader, modifying, 149
- client
  - certificates, 177, 180
  - java keystore, 183
  - restricting, 188
  - WS Man, 219
- clusters
  - certificates, 179
  - installing, 63, 76
  - licenses, 165, 171
  - supported, 53
  - upgrading, 119
- ConfigureMachineTypes script, 112
- configuring
  - agent types, 111
  - case sensitivity, 138
  - hint separator, 137
  - hostname separator, 138
  - HPOM DMA, 91, 117
  - LDAP, 193
  - logging, 224
  - MSI process order, 140
  - performance, 217
  - performance parameters, 218, 221
  - tips, 217
  - UI Launch, 127
    - web application, 133



- console
  - password, 93
  - starting, 73, 88, 89
  - user, 93
- containmentrelations.xml, 231
- credentials, HPOM web service, 223
- customizing
  - smart message mapping, 135
- D**
- data directory, 230
- default synchronization package, 243
- DefaultSyncTask.settings, 177, 183, 231
- deinstalling, 203
- deleting user, 94
- deploying
  - OM DMA Policy Group, 108, 116
- directories
  - locations, 229
  - structure, 241
  - sync-packages, 232
- disabling SPI discovery, 146
- discovery
  - administrator, 24
  - data, 61
  - installing pattern, 150
  - set up, 61
  - source
    - resetting, 213
    - selecting, 146
  - SPI, 48, 146
  - UCMDB, 48, 55, 146
- dmatoolgen.bat, 131
- dmatoolgen.sh, 129
- DNS, 56

- E**
- enabling Server MSI, 72, 134
- enrichment rule
  - applying, 105
  - Database Dependency, 102
  - Node Server Type, 102
- EUM synchronization
  - activating package, 164
  - BAC package, 162
- exporting certificates for clients, 177, 180

- F**
- file
  - attributemapping.xml, 232, 241
  - bundle.xml, 232, 241
  - DefaultSyncTask.settings, 177, 183, 231
  - ldap.properties, 190, 193, 232, 234
  - locations, 229
  - log files, 111, 206, 235
  - MachineTypes.xml, 232
  - MachineTypes\_template.xml, 112, 232
  - nodemapping.xml, 232
  - nodetypes.xml, 231
  - schedule.xml, 231
  - servicemapping.xml, 232, 241
  - structure, 241
  - users.properties, 232

- H**
- hardware, 57
- heap size
  - Tomcat server, 218
- hint, smart message mapping, 41, 244
- hint separator, configuring, 137
- Host DNS Name, 61, 244
- hosted\_on, 61
- hostname separator, configuring, 138

HP Business Availability Center, 55

HPOM, 52

- administrators, 25

- for Linux

  - agents, 56

- for UNIX

  - agents, 56

- for Windows

  - web services message size, 221

- operators, 26

- patches, 56

- web service credentials, 223

HPOM DMA package, 97

HP Universal CMDB, 55

- Advanced, 55

- Free, 55

- Standard, 55

## I

impact analysis, 15

incident analysis, 15

installing

- BAC/UCMDB discovery pattern, 150

- clusters, 63, 76

- directory, 230

- HPOM DMA, 63

  - PA-RISC, 75

- license, 173

- on HP-UX and Solaris, 66

- on Windows, 66

- repair, 64, 77

- UI Launch

  - tools, 127, 131

integrators, 24

Internet Information Services (IIS), 186

## J

Java, 61

JAXB, 262

JAX-WS, 262

## K

keystore, 182, 183, 191

## L

LDAP

- authentication, 190

- configuring, 232

- server certificate, 191

- server certificates, 185

ldap.properties, 190, 232

license

- activating, 169

- agreement, 68, 81

- checking, 167

- clusters, 171

- Evaluation, 166

- information, 169

- installing with AutoPass, 173

- Instant-On, 166

- password

  - delivery centers, 172

  - receiving, 173

- Password Delivery Centers, 172

- Permanent, 166

- requesting, 171

- server, 165

- setting up, 169

- verifying with AutoPass, 174

Linux, 66

- enabling MSI, 134

- file locations, 229

listing users, 94

localhost, restricting access, 188

- location
  - file, 229
  - synchronization package, 232

- log files
  - used by HPOM DMA, 235
  - XPL, 224

- logging, configuring, 224

## M

- machine types, 232

- MachineTypes.xml, 112, 232

- MachineTypes\_template.xml, 112, 232

- maxBufferSize, 221

- maxReceivedMessageSize, 221

- memory

  - Tomcat server, 217

- message

  - HPOM operators, 26

  - license, 167

  - logging, 224

  - size, 221

  - smart message mapping, 45

  - SPI-generated, 146

  - status change, 159

- migrating, 197

- modifying

  - classloader, 149

  - LDAP properties, 193

  - XPL configurations, 148, 214

- mount point, 65, 78

- moving configuration, 200

- MSI process order, configuring, 140

- MyServiceBinding, 221

## N

- node attribute, 218

- node group, 102, 237, 249, 250, 251, 253
  - CMDB, 108, 211

- node mapping

  - file, 232

  - Informix, 251

  - Microsoft SQL Server, 252

  - Oracle, 253

  - Sybase, 254

  - UNIX, 249

  - Windows, 250

- nodemapping.properties, 234

- nodemapping.xml, 232

- nodetypes.xml, 231

- Non-XPL

  - performance parameters, 221

## O

- OM DMA policies, 240

- Open Source Software, 262

- OutOfMemoryException, 218

## P

- performance

  - configuration tips, 217

  - limit alerts

    - deleting, 215

    - setting up, 161

  - parameter configuring, 221

- policy

  - HPOM DMA Smart Message Mapping
    - log, 240

  - HPOM DMA Synchronization log, 240

  - HPOM Web Service log, 240

  - OM DMA, 116, 239

  - opcmsg, 159

  - uCMDB missing Node, 240

- postUpload.groovy, 233

- preMapping.groovy, 233
- preUpload.groovy, 233
- propagation rules, 237

## R

- reference, 229

- relationship

  - database depends on host, 102
  - host contains databases, 102

- removing

  - applications, 212
  - BPM integration, 215
  - CI status alerts, 215
  - configuration files, 206
  - files from BAC system, 208
  - files from HPOM system, 211
  - files from UCMDB system, 208
  - files on BAC, 206
  - files on UCMDB, 206
  - log files, 206
  - performance limit alerts, 215
  - smart message mapping, 213
  - tools, 212
  - UCMDB discovery, 213

- repairing, installation, 64, 77

- requirements, 57

- restoring, 197

- restricting synchronization, 149

- root

  - cause analysis, 15
  - service, 237

- ROOT\_DMA\_Service

  - Service Group, assigning, 107

- rules

  - attribute enrichment, 232
  - calculation, 237
  - node group mapping, 232
  - propagation, 237
  - service type definition mapping, 232
  - user profile mapping, 232

## S

- schedule.xml, 231

- script

  - postUpload.groovy, 233
  - preUpload.groovy, 233

- script ConfigureMachineTypes, 112

- scripting

  - synchronization, 39

- securing, 175

- server

  - certificate, 182
  - license, 165
  - Tomcat, 222

- Server MSI

  - enabling, 72, 134
  - unconfiguring, 213

- service

  - ID, 41, 45
  - root, 237
  - smart message mapping, 45
  - tree, 26, 49, 146
  - view, 15, 23
  - designer, 23

- service mapping, 243

  - Informix, 251
  - Microsoft SQL Server, 252
  - Oracle, 253

- servicemapping.xml, 232, 241

- Service Navigator, 23, 25, 48, 146

- service type definition, 232
    - automatic creation, 108, 114
  - severity, 41
  - shared directory, 230
  - simulation
    - smart message mapping, 142
  - smart message mapping
    - configuring, 72, 134
    - configuring case sensitivity, 138
    - configuring hint separator, 137
    - configuring hostname separator, 138
    - customizing, 135
    - discovery data, 61
    - hints, 244
    - introduction, 41
    - log file, 235
    - MSI process order, 140
    - simulation, 142
    - sleep time, 139, 140
    - starting, 135
    - stopping, 135
    - UCMDB display label, 244
    - unconfiguring, 213
  - SPI
    - discovery, 45, 146
      - disabling, 146, 147
      - reabling, 213
  - SSL
    - certificates for clusters, 179
    - exporting certificate for clients, 180
    - LDAP, 191
  - starting
    - applications during installation, 64, 76
    - HPOM DMA Console, 73, 89
    - smart message mapping, 135
  - stopping
    - applications during installation, 64, 76
    - smart message mapping, 135
    - Tomcat server, 185
  - Sun Solaris, 52, 66, 247
  - synchronization, 55
    - BAC package for EUM, 162
    - configuration, 231
    - customizing, 39
    - log file, 235
    - managed nodes only, 149
    - memory problem, 218
    - settings, 117
  - synchronization package
    - copying, 200
    - default, 243
    - DNS mapping, 257
    - end user management, 256
    - Informix, 251
    - location, 232
    - locations, 241
    - Microsoft SQL Server, 252
    - my company, 256
    - Oracle, 253
    - Sybase, 254
    - trigger policy distribution, 111, 255
    - UNIX, 249
    - Windows, 250
- ## T
- template
    - MachineTypes\_templates.xml, 112
  - timeout
    - WS Man Client, 219
  - Tomcat server
    - clusters, 179
    - HTTP, 179
    - log file, 236
    - memory, 217
    - performance parameters, 222
    - start/stop, 185

- tools
  - dmatoolgen.bat, 131
  - dmatoolgen.sh, 129
  - removing, 212
  - upload, 129
  - uploading, 127
  - upload UI Launch, 131

- TQL queries, 23, 98
  - modify, 153

- trouble ticket, 26

## U

- UCMDB

- discovery, 146
  - discovery administrators, 24
  - Node Groups, assigning, 108

- UI Launch

- configuring, 127
  - configuring web application, 133
  - installing, 127
  - introduction, 18
  - log file, 235
  - prerequisites, 61
  - removing, 212

- UNIX

- enabling MSI, 134
  - file locations, 229

- upgrading

- HPOM DMA, 119

- uploading

- services, 146
  - tools, 129
  - UI Launch tools (UNIX), 129
  - UI launch tools (Windows), 131

- usermapping.xml, 232

- user profile

- assigning to services, 38
    - Linux, 109
    - UNIX, 109
    - Windows, 115
  - mapping, 110, 115
  - mapping file, 232

- user role

- assigning to services, 38
    - Linux, 109
    - UNIX, 109
    - Windows, 115
  - mapping, 110, 115

- users

- Application Support Engineer, 26
  - HPOM Administrator, 25
  - HPOM DMA, 23, 93, 232
  - HPOM Operator, 26
  - Integrators, 24
  - Service View Designer, 23
  - UCMDB Discovery Administrator, 24

- users.properties, 232

## V

- verifying product licenses, 174

- version

- HP Business Availability Center, 55
  - HP Universal CMDB, 55

- views, 99

## W

- web application, 133

- web service
  - client
    - chunk size, 219
    - export certificate, 180
  - cluster, 179
  - connections, 117
  - credentials, 223
  - IIS extension, 186
  - log files, 235
  - server
    - message size, 221
- Web Service Endpoint Connections, 117
- Windows
  - enable MSI, 135
- WisemanA, 262

## X

- XPL
  - configuration, 147
  - logging parameters, 224
  - performance parameters, 219

