HP Client Automation Enterprise

Application Usage Manager

for the Windows® operating systems

Software Version: 7.80

User Guide

Manufacturing Part Number: None Document Release Date: November 2009 Software Release Date: November 2009



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 1993-2009 Hewlett-Packard Development Company, L.P.

Trademark Notices

Linux is a registered trademark of Linus Torvalds.

 ${\rm Microsoft}^{\$}, {\rm Windows}^{\$}, {\rm and} \; {\rm Windows}^{\$} \; {\rm XP} \; {\rm are} \; {\rm U.S.} \; {\rm registered} \; {\rm trademarks} \; {\rm of} \; {\rm Microsoft} \; {\rm Corporation}.$

OpenLDAP is a registered trademark of the OpenLDAP Foundation.

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

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

OpenLDAP Copyright 1999-2001 The OpenLDAP Foundation, Redwood City, California, USA. Portions Copyright © 1992-1996 Regents of the University of Michigan.

OpenSSL License Copyright © 1998-2001 The OpenSSLProject.

Original SSLeay License Copyright © 1995-1998 Eric Young (eay@cryptsoft.com) DHTML Calendar Copyright Mihai Bazon, 2002, 2003

Documentation Updates

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

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

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

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

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

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

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

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

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

Chapter	Version	Changes
All	7.50	"CM" components for Application Usage Manager and KB Server have been rebranded to "HP Client Automation" as of this release.
		The Agent now installs into this path: Drive:\ProgramFilesFolder\Hewlett-Packard\HPCA\AUM
		Agent

Chapter	Version	Changes
All	7.20	Most components within the HP Configuration Management family of products have been rebranded to HP Client Automation Enterprise (HP CAE). This product has not been rebranded. For more information, refer to the HPCAE Release Notes for Version 7.20.
	Aug 2008	Throughout this guide, several references to "CM" components now refer to "HPCA" components to reflect the correct branding for Version 7.20.
All	7.80	Removed information about RIS-based Portal Management reports since they are no longer supported.
Chapter 1	7.20	Page 14, Hardware and Software Requirements, Added support for SQL Server 2008 and Oracle 11g databases.
Chapter 2	7.50	Page 32, Using Standard Materialized Views or Filtered Materialized Views, added note: The script names may abbreviate "Materialized" to "Mat", as in: StepX_Define Filter Mat Tables and Indexes.sql.
Chapter 2	7.20	Page 26, Defining a Application Usage Manager Database for Microsoft SQL Server, updated procedures for using a SQL Server 2008 database
		Page 28, Defining a Application Usage Manager Database for Oracle, updated scripts for using Oracle 11g database and running the schemas using SQL Developer with Autocommit enabled.
Chapter 2	7.50	Page 47, Adding the USAGE Domain, filenames used to import the Usage Domain changed from USAGE750.xp* to USAGE780.xp*.
Appendix A	7.20 Aug 2008	Page 104, Implementing Application Usage Manager in a Non- HPCA Environment, title corrected from Implementing Application Usage Manager in a Non-CM Environment since other products have been renamed to HPCA for Version 7.20.

Chapter	Version	Changes
Appendix A	7.20 Aug 2008	Page 114, Common Files Required by Application Usage Manager Agent, deleted reference to these files being located in the \Infrastructure directory of the Client Automation Enterprise media; they are only located on the \Usage Manager directory.

Support

You can visit the HP Software support web site at:

www.hp.com/go/hpsoftwaresupport

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

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

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

Most of the support areas require that you register as an HP Passport user and sign in. Many also require an active support contract. To find more information about support access levels, go to the following URL:

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

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

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

Contents

1	Introduction	. 12
	Audience	12
	What is the Application Usage Manager?	12
	Data Collection Types	
	System Requirements	
	Platform Support	14
	Hardware and Software Requirements	
	Platform Support	15
	Processing	15
	Application Usage Manager Environment	15
	Common Infrastructure Requirements	16
	Infrastructure Requirements	17
	Infrastructure Requirements for Reporting	17
	Recommended Software Configurations	18
	Application Usage Manager Agent Operation Overview	18
	Collection Processing	20
	Collection Point Destinations	21
	Agent Processing of Data Collection Request	22
	Executable Inventory Scan and Options	22
	Initiating Collection of Agent Data	
	Portal Web Services and the Application Usage Manager	23
2	Configuring Your Environment	. 25
-	6 6	
	Configuring Your Client Automation environment	25
	Defining a Application Usage Manager Database for Microsoft SQL Server	26

Defining a Application Usage Manager Database for Microsoft SQL Server	26
Defining a Application Usage Manager Database for Oracle	28
Service Pack Installation (If applicable)	30
Optional Features for Database Performance and Maintenance	32
Using Standard Materialized Views or Filtered Materialized Views	

Create an ODBC Connection	33
Update httpd*.rc File	
Configuring the put.cfg file (For Knowledge Base Server)	
Configuring the Database usage.cfg File	40
Installing and Configuring the Knowledge Base Server	
Starting and Stopping the KB Server	47
SQL Server Requirements for the KB Server	
Adding the USAGE Domain	47

3 Aggregation of Usage Data Files with Tier-Level Store and Forward50

Introduction	50
What is Aggregation?	50
Implementation	51
Installing Messaging Server and Configuring Usage Data Files Store and Forward	53
System Requirements for Messaging Server	53
Platform Support	53
Installing Messaging Server with Aggregation Support	53
Configuring Aggregation	54
About the Sections in USAGE.DDA.CFG File	54
Performance	56

4	Application Usage Manager Agent	58
	The USAGE Domain Defined	58
	Significance of Collection Instances	60
	Configuring the Application Usage Manager Agent	60
	The Application Usage Manager Agent Installation using an HPCA environment	66
	Filters	68

69
70
71
72
73
73
74
75

Using Concurrency	80
Initiating Inventory and Usage Collections	82
Initiating Inventory Data Collection	82
Configuring Usage Data Collection	82
Defining a Database Collection Point	
Initiating a Usage Data Collection Request	83
Initiating a Usage Data Re-collection Request	83
Enabling Privacy	84
Internet Explorer Usage Counts for Windows Vista	85

Accessing the Reporting Server	86
Viewing Usage Information Using the Reporting Server	87
Reporting Views for Usage Reports	87
Filtering Usage Management Reports with Reporting Server	88

Application Usage Manager Admin Search Function	90
Creating Criteria, Rules, Rule Sets, and Rule Set Groups	91
Operators AND versus OR	91
Criteria Tab	92
Rules Tab	96
Rule Sets Tab	98
Rule Set Groups Tab	100

Configuring the Application Usage Manger Agent for SSL Communication	ns with
a Secured Portal	112
Modifying the Application Usage Manager Agent	113
Removing the Application Usage Manager Agent	114
Silent Removal of the Agent	114
Common Files Required by Application Usage Manager Agent	114
Collecting Data	115
Configuring Collection Parameters	
Command to Install Usage Database Collection	
Generating Reports	118
Installing the Application Usage Manager Agent and Collection Parameters	118
Index	120

1 Introduction

Audience

This guide was written for system administrators who want to use the HP Client Automation Application Usage Manager (Application Usage Manager) to assess and obtain reports on software usage in their IT enterprises. The Application Usage Manager allows an administrator to know who is using what applications, and how often. Armed with this information, an administrator can increase efficiency by prioritizing and implementing IT projects, accordingly.

The Application Usage Manager agent is installed with or without an existing HP Client Automation (HPCA) infrastructure. However, implementation is much faster and more flexible if you leverage your existing HPCA infrastructure. In order to implement the Application Usage Manager in an HPCA environment, you need a basic understanding of a few components, including the HP Client Automation Administrator CSDB Editor (Admin CSDB Editor) and the Portal, as well as a general understanding of the agent connect process.

What is the Application Usage Manager?

You can use the Application Usage Manager to assess patterns of application usage in your environment. This allows you to facilitate adherence to license agreements, re-provision licenses if needed, and monitor user productivity.

The Application Usage Manager monitors the use of every application on all of your servers, desktops, and laptops. This enables you to:

- Enforce corporate standards by identifying non-standard software and software versions in use within your enterprise.
- Implement license tracking, giving you the ability to purchase and maintain only those licenses that are needed.
- Enable OS migration support by prioritizing software distribution based on actual usage.

• Use reporting to view the actual use of application resources.

The Application Usage Manager can be used in your existing environment whether or not you are currently using HPCA for software distribution. For implementation details regarding non-HPCA environments see Appendix A, Implementing Application Usage Manager in a Non-HPCA Environment.



Figure 1 Application Usage Manager

Data Collection Types

The Application Usage Manager collects two types of application data: usage and inventory.

- Inventory data consists of information about all applications currently installed on a computer.
- Usage data consists of information about what applications were in use over a specific time period.

Usage data incorporates another form of data called concurrency usage. Concurrency usage data is a more specific form of usage data.

Regular usage data is collected on a daily basis anytime an application is used during the course of a day, while concurrency data can be collected for a single application over a period of time as short as fifteen minutes. This ability allows for capacity planning as well as provides specific data to organizations that may be interested in migrating users into a terminal server environment.

System Requirements

Platform Support

• For more information about the platforms that are supported in this release, refer to the accompanying *HPCA Release Notes*.

Hardware and Software Requirements

Application Usage Manager Knowledge Base

SQL Server 2005 or SQL Server 2008

Oracle 10g, or 11g Rel 1. Apply the latest Oracle patchset.

• Reporting

Reporting Server, v5.00 or above

Application Usage Manager Administrator (formerly called the Rule Editor)

• Applications and Infrastructure

Application Manager or Application Self-Service Manager Configuration Server Administrator CSDB Editor Integration Server (typically, from the Portal)

Platform Support

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

Processing

You can distribute and install the Application Usage Manager agent on your computers using your existing Client Automation infrastructure. Default HPCA-defined installation settings install and configure the Application Usage Manager agent to perform executable inventory scanning, application usage, and usage data collection through predefined Application Usage Manager packages. The next time an agent connects to the Configuration Server, the package is delivered and Application Usage monitoring begins automatically.

Periodically, the usage data is collected based on user-defined parameters. This data is sent to a predefined collection point for further processing. Collection points may be a network share or an HPCA Portal destination. This location is monitored by the Knowledge Base Server, which in turn extracts the usage data from the files collected from each agent computer and loads this data into your SQL-enabled database, making the data available for reporting purposes. Reports can be generated using the Reporting Server.

Application Usage Manager Environment

The Application Usage Manager has different infrastructure requirements, based on whether or not HPCA is being used to manage the environment.

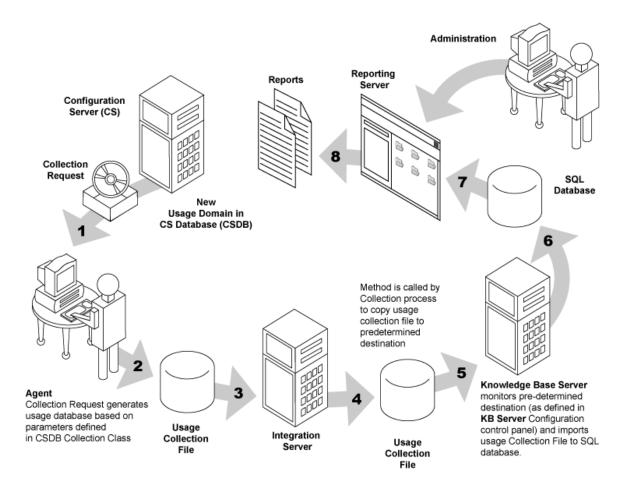


Figure 2 Application Usage Manager Environment

Common Infrastructure Requirements

Common infrastructure requirements are needed for both HPCA and non-HPCA management of the Application Usage Manager environment to capture usage data on the agent and move the data to a server, and ultimately to an SQL database for reporting purposes.

Common infrastructure includes the following computers with the required software installed:

- Monitored Agent or Server Application Usage Manager Agent and its collection configuration
- SQL Server or Oracle Database Microsoft SQL Server and its enterprise management tools (may be an MSDE version for evaluation) or an Oracle database with SQL Plus tools.
- **Knowledge Base Server** The KB Server imports the usage data into the database.
- Usage Manager Administrator Application Usage Manager Administrator provides a Rule Editor.

For information regarding non-HPCA management of the Application Usage Manager see Appendix A, Implementing Application Usage Manager in a Non-HPCA Environment.

Infrastructure Requirements

In addition to the common infrastructure requirements, additional components must be available for HPCA management of the Application Usage Manager environment. HPCA infrastructure requires the following computers and installed software:

• Administrator

This is the HP Client Automation Administrator selection on the Windows Start menu.

- **Configuration Server and Database** Configuration Server Database requires the PRIMARY File USAGE Domain.
- **Portal** The Portal is typically used.
- Enable HTTP File Copy

Infrastructure Requirements for Reporting

The infrastructure needed to support reporting offers choices, based on whether the Reporting Server has been installed and whether the Portal is available. The reporting software may be installed by anyone who requires the ability to view and generate reports.

• Reporting Server 5.00 or above

Recommended Software Configurations

A single server may have one or more software components installed to minimize the number of computers required. The following are recommendations for consolidating software:

SQL or Oracle Database Server

To minimize hard-drive thrashing, the SQL or Oracle database server should have at least two hard drives. Each drive would store:

- The SQL database
- Collection files from each monitored machine

Knowledge Base Server

may be installed on:

- SQL or Oracle Database Server (recommended)
- Portal
- Another server

Application Usage Manager Administrator

may be installed on the:

- Administrator's workstation (recommended)
- Knowledge Base Server

Agent for Application Usage Manager – **Collection File Destination** The Application Usage Manager generates files on the monitored machines that contain both the current executable inventory and the usage information. This information is transferred through the network so it can be imported into an ODBC database. To eliminate network transfer during database import, it is recommended that collection files be placed on the Knowledge Base Server when it also serves as the SQL or Oracle database server machine.

Application Usage Manager Agent Operation Overview

The Application Usage Manager agent supports monitoring of all executable usage.

Once monitoring has started, there are three usage files on the agent machine: the **active application monitoring file**, the **history file**, and the **collection file**.

Active Application Monitoring File

• Contains current application usage information, including (where available):

Machine name

Machine domain name

OS major, minor, build versions

User name

User domain name

Vendor name

Product name

Product version

Application name

Application version

Original application name (if renamed)

Application description

Application module file type

Path name application was launched from

Logical root folder name (i.e., ProgramFilesFolder)

Remaining path name

MD5 hash

Link time

Number of times application was launched

Number of seconds application was active

Number of seconds application was in the foreground or "in-focus"

History File

• Data will be accumulated in a history file by machine, user, executable, and day. Note that data is summarized by day in the history file.

- The usage history file will be maintained for a designated period (default is the last 12 months).
- Old data is aged out of the file.
- The agent history file will maintain separate entries for all executable inventory and usage data reported to each database.

Collection files

- Contains the usage and current executable inventory data that is to be imported into a specific SQL Server or Oracle database. Data collection will be done on a per database basis.
- Each database has a filter policy associated with it that contains a set of filtering rules. A collection file is built for each database.
- There can be any number of usage monitor databases that can request the same or different data from any agent based on the filtering rules.
- Filter policies will be maintained for each database on the agent or as objects in the Configuration Server.
- The agent-generated collection file must be sent to the correct database import path. The Knowledge Base Server will perform importing of the collection data file. The Portal performs the role of moving the collection files to the database import path location.
- When implemented through HP Client Automation, the default collection file name is the &ZOBJID of the UMCOLLCT Class.

Collection Processing

When collection is requested for a database, the agent will compare the current archive data against the reported data for that database. All file inventory data will be compared. Usage data is only compared for files that pass the inclusion filter. Any differences in inventory or usage are added to the collection file.

Once the collection file has been created, it is sent to the destination defined in the PRIMARY.USAGE.UMDESTPT class, COLLDEST instance attribute, or the USDBCOLL.ini **CollectionPoint** parameter for HPCA or non-HPCA implementations.

To minimize bandwidth requirements, the collection files contain only what has not yet been sent to the specific database requesting the collection. These files also contain data aging and deletion information for removing old data from the database.

The history file contains all usage data, regardless if it has been requested for upload into a database for the machine and all of its users. The history file contains up to one year's data and as new days are added, data older than one year is deleted. The number of months is determined by the History Retention Months setting. This feature allows a database collection process to modify policy collection filters to capture any data that is up to a year old. If a new database is added as a destination point, then it can request any of this data from any machine that the Application Usage Manager has monitored either presently or in the past.

Collection Point Destinations

A collection point is a directory destination to which a collection file is copied, and then automatically imported into a SQL database by the Knowledge Base Server.

Automated Import

Automated import directories are watched by the Knowledge Base Server automated import service. Each time a new collection file is placed in an autoimport directory, the Knowledge Base Server will recognize this and then:

- Connect to its pre-configured SQL database through a system-level ODBC connection.
- Import the contents of the collection file into the SQL database.
- Archive the collection file once the import is successful, or copy it to an error directory should the import fail for any reason.
- Perform a rollback of the import if the import is unsuccessful.

Collection Destination Point Unavailable

If a collection request fails to successfully copy the current usage data, then the collection file is placed in the Usage Manager\Collect directory with the file name DatabaseName.USDBase, where DatabaseName is the file name set in the DBNAME instance of the PRIMARY.USAGE.UMDBASE class, or the USDBCOLL.ini **DatabaseName** parameter for non-CM or non-Client Automation implementations. This file can then be manually collected by copying it from the machine, or it will be recreated with the latest application usage data and then collected when the agent receives the next collection request.

Agent Processing of Data Collection Request

The monitoring process collects data for every executable that has been run on the machine. This data is saved in the **active monitoring file**. Since administrators need reports on what exists on the machine, but has not been used, an **executable inventory** is also run to augment the active usage data collected.

Executable Inventory Scan and Options

Since the inventory capture process may take several minutes to complete, the inventory process can be configured during installation to be collected at a pre-defined time, daily or weekly at, for example, 1:00 AM Sunday. The request for data collection can aggregate this pre-collected inventory data with the current usage monitoring data at the time of the collection request. Also, the inventory collection can be configured to run at the time the collection request is issued to provide a more up-to-date inventory. Since the executable file inventory scan can take several minutes, the request for collection is performed synchronously once the inventory scan has finished.

Initiating Collection of Agent Data

Collection of monitoring data is initiated by running an executable with the appropriate command line parameters. Each collection request is SQL database-specific and the technique of launching an executable allows one or more collection requests to the same agent computer for either the same or differently filtered data destined for different SQL databases.

The usage time for appropriate applications is collected based on parameters that you select. This usage time should not be confused with focus time (the time that an application was in focus, that is, the active window in the forefront on a user's desktop).

Portal Web Services and the Application Usage Manager

The Application Usage Manager requires components that run under the control of a Portal or other another HPCA server's Web Services. The Portal or Integration Server provide Web services that are shared by all loaded modules in their respective resource control file (httpd*.rc), resulting in a single entry point for all HTTP (Web-based) requests. The Application Usage Manager leverages the abilities of these servers to perform HTTP-based file copying. If the Portal or Integration Server is secured using SSL, HTTPS-based file copying is supported.

The Portal can be used to move the application usage data collection files from the monitored machines to one or more server directories. From the server directories, the data are imported into a database.

2 Configuring Your Environment

Configuring Your Client Automation environment

Before you can use the Application Usage Manager, your Client Automation environment must be prepared. To configure your components to use the Application Usage Manager you will need to complete the following tasks:

- 1 Create and configure your Application Usage Manager database.
 - Define a SQL Server database or Oracle database.
 - Execute the provided script files to configure the Application Usage Manager DB table schema.
 - Configure your ODBC connection.
- 2 Install and configure Application Usage Manager software:
 - Configuration Server

Installation requirements, as well as instructions for installing the Configuration Server, are documented in the *HPCAE Configuration* Server, Portal and Enterprise Manager Getting Started Guide.



Make sure you select the **Application Usage Manager** option during the installation.

– Administrator

Installation requirements, as well as instructions for installing the Administrator, are documented in the *Administrator User Guide*.

- Knowledge Base Server (one per SQL database) and a configured ODBC connection.
- Portal

You must have an active Portal available for processing requests to copy the application usage files (.USDB) from each agent computer to a central location.

General requirements and instructions for installing the Portal are documented in the *HPCAE Configuration Server*, *Portal and Enterprise Manager Getting Started Guide*. The Integration server that the Application Usage Manager uses comes along with the Portal.

The Integration Server is also installed with several infrastructure components, such as the legacy Proxy Server, Policy Server or Patch Manager Server, and these can also be used for Usage reporting.

Application Usage Manager Administrator

- Configure your Application Usage Manager agent using the Admin CSDB Editor.
- 3 Install the Application Usage Manager agent.

The Application Usage Manager requires that the USAGE Domain be included in your Configuration Server Database. The USAGE Domain is included with the Configuration Server Database as of Version 4.x. If you migrated from an earlier version of the Configuration Server Database, you may need to import the USAGE Domain into your database. For more information, see Adding the USAGE Domain on page 47.

• The following sections describe the steps needed to configure your environment. Installing and configuring the Application Usage Manager agent (steps 3 and 4 above) is covered in Chapter 4, Application Usage Manager Agent.

Task 1 Create and Configure Application Usage Manager Database and Schema

The Application Usage Manager Knowledge Base is a database that contains the application usage data that is needed to effectively manage the enterprise including information about the machines, users, files, and file usage. It is designed such that application packaging and other state file data generated by the HP Configuration Management Extensions for Windows Installer and Inventory Manager can be leveraged during data analysis and reporting.

Refer to the appropriate set of instructions below to define and configure your database schema for a SQL Server database or an Oracle database.

Defining a Application Usage Manager Database for Microsoft SQL Server

New Application Usage Manager databases are created using the SQL data definition language files referenced below.

Use the following tasks to create the Application Usage Manager database for a Microsoft SQL Server database. The first task creates the database and the second task creates the table schema.

To create the Application Usage Manager database for SQL Server

- 1 Open the SQL Server Enterprise Manager or SQL Server Management Studio.
- 2 Right-click the Database folder for the appropriate server and select **New Database**. Complete the entries as follows:

General Tab

— Name

Usage (or a name of your choice excluding blanks and underscores)

- Collation Name:
- Usage Schema Supports Unicode. Leave the collation as server default or Choose a collation name of your choice, for example: French_CI_AS or Japanese_CI_AI_KS.

Data Files Tab

— File Name

 $Usage_Data$ (or name of your choice excluding spaces). Set the initial size to 1000 MB.

— Select Automatically grow file by 20%



For improved performance, we recommend that you create the Application Usage Manager database on a drive other than the drive that is used to create state files.

Transaction Log Tab

— File Name

 $Usage_Log$ (or a name of your choice excluding blanks). Set the log size to 250 MB.

- 3 Click **OK** to create the database and log files. The Application Usage Manager database is now added to the Databases folder of your server, within the Server Manager.
- 4 When you are finished creating the database, create the database table schema.

To create the table schema for SQL Server

- Within the SQL Server Enterprise Manager, in the Tools menu, select **SQL Query Analyzer**.
- 2 Make sure the drop-down box displays the database you just created.
- 3 From within the Query Analyzer or SQL Server management Studio, open your Application Usage Manager media and navigate to the appropriate folder for your SQL Server version: \SQL Server\SQL Server 2005\ or \SQL Server\SQL Server 2008\.
- 4 Execute each SQL script in the directory in order (the scripts are named accordingly) beginning with Step 2.

Use Query Execute or press F5 to run each script.

At the end of the query execution you will see a series of messages possibly displaying sysdepends dependency and several row insertions. This indicates a successful installation of the database definitions.

- Step2_Define_UsageManager_Tables.sql
- $Step3_Define_Common_Tables.sql$
- Step4_Define_Views.sql
- Step5_Define_Stored_Procedures.sql
- Step6_Insert_Common_Functions.sql
- Step7_Insert_Common_DefaultData.sql
- 5 Close the SQL Query Analyzer.
- 6 Continue with Create an ODBC Connection on page 33.

Defining a Application Usage Manager Database for Oracle

First create a database for Oracle of your choice. If you require a Unicode Oracle database with a Unicode data type, create a Unicode database with a DB Character Set that supports Unicode data, preferably the DB character set Al32UTF8 and National Character Set UTF8.

Configuring your database schema for Oracle requires the execution of several SQL script files that are provided with your Application Usage Manager media in the Oracle directory. Copy these files to a location accessible by your Oracle administrator. Make sure to use the files located in the appropriate Oracle version directory. The scripts will, by default, install the database into the user's schema.

To configure your Application Usage Manager database schema for Oracle

- 1 For the scripts to run successfully, replace the %Install_Path% in Step1_Define_Tablespaces.sql and make sure that it references the Oracle installation path. (For example a typical %Install_Path% with a default installation of Oracle 11g would refer to C:\app\Administrator and Oracle 10g would refer to c:\oracle\product\10.2.0 and on Oracle 9i would refer to C:\ORACLE)
- 2 Choose an Oracle application and logon as database administrator:

Oracle 10g users:

Use the Oracle SQL Plus Worksheet application and log on as a database administrator.

Oracle 11g users:

Oracle 11g users may use the SQL Plus or Oracle SQL Developer *with the Autocommit feature enabled* to execute the scripts; log on as database administrator.

To enable Autocommit in Oracle SQL Developer:

- a From Oracle SQL Developer, go to the Tools \rightarrow Preferences \rightarrow Database \rightarrow Worksheet Parameters page.
- b Ensure Autocommit is checked; if necessary, save your changes.



Certain SQL PLUS commands may be ignored when executing the schemas using SQL Developer; you can ignore these warning messages.

- 3 Make sure the folders as described in the comment text of the script Step1_Define_Tablespaces.sql (\ORADATA\CM\DB, \ORADATA\CM\REDO01 and \ORADATA\CM\RED002) are created before running the scripts.
- 4 Review the tablespaces parameters and change them to suite your database needs and physical hard drive space.
- 5 Execute the SQL scripts that are just modified by you, in order, as determined by their filenames, making sure to include the correct path to the script locations. Review the comments within each script (step 1 through step 5).

For example, if your SQL scripts are located in the directory \AppUsageManager\Oracle\Schema, you would execute the first script by typing

SQL> @C:\AppUsageManager\Oracle\Schema\Step1_Define _TableSpaces.sql

followed by Enter.



Make sure to select the correct group of SQL files depending on the version of Oracle you are using:

- Oracle\Oracle_10g
- Oracle\Oracle_11g

For Oracle 10g or 11g: (These scripts are version-specific.)

- Step1_Define_TableSpaces.sql
- Step2_Define_Common_Roles.sql
- Step3_Define_Common_Tables.sql
- Step4_Define_UsageManager_Tables.sql
- Step5_Insert_Common_DefaultData.sql

For example, if your SQL scripts are located in the directory \AppUsageManager\Oracle\Schema, you would execute the first script by typing:

SQL> @C:\AppUsageManager\Oracle\Schema\Step1_Define _TableSpaces.sql

followed by Enter.

If you are using SQL Developer, browse and open the file, and click $\ensuremath{\textbf{Run}}$ Script.

- 6 Make sure each script executes properly.
- 7 Log on as SYSDBA and execute Step6_Create_CMDBA_Role.sql.



Additional scripts are located in the \Optional_Features directory for performance enhancements or for removing the Application Usage Manager Database. They are not required here.

Service Pack Installation (If applicable)

When you are finished executing the SQL scripts, check to see if the SQL or Oracle version directory folder on the Application Usage Manager media includes a ServicePacks folder.



Schema Version 7.80 does not require any service packs.

- If the ServicePacks folder does not exist, continue with Create an ODBC Connection on page 33.
- If a ServicePacks folder exists, you need to apply the supplied service packs located within the Oracle version directories. There are two types of service packs supplied, **required** and **optional**. Apply the required service packs first, in the proper order, then, if desired, apply the optional service packs.

To apply any supplied service packs for SQL Server

- 1 Within the SQL Server Enterprise Manager, in the Tools menu, select **SQL Query Analyzer**.
- 2 Make sure the drop-down box displays the correct database.
- 3 From within the Query Analyzer, open your Application Usage Manager media and navigate to \SQL server\SQL Server 2005\ServicePacks or \SQL server\SQL Server 2008\ServicePacks.
- 4 Execute the service pack SQL scripts. Make sure each script executes properly.

To apply any service packs for Oracle

- 1 The service packs are located within the Oracle version directories within the ServicePacks folder.
- 2 Use the appropriate Oracle application (SQL Plus for 9i and 10g or SQL Developer for 11g) and login as a database administrator.
- 3 Execute the service pack SQL scripts located within the ServicePacks folder within the proper Oracle version directory of your Application Usage Manager media, making sure to include the correct path to the script locations. Run the scripts in order as determined by their filenames.
 - After applying the SERVICE_PACK_XXX.SQL files, the Oracle server does not recompile all of the parent views when a child view is updated. This may leave a number of views invalid after applying the updates. To make sure all views are valid, select all of the views in the Oracle Enterprise Manager, rightclick and select **Recompile**. This will re-validate all of the views.

Optional Features for Database Performance and Maintenance

An Optional Features folder within the SQL Server and Oracle folders include several scripts that can be applied to enhance reporting performance.

Using Standard Materialized Views or Filtered Materialized Views

The Materialized View options are explained below. Both enhance reporting performance. Either one can be optionally applied to a database. Refer to the comments in the scripts for additional information.



The script names may abbreviate "Materialized" to "Mat", as in: StepX_Define Filter Mat Tables and Indexes.sql.

Standard Materialized Views (SMV) – A feature where all the views (which is what the reports access) are converted into tables, and indexes are added to enhance the query speed.

Filtered Materialized Views (FMV) – A feature similar to SMV, but differs in that it requires filters to be applied at the time the views are converted into tables. The filters are stored in a separate table. As an example, if a filter for Notepad.exe is selected, the FMV table will be populated with only notepad details for all the devices. In this way the customer can choose to see only those applications which are important to them.

To apply the scripts for SMV or FMV:

- 1 Stop the service for the **HPCA Knowledge Base Server.** The service may be stopped and started through the Administrative Tools\Services options of Windows Control Panel.
- 2 Use normal procedures to execute the database scripts, in the given order, provided in the following locations:

For SQL Server:

\SQL Server\Optional Features\Filter Materialized Views

or

 \SQL Server \Optional Features \Standard Materialized Views

— For Oracle:

\Oracle\Optional Features\Filtered Materialized Views

 \mathbf{or}

\Oracle\Optional Features\Standard Materialized Views

Each of the above locations also includes a script to remove the view from your database. For example, for SQL Server and Filtered Materialized Views, the script name is:

SQLServer - Remove All Filter Mat Tables and Indexes.sql.

Create an ODBC Connection

To create an ODBC connection

1 From your system's control panel, go to **Administrative Tools** and double click **Data Sources (ODBC)**.

Name	Driver	A <u>d</u> d
LocalServ	ver SQL Server	<u>R</u> emove
		<u>C</u> onfigure

2 Click the **System DSN** tab and then click **Add**.

	Name Microsoft FoxPro VFP Driver (*.dbf) Microsoft 0DBC for Oracle Microsoft Paradox Driver (*.db) Microsoft Textoriver (*.txt; *.csv) Microsoft Text-Treiber (*.txt; *.csv) Microsoft Visual FoxPro Driver Microsoft Visual FoxPro-Treiber SOL Server	V▲ 1. 2. 4. 4. 4. 4. 1. 1. 2. ↓ •
--	---	--

- 3 A list of drivers is displayed. Select SQL Server (if the database you just installed is in Sql server) or Microsoft ODBC for Oracle (if the database you installed is in Oracle).
- 4 For an Oracle database, enter the Data Source Name, Description, Username, and Server.
- 5 For Sql Server, select **SQL Server** and click **Finish**.

The initial Microsoft SQL Server DSN Configuration window opens.

6 Enter the appropriate name (any name of your choice), a description and the server name. Enter the Server name manually or select it from the drop down list.

Create a New Data Sour	ce to SQL Server
Select a divier to Select	This wizard will help you create an ODBC data source that you can use to connect to SQL Server. What name do you want to use to refer to the data source? Name: ApplicationUsageManager How do you want to describe the data source? Description: Which SQL Server do you want to connect to? Server:
	Finish Next > Cancel Help

- 7 Click Next.
- 8 For the Authenticity of the login ID option, select the option, **With SQL** Server authentication using a login ID and password entered by the user.

Microsoft SQL Server DS	N Configuration	×
Select a diriet to me of dataset biological biolog	How should SQL Server verify the authenticity of the login ID?	
	Client Configuration Client Configuration Client Configuration Client Configuration Client Configuration options. Login ID: Administrator Password:	
	< <u>B</u> ack <u>N</u> ext> Cancel Help	

- 9 Enter the Login ID and password, and click Next.
- 10 Select the database Name from the drop-down list or enter it manually.

- 11 The remaining options can be left with their default settings.
- 12 Click Next.

Microsoft SQL Server DSM	Configuration
Select a divier to: Internet Access oil dBase fr oil dBase fr internet Access oil dBase	 Change the language of SQL Server system messages to: English Use strong encryption for data Perform translation for character data Use regional settings when outputting currency, numbers, dates and times. Save long running queries to the log file: C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\QU Browse Log QDBC driver statistics to the log file: C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\ST Browse
	< <u>B</u> ack Finish Cancel Help

- 13 Click Finish.
- 14 The ODBC connection is created. Test the connection by using the Test Data Source feature.

Task 2 Configure the Portal and Web Reporting Components



Oracle requires an Oracle agent be installed on the computer where the Portal is installed, as well as on the computer where the Knowledge Base Server is located.

You must have an active Portal available for processing requests to copy the application usage files (.USDB) from each agent computer to a central location. This server listens for requests to copy the usage files from the individual devices and transfers them to a common collection point. Once transferred, the KB Server monitors this common collection point and imports the data into the appropriate database.

A single Portal may server as the focal point for gathering usage files that are to be imported from each agent into different SQL databases. However, it is recommended that only one server be used to service a single SQL database. The KB Server may run on the same computer as the Portal. Your Portal must be restarted after configuring the components required by the Application Usage Manager.



Before copying and replacing any files on the Portal, make sure to create a backup.

Update httpd*.rc File

Update the httpd*.rc file of the server (Portal) that will copy the application usage files (.USDB) from each agent computer to a central location.

To update an httpd*.rc file for a Portal

Stop the **HPCA Portal** service through the **Administrative Tools\Services** options of the Control Panel.

Edit the httpd-managementportal.rc file located in the folder: [ProgramFilesPath]\Hewlett-Packard\CM\ManagementPortal\etc.

Add the following plug-in commands to the existing module load statements near the end of the file:

```
# HTTP Put Server
module load put
# Padia Usage Manage
```

Radia Usage Manager
module load usage



These module load statements may exist in the httpd*.rc file as comments. To activate them, delete any characters in front of the word module.

Save your changes and restart the HPCA Portal service. When you start the service, this updated httpd-managementportal.rc file is used.

Configuring the put.cfg file (For Knowledge Base Server)

When the Portal is started with an httpd*.rc file that includes the module load put command, a put.cfg file is created in the target \ManagementPortal\etc directory. The put.cfg file identifies and correlates an HTTP URL with a destination directory to which to copy the .USDBASE files.

If you already have the put.cfg file in your \ManagementPortal\etc directory, it will not be overwritten.

The file must be updated if you intend to use multiple SQL databases.

No editing of this file is required unless you want to change the default location of the automated import directory that the KB Server monitors and will use to update the SQL database. The default location is the \etc\Usage\KB_Mgr1_Usage subdirectory under the root directory of where the Portal is installed. For the Portal, this default directory is:

```
C:\[ProgramFilesPath]\Hewlett-Packard\CM\ManagementPortal\
etc\Usage\KB_Mgr1_Usage
```

Using Multiple SQL Database Destinations

To configure the Portal to accept usage database files to be imported into multiple SQL databases, modify the put.cfg script to create a new destination directory for each of the unique SQL databases. Do this by adding the text in the code sample below between the Begin and End comment lines. Lines beginning with a pound sign (#) are comment lines that are not processed.

The following is a sample script:

```
_____
# - CMIS Application Usage Manager Destination Directories - BEGIN -
# - The following two lines create a directory that a
# - Knowledge Base Server service is watching so it can autoimport
# - Application Usage Manager information into a SQL database. This
# - directory creation can be extended to any number of specific
# - directory/Knowledge Base Server/SQL database environments.
# -
# - This request is configured as the Collection Point destination
# - For example:
# -
    CollectionPoint=HTTP://192.168.101.151:3466/KB_Mgr1_Usage/
# -
# _____
# - CMIS Application Usage Manager Destination Directories - BEGIN
file mkdir $Config(ROOT)/etc/usage
file mkdir [set dir "$Config(ROOT)/etc/usage/KB_Mgr1_Usage"]
Put_AddRoot /KB_Mgr1_Usage $dir
# ------
# - The 'file mkdir' line defines the physical directory that is the HTTP
# - request file destination.
# - The 'Put_AddRoot' line defines the last node in the HTTP request.
# - For example:
# -
    HTTP://192.168.101.151:3466/KB_Mgr1_Usage/
# - would result in the Usage Collection File being copied to the directory
# - <<CMIS Path>>\etc\usage\KB_Mgr1_Usage
# ------
# - Repeat the above two file mkdir lines to create additional
```

```
# - CollectionPoint/KB Server auto import directories
# ------
#file mkdir $Config(ROOT)/etc/usage
#file mkdir [set dir "$Config(ROOT)/etc/usage/KB_Mgr2_Usage"]
#Put_AddRoot /KB_Mgr2_Usage $dir
```

----- CMIS Application Usage Manager Destination Directories - END -# -----

In the sample script an enterprise and a local level SQL database are used by the organization on a single Portal. There is a Knowledge Base Server automated import service running on two separate computers. One of these monitors activity in the KB_Mgr1_Usage folder and the other monitors activity in the KB_Mgr2_Usage folder.

The file mkdir[set dir "physical directory name"] command sets the physical directory that the usage files are going to be copied into from the HTTP_PUT request.

The Put_AddRoot /logical_name \$dir command associates the http logical collection point with the name of the physical file into which the file is copied.

The collection point is defined in the Configuration Server Database's PRIMARY.USAGE Domain in the UMCOLLCT Class object as:

```
HTTP://Portal_Server_IP_destination:port_number/
Logical_name
```

For example, by setting a collection point destination of:

HTTP://192.168.0.150:3471/KB_Mgr1_Usage

The agent usage files will be sent to the Portal and copied into the directory:

<Portal_Path>\usage\KB_Mgr1_Usage\UsageFile.USDBase

The above entry configures the Knowledge Base Server to watch for activity on the directory <<Portal_Path>>\usage\KB_Mgr1_Usage and perform automated import processing of the data into its associated SQL database once the file has been copied.

After copying and editing the files, start the Portal Server. The following folder is created under the base install directory of the Portal Server:

```
\etc\usage\KB_Mgr1_Usage.
```

Defining an SSL-Secured Collection Point

For an SSL-secured Portal, the collection point is defined using HTTPS and the secure port number, such as 443:

HTTPS://Integration_Server_IP_destination:secure_port_num/
Logical_name

Configuring the Database usage.cfg File

The \Usage folder of the HPCA media contains this directory:

\IntegrationServer\etc

Copy the entire \mc folder from the above \Usage Manager\IntegrationServer\etc media location to your \ManagementPortal\etc directory. By default, this directory is:

```
C:\[ProgramFilesPath]\Hewlett-Packard\CM\ManagementPortal \etc
```

- 2 Also copy the appropriate usage*.cfg configuration file from the Usage Manager\IntegrationServer\etc media location to your Portal Server \etc directory; choose the configuration file for your database type:
 - For Oracle, copy usage_Oracle.cfg
 - For SQL, copy usage_SQL_Server.cfg
- 3 Once copied, rename this file to usage.cfg.
- 4 Then, using a text editor, open the usage.cfg file and enter your ODBC name, user ID, and password. You may also change the DSN value if required. The next code sample is an example of a configured usage.cfg file that uses sa as the user name and a blank password.



The user ID used in the usage.cfg file must have sufficient access rights to select and execute stored procedures and functions.

A sample configured usage.cfg file for SQL Server will look like the following:

```
usage::init {
    DATABASE "SQLSERVER"
    DSN "ApplicationUsageManager"
    DSN_USER "sa"
    DSN_PASSWD ""
    DL_DATEFMT {%Y-%m-%d %T}
}
```

Task 3 Install the Application Usage Manager Administrator

The Application Usage Manager Administrator allows you to create rules that will enable you to select which data will be used to create your usage reports. Install this component on an administrator's workstation (preferred), or on the computer that houses the Knowledge Base Server.

To install the Application Usage Manager Administrator

- 1 From your HP Client Automation Enterprise media for the Application Usage Manager, navigate to the Usage Manager Administrator folder.
- 2 Double-click **UsageManagerAdministrator.msi** to start the installation.
- 3 Click **Next**. The end-user license agreement dialog box opens.
- 4 Read and accept the HP Software License terms. Click **Next**. The installation location dialog box opens, showing the default location.
- 5 If you want to install the Application Usage Manager Administrator in a different location, click **Browse** to navigate to the location.
- 6 Click Next. The Ready to Install dialog box opens.
- 7 Click Install.
- 8 When the installation is finished, click **Finish**.

The Application Usage Manager Administrator is installed and a shortcut is added to your Programs under **HP Client Automation Usage Manager Administrator**. Once an ODBC connection to a database is established, use the start menu shortcut or the RADPIMGR.exe file to access the Application Usage Manager Administrator. By default, RADPIMGR.EXE is located in the directory: [ProgramFilesPath]\Hewlett-Packard\CM\Usage Manager Administrator\bin\.

Task 4 Install and Configure the Knowledge Base Server

≻

Oracle requires that an Oracle client be installed on the computer where the Knowledge Base Server is located, as well as the computer where the Portal is installed.

The **Knowledge Base Server** provides services to manage the Application Usage Manager Knowledge Base. It also services requests for a Knowledge Base available through the Extensions for Windows Installer product. The Knowledge Base Server installs as a Windows service.

The Knowledge Base Server performs automated import processing of the state files and other files into the Knowledge Base. Automated importing may be defined for the following types of directory structures:

• Application Usage Manager Collection files extension (USDBase).

- Simple state file automated import directories containing state files (.ISState extensions). These are typically created by the Packager for Windows Installer or the Patch Manager.
- Configuration Server service export directories that have required subdirectory structures that are built by the Extensions for WI features which enable extraction and conversion of packages contained in Services to .ISState file formats.

The Knowledge Base Server automated import server runs independently of the Configuration Server to import files found in the automated import directories.

Installing and Configuring the Knowledge Base Server

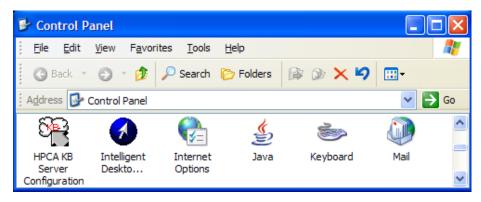
For installation instructions, refer to the *Knowledge Base Server Guide*, available on the HP Software support web site.

After an ODBC connection to a database is established, configure the Knowledge Base Server using the Windows Control Panel application KB Server Configuration. When finished with the configuration, start the **HPCA Knowledge Base Server**.

Configuring the Knowledge Base Server

Configuration for the Knowledge Base Server is controlled through the HPCA KB Server Configuration control panel.

Figure 3 HPCA KB Server Configuration icon on Control Panel



To access the HPCA KB Server Configuration from Control Panel

Click Start→Settings→Control Panel.

2 Double-click the HPCA KB Server Configuration icon.

The Knowledge Base Server Configuration window opens.

🕆 HP Client Automation K	Knowledge Base Server Configuration	
Ф НРСАК	nowledge Base Server Configuration	
Create / Maintain the Knowle Knowledge Base Name:	edge Bases for each installed and configured database Add Edit Delete	9
Create / Maintain the Tasks	which does Import and Maintenance of data	
Task Name	Directory Add Iask	
	Delete Task	
	Modify Task	
	Save Configurati	ons
	_ <u>R</u> evert Configurat	ions
	Exit	
General Configurations for th Log Path Log Level Database Reconnect Import Directory Scan Switch Tasks after	he Knowledge Base Server C:\Program Files\Hewlett-Packard\CM\Knowledge Base Serv Frrors / Other 5000 msecs 5000 mins	

To configure the KB Server automated import directories

1 Click **New** to add a new Knowledge Base data source. The New Knowledge Base – Configuration dialog box opens.

New Knowledge Base - Configuration	×
Knowledge Base Name: Data Source Name: ApplicationUsageManager	ОК
User Name:	Cancel
Password:	

2 Enter the following information:

Knowledge Base Name:	Enter the Knowledge Base name. (Any name of your choice)
Data Source Name:	Enter the Data Source Name (DSN).
User Name:	Type a user ID that has owner authority for the database.
Password:	Type a valid password for the user ID.

- The KB Server administrator must supply a logon ID and password for the person who has rights to access the SQL database. This ID must have full access rights to the database objects including table and stored procedures. Enter the ID with these rights and its password.
- 3 Click OK.

When you are finished adding a Knowledge Base, create a task by clicking **Add Task**.

i ask i ype.	HPCA Application Usage Manager (Collection Files	•
Task Name:			
Import Directory:			Browse
After Import:	Archive		

4 From the Task Type drop-down list, select one of the following tasks related to Application Usage Manager:

HPCA Application Usage Manager Collection Files Create a task of this type to define your automated import directory for usage files that are collected.

HPCA Application Usage Manager Purge Criteria Use this task to purge usage data from your database. You must define whether the purging will take place daily, monthly, or yearly. Recommended settings: Daily: 31-62 days Monthly: -1 Yearly: -1

— HPCA Application Usage Manager Move File(s) Use this task to move the USDBase files from your Archive / Error directory to the import directory (for re-import purposes). Refer to the *Knowledge Base Server Guide* for more information on the Move File(s) task.

5 The type of task you select will determine what information is required in the following text boxes. Depending on the task you select, some of these text boxes may not appear.

Task Name:	Type a name for the task, for example, Collection Files.
Import Directory:	Enter the path for the directory from which files will be imported. Click Browse to navigate to it. For example:
	C:\Program Files\Hewlett-Packard\CM\ ManagementPortal\etc\Usage\Kb_Mgr1_Usage
After Import:	Select the action taken after import, Archive, or Delete. This option allows you to remove the files from the import directory immediately after they are imported.

- 6 Click **OK** and you are returned to the KB Server Configuration window. It now displays the information you just entered.
- 7 Click **Save Configurations** to save the just entered configuration settings. Click **OK**.

Task Name		Directory	
Collection Files			Add <u>T</u> ask
Licensed Vendor Application	ns Rule Definitions		
			<u>D</u> elete Task
			Modify Task
			Save Configurations
			<u>Revert Configurations</u>
•		Þ	E <u>x</u> it
General Configurations for th Log Path	_	erver swlett-Packard\CM\Knowledge Base Serv	View Log
Log Level	Errors / Other		
Database Reconnect	5000	msecs	
Import Directory Scan	5000	msecs	
Switch Tasks after		mins	

- 8 To complete the KB Server configuration, edit the following text boxes located at the bottom of the KB Server Configuration window:
 - Log Path (default is $C: \setminus$)

Default log path for AutoImport processing status information. All exceptions are logged as well as successful imports and \Notify file deletions after successful imports of HPCA Service state files.



The log path must exist before starting the service for the KB Server.

— Log Level

Select the level of logging from the drop-down list. Select **Errors Only**, **Errors/Other** (default) for specific information only, **Verbose** for all errors and messages, or **Debug** for debugging related messages only.

- Database Reconnect (msecs) (default is 5000)
 Number of milliseconds to wait between reconnect attempts to the SQL database server. Recommended: 60000.
- Import Directory Scan (msecs) (default is 5000)
 Number of milliseconds to wait between each check of the import directory for new files. Recommended: 60000.
- Switch Tasks after (mins): (default is 1)
 Number of minutes to wait before switching to the next scheduled task.
- Click Save Configuration & Exit.

9 Restart the **HPCA Knowledge Base Server** to have the new configuration take effect. For details, refer to the topic below.

Starting and Stopping the KB Server

The KB Server is controlled as a Windows service. The friendly service name is **HPCA Knowledge Base Server** and the executable is **hpkbmanager.exe**. The service may be stopped and started through the Administrative Tools\Services options of the Control Panel.

SQL Server Requirements for the KB Server

To process Knowledge Base requests, the KB Server requires a SQL Server or Oracle logon ID. A user ID of any name can be configured (the default is **sa** for SQL Server or **usage** for Oracle). This ID is used to define the DB_OWNER for the Knowledge Base database with full permissions for administering the database. This ID is referred to as the AppLogin user ID.

Adding the USAGE Domain

Configuration Server Database users who did not enable the Application Usage Manager option while installing Configuration Server will need to import the USAGE Domain into their Configuration Server Database. To do this, import the latest class, instance, and resource files using the Client Automation tool ZEDMAMS.

The files for importing located in the $\Usage Manager\CSDB_Classes\USAGE_DOMAIN\ directory of the Client Automation Enterprise media and listed below:$

Usage domain class
Usage domain instances
Usage domain resources

To import the class, instance and resource files

1 Stop the Configuration Server Service.

- 2 Copy the above mentioned files to Root\Program Files\ Hewlett-Packard\CM\ConfigurationServer\bin folder
- 3 At the command prompt, navigate to the Root\Program Files\ Hewlett-Packard\CM\ConfigurationServer\bin folder and then execute the following commands:

```
Zedmams verb=import_class,file=usage780.xpc,
preview=no,replace=yes,continue=yes,duplicates=manage,
commit_changes=yes
```

```
Zedmams verb=import_instance,file=usage780.xpi,
xpr=usage780.xpr,preview=no,replace=yes,
continue=yes,duplicates=manage,commit_changes=yes
```

Additional instructions for using this tool can be found on the HP Software support website.

- 4 Copy all the .ico files in \CSDB_Classes\USAGE_DOMAIN\ directory on your Application Usage Manager media to the directory that contains the Admin CSDB Editor of the Administrator. (The executable is radxplor.exe).
- 5 Start the HPCA Configuration Server Service.
- 6 Open the Admin CSDB Editor from the HP Client Automation Administrator program group. Check that the USAGE Domain exists in the PRIMARY File.

3 Aggregation of Usage Data Files with Tier-Level Store and Forward

Introduction

The Aggregation of Application Usage Manager (Usage) data files with Tier-Level Store and Forward support is based on the methodology that the Usage data files will pass through a set of existing upstream servers within a centralized network (Store and Forward Messaging Servers), which reduces the need to install multiple Usage Databases and Knowledge Base Servers. The Store and Forward Messaging Servers will accept the incoming Usage data files and forward them to another upstream server. Upon receipt and prior to being forwarded, the Usage data files will undergo an Aggregation process.

Making use of tiered store and forward servers with aggregation tools drastically improves scalability and reduces large-scale issues that can arise when dealing with large numbers of Application Usage Manager agents across an enterprise. When using store and forward aggregation, a single KB Server can support much larger numbers of Application Usage Manager agents, as well as show improved performance when supporting the same number of agents.

What is Aggregation?

Aggregation is a process of merging two or more USDBase files into a single USDBase by eliminating all the duplicate data among the USDBase files.

When the Knowledge Base Server imports the Usage data, it must query the database for each import data record to check for its existence, and then updates the database accordingly. If there are N number of files with common data to import, the KB Server has to query the database N number of times. If the data in these common files can be aggregated into a single file, the KB Server only needs to query the database and update it once. Thus,

aggregating the data for common files prior to import improves the KB Server performance enormously.

An aggregated file contains only a single reference of a data for each file involved in aggregation. This will reduce the size of an aggregated file and reduces the overhead of multiple queries to the database when importing.

Implementation

The Messaging Server's Store and Forward capability is used to implement the Usage Data Files Store and Forward. The Messaging Server is responsible of storing all the USDBase files, trigger the aggregation process once the trigger constraint satisfied, and forward the aggregated file.

In the non-Store and Forward scenario, all the Usage Agents will be sending its usage data collection files to a predefined collection point that is monitored by Knowledge Base Server which in turn extracts the usage data from the files collected from each agent computer and loads this data into your SQL-enabled database, making the data available for reporting purposes.

With Store and Forward, all the Usage Agents will send its usage data collection files to a Messaging Server. We can have multiple such Messaging Servers in an enterprise to form a tier level architecture. The Tier Level architecture should be implemented according to the number of Usage Agents available in that Enterprise to get better performance.

In an n-tier level architecture, the level 0 is the tier with only the Usage Agents, level n is the final tier having the Portal installed with Knowledge Base Server configured for importing usage data files. All middle level tiers will have Messaging Server with Aggregation enabled and may have Usage Agents. Each middle level can have one or more Messaging Servers configured to forward the aggregated usage file (AU file) to the next level Messaging Server.

All the Usage Agents should be configured to send their usage data collection files to its immediate next level tier Messaging Server. This is the only change required in the Usage Agent needed to implement Store and Forward Aggregation.

Once the Messaging Server in a middle tier receives the USDBase files, depending on the configurations set it will trigger the Aggregation Process by executing the USDBAggr.exe which is the tool for performing Aggregation. After the Aggregation Tool is successfully executed, the Messaging Server will transfer the aggregated usage file to the next tier server. If the next tier is one of the middle level tiers, then the aggregation process continues till it reaches the final tier. If the next tier is the final tier, then the aggregated usage file gets imported into the database by the Knowledge Base Server (KB Server).

Figure 4 below illustrates a multi-tiered Messaging Server architecture being used to provide aggregated usage (AU) files for import into the usage database.

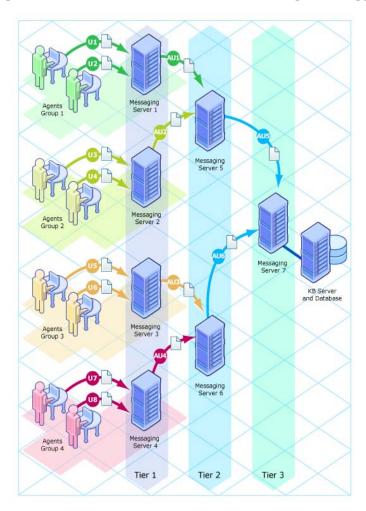


Figure 4 Tier-Level Architecture for Usage File Aggregation

Installing Messaging Server and Configuring Usage Data Files Store and Forward

System Requirements for Messaging Server

You must have administrator rights to the computer to install the Messaging Server.

Messaging Server v5.10 or above must be installed on a supported Windows platform.

Platform Support



Even though Messaging Server supports non-Windows platforms, the aggregation of usage files and the Usage Data Delivery Agent is only supported by a Messaging Server on a Windows platform.

For detailed information about the supported Windows platforms for Messaging Server, refer to the *Release Notes* document that accompanies this release.

Installing Messaging Server with Aggregation Support

Installation requirements, as well as instructions for installing the Messaging Server, are documented in the *Messaging Server Installation and Configuration Guide*.

To provide support for the aggregation of usage data, run, or rerun, the standard installation for Messaging Server v 5.10 or above. When prompted to **Select each Data Delivery Agent (DDA) to Install**, make sure to select the option:

Load the usage.dda module

Following installation, you must add and configure the aggregation-related code and parameters as discussed in Configuring Aggregation on page 54.

Configuring Aggregation

Before you can use the Aggregation support, you need to add and configure Aggregation Tools within the Messaging Server.

From the HPCA media's \Usage\Aggregation location, copy the entire
\Usage folder to your Messaging Server's \etc directory. By default, this
directory is:

[MessagingServerInstallPath]\etc

- 2 Configure the entries in the usage.dda.cfg file, using the topic below.
- 3 Following configuration, restart the service for the HPCA Messaging Server, rms.tkd.

You can have multiple tiers of Messaging Servers performing aggregation. The URL parameter in the **msg::register usage-forward** section of the usage.dda.cfg will determine whether the aggregated usage data is forwarded to the next-tier Messaging Server, or to a KB Server import location.

About the Sections in USAGE.DDA.CFG File

The usage.dda.cfg file within the Messaging Server's defines the configurations available for Aggregation. The file has the following main sections after the header and the required lines.

DO NOT REMOVE FOLLOWING LINE

package require nvd.httpd

msg::register usagehttpd

This is the HTTPD Section Type for the usage.dda configuration. If the Messaging Server is receiving USDBase files from one or more Usage Agents or another Messaging Server, define the URLHANDLER location on which to look for the files. This location is the source folder for the Aggregation Tool.

The parameters in the URLHANDLER are summarized below:

 ${\bf USE}$ defines the name of AGGREGATE Type that will receive the incoming file

DIR defines the directory for the HTTPD Type.

URL defines the prefix that that will be accepted by the Messaging Server. When messages are received with the designated URL they are deposited in the associated queue

HTTPMETH defines the method used by the agent to transfer the file. Set the HTTMETH type to PUT.

msg::register usage-aggregate-queue-in

This is the AGGREGATE Type section for the usage.dda configuration. This defines the Aggregation Queue in which the USDBase files will be queued up for processing by the aggregation tool.

DIR defines the source directory for the Aggregation Tool. This should be same as that of the HTTPD Type.

 $\ensuremath{\textbf{USE}}$ defines the name of the HTTP Type that will forward the aggregated file.

COUNT defines the minimum number of USDBase files expected in the DIR directory to initiate the Aggregation Process. (what are min, max, default?)

POLL defines the interval, in seconds, used to poll the source DIR directory for USDBase files.

TIMEOUT defines the maximum interval to wait, in minutes, for the number of USDBase files to reach the COUNT.

USER_DEFINED is a flag to allow a user-defined procedure to execute whose return value will control the triggering of the Aggregation. Set to Y if a user-defined procedure is to be used. When set to Y, the COUNT and TIMEOUT parameter are ignored, and the UD_TCL_FILE and UD_PROC parameters must be used to define the location and procedure name to execute.

UD_TCL_FILE defines the fully-qualified path to the TCL file containing the user-defined procedure, when USER_DEFINED is set to Y.

UD_PROC defines the user-defined procedure name to execute, when USER-DEFINED is set to Y.

USDBAGGRPATH defines the full path of the Aggregation Tool.

TARGET defines the fully-qualified path to the directory where the aggregated USDBase file will be placed.

ERRORPATH defines the fully-qualified path to the directory where the erroneous USDBase file will be moved from the DIR directory.

ARCHIVE Set to Y to archive the USDBase file after aggregation; set to N to delete the USDBase file after aggregation.

ARCHIVEPATH defines the fully-qualified path of the directory where the USDBase file is placed when ARCHIVE is set to Y.

MAXSIZE defines the maximum size, in bytes, for the generated aggregated file.



If the Input USDBase file size is larger than the MAXSIZE, the file will not be aggregated and will be sent without any modification.

LOGPATH defines the fully-qualified path of the directory where the log files are written by the aggregation tool.

msg::register usage-forward

This is the HTTP Type for the usage.dda configuration. This will define the forwarding server to which the aggregated file will be sent.

PRI denotes the priority in which to send the files to the companion URL. The default Priority is 10. This setting only matters if multiple ADDRESS entries are configured.

URL specifies the URL to use to send the aggregated file. This URL entry uses the same syntax as the COLLDEST for the Usage Agents, discussed on page 62.

— To send the aggregated file to a Portal that has the KB Server installed on it, code the URL as:

URL http://Portal_IP:3471/KB_Mgr1_Usage/

— To forward the aggregated file to the next tier Messaging Server enabled for the aggregation of usage data, code the URL as:

URL http://messaging_svr_IP:3461/proc/usage



If the target servers are SSL-secured, adjust the URL syntax to include https and the secure port number.

For more information on these section types, please refer to the *Messaging Server Guide*.

Performance

You must fine tune the configuration parameters in usage.dda.cfg to obtain the best aggregation performance. The main parameters that need tuning include:

MAXSIZE – This parameter directly impacts the compression ratio of an aggregated file, because MAXSIZE determines the number of files that can be placed in an aggregated file.

COUNT – This will affect the MAXSIZE. Make sure the number of files in COUNT is sufficient enough to reach the aggregated file size set in MAXSIZE.

 $\ensuremath{\textbf{POLL}}$ – This parameter determines how often the files are collected from the source folder.

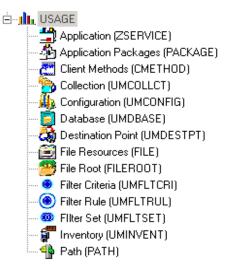
4 Application Usage Manager Agent

The USAGE Domain Defined

The Application Usage Manager utilizes the USAGE Domain within your Configuration Server Database, enabling management of the Application Usage Manager in the enterprise. The USAGE Domain is comprised of classes that you use to create Application Usage Manager services to distribute to your agent computers. These services install the Application Usage Manager agent, which collects usage data based on your specifications. The next few sections describe the USAGE Domain classes.

Use the HP Client Automation Administrator CSDB Editor to configure each class in the USAGE Domain.

Figure 5 USAGE Domain in the Admin CSDB Editor



Class	Description
Application (ZSERVICE)	Contains the Application Usage Manager services
Application Packages (PACKAGE)	Contains the Application Usage Manager packages
Client Methods (CMETHOD)	Client methods used to process each instance
Collection (UMCOLLCT)	Controls the Application Usage Manager collection options that represent the unique collection criteria with which the usage collection files on each computer are associated. A single computer may have multiple collections targeted, each associated with a unique data store. The collection file contents are sent to different collection points and ultimately to different SQL databases.
Configuration (UMCONFIG)	Controls the Application Usage Manager installation options.
Database (UMDBASE)	Unique usage database name, which correlates to a backend SQL database.
Destination Point (UMDESTPT)	Location where usage data is stored.
File Resources (FILE)	File instances included within a package.
File Root (FILEROOT)	Defines the base location of a file without any extended path information. Can be a drive, like C: or a well known folder location, like ProgramFiles folder. File Roots are only used for filtering the collection file content collected from the agent in the Admin
Filter Criteria (UMFLTCRI)	CSDB Editor.

Table 2USAGE Domain classes

Class	Description
Filter Rule (UMFLTRUL)	Connects to usage filtering criteria. The filter type determines whether it is an inclusion or exclusion Filter Rule, and its priority determines its importance when compared with other Filter Rules defined in a Filter Set. Refer to Filters on page 68 for more information.
Filter Set (UMFLTSET)	Connects to one or more Filter Rules. Filter Sets are in turn connected to collections in the UMCOLLCT Class. Each UMCOLLCT Class may then have specific filtering associated with its data collection.
Inventory (UMINVENT)	Defines default configuration criteria for the Application Usage Manager inventory scan.
Path (PATH)	A unique path to one or more components.

Significance of Collection Instances

Collection class instances, and their related filter class instances, establish the content that is uploaded to a specific SQL database from the device which the usage data is collected. Collection class instances define the databasespecific agent collection properties; they also define the destination location once the usage and inventory data has been aggregated on the agent machine and is ready to be passed through the network for import into a specific SQL database.

Configuring the Application Usage Manager Agent

The Application Usage Manager agent is installed as a service to the existing Client Automation Agents in your environment.

The Application (ZSERVICE) class in the USAGE Domain contains a service out of the box that requires minimal configuration. This is named **Application Usage Mgr Agent Install – Enterprise Collection**. Connect this service to the appropriate agent machines and then during the next agent connect the Application Usage Manager agent is distributed. Use this service to define inventory and collection parameters and for distribution to your agent computers.

Go to View \rightarrow Options. Open the Instance Options tab and select **Both** and click **OK**.

Reopen the Admin CSDB Editor.

To configure the Application Usage Manager agent for distribution

- 1 Start the Admin CSDB Editor and double-click **PRIMARY**, then **USAGE**.
- 2 Double-click to expand the **Application (ZSERVICE)** class.

This class contains several services you can use to distribute the Application Usage Manager agent as well as apply any collection filters. The service **Application Usage Mgr Agent Install – Enterprise Collection** distributes the Application Usage Manager agent to your environment and contains a default collection instance.

The service contains four configurable connections:

Application Usage Manager Agent	Application (PACKAGE) instance
Configuration – Entire Enterprise	Configuration (UMCONFIG) instance
Inventory – Sundays at Midnight	Inventory (UMINVENT) instance
Collection – Entire Enterprise	Collection (UMCOLLCT) instance

- 3 Double-click **Configuration Entire Enterprise**. The Editing Instance dialog box opens.
- 4 Click **SERIAL** to edit the instance. Enter your Usage Manager serial number.

J X Pa A X Co I I A A THE AND AND A	Configuration class Cont	figuration-Entire Enterprise Instance Attributes:	
Database	Name	Attribute Description	Value
🛉 💾 LICENSE	NAME	Friendly Name	Configuration-Entire Enterprise
PRIMARY	ENABLED	Enable Usage Monitoring [Y/N]	Y
🖶 🤠 ADMIN	ENAFOCUS	Enable Application Focus Time [Y/N]	Y
	ENA16BIT	Enable 16 Bit Module Support [Y/N]	Y
🗉 🧟 AUDIT	W HISTMNTH	Save Client History for nn Months	12
	LOGCOUNT	Number of Daily Logs to Maintain	7
H PATCH	W INSTLDIR	Installation Directory	[ProgramFilesFolder]Hewlett-Packard\HPCA\AUM Agent
B POLICY	V LOCLPATH	Local Path for Usage Monitor Files	[ProgramFilesFolder]Hewlett-Packard\HPCA\AUM Agent\Usage Man
	SERIAL	Usage Monitor Serial Number	RA-00-0000-0000000-0000-0000-xxxxxxx
	V OBFSUSER	Obfuscate User Name [Y/N]	N
B SYSTEM	OBESCOMP	Obfuscate Computer Name [Y/N]	N
	OBFSDOMN	Obfuscate Domain Name [Y/N]	N
Application (ZSERVICE)	OBFSUSAG	Obfuscate Usage Times [Y/N]	N
BASE_INSTANCE_ Application Usage Mor Agent - CCM Application Usage Mor Agent Install - Enterprise C Application Usage Morage Agent Agent Application Usage Morage Agent Collection Collection Usage Morage Agent Collection Collec		Configuration Clent Method	

- 5 Click **OK** to close the window.
- 6 Double-click Collection Entire Enterprise.

7 Double-click HTTP - CMIS_IP_ADDR:Port\URL.

	ME>>:3466/KB_Mgr1_Usage/		
Name	Attribute Description	Value	
V NAME	Friendly Name	HTTP - CMIS_IP_ADDR:Port\URL	
COLLDEST	Collection Destination Point Ta	http://< <hostname>>:3466/KB_Mgr1_Usage/</hostname>	

- 8 Select **COLLDEST** and enter the url and port of the HPCA Server being used to collect the USDBase files from the HPCA Agents in your environment.
 - If you are using Messaging Servers enabled for usage aggregation to collect usage files from the HPCA Agents, specify COLLDEST using the hostname and the listening (store and forward) port of your Messaging Server:

http://1.1.1.10:3461/proc/usage

or

https://1.1.1.10:3461/proc/usage

 If you are using a Portal to collect usage files from the CM Agents, follow the examples below.

http://1.1.1.10:3471/KB_Mgr1_Usage/

If your Portal has been SSL-secured, specify the **COLLDEST** url using **https**, such as: **https://1.1.10:443/KB_Mgr1_Usage/.**

The Knowledge Base Server monitors this collection point and moves any files it finds into your SQL database for viewing. After the files are moved out of the collection point, they are saved in a subdirectory called Archive.

The default collection parameters are described in Table 3 below.

Instance	Default Value	Description
NAME	Primary Collection Parameters	Friendly Name.
INTERVAL	Weekly	When the collection will take place. [Monthly/Weekly/Daily/None]
DAYOFMON	1	Day of the month collection will take place. [01-31]
DAYOFWK	1	Day of the week collection will take place [1=Sun] [1-7]
COLLHOUR	00	The hour of the collection. Midnight is hour 00. [00-23]
COLLMIN	00	The minute of the collection. [00-59]

 Table 3
 Default Collection Parameters (UMCOLLCT)

Instance	Default Value	Description
COLLRAND	0	Randomized Collection. Maximum delay minutes to use to randomize the collection start time. If non-zero, randomizes the collection process to occur anytime from the start time through a randomly generated number of minutes later. [0-720]
ENABLED	Y	Whether or not collection is enabled.
COLLCNCT		Collect on CM Agent Connect? [Y/N]
		<i>Note:</i> CM Agent Connect now refers to an HPCA Agent connect.
DBASCONN	USAGE.UMDBASE.PRIMARY	Usage database connection.
DESTCONN		This is a connection to a predefined collection point. This is the location where files will be stored until the Knowledge Base Server moves them into your SQL database.
CMETHOD	CMETHOD.UMCOLLCT	The collection method.
FLTSET01	USAGE.UMFLTSET.USAGE_I NCLUDE_ALL_FILES	Filter Set connection.
FLTSET02 through FLTSET10		Filter Set connections.

- 9 Click **OK** to close the dialog box.
- 10 Connect any Filter Sets you would like to include with your service by dragging the Filter Set instance onto the service name. For more information on creating and applying filters, see Filters on page 68.

📓 🔏 🖬 🖬 🖬 🖬 🖬 🖬 📓			
Database Tree View:	Inventory class Inv	entory - Sundays at Midnight Instance Attrib	utes:
	Name	Attribute Description	Value
Application (ZSERVICE)	NAME	Friendly Name	Inventory - Sundays at Midnight
BASE_INSTANCE_	INTERVAL	[Monthly/Weekly/Daily/Collect/None]	Weekly
Application Usage Mgr Agent - CCM	DAYOFMON	Inventory Day of Month [01-31]	1
Application Usage Mgr Agent Install - Enterprise	DAYOFWK	Inventory Day of Week (1=Sun) [1-7]	1
Application Usage Manager Agent Application Usage Manager Agent: <all <a="" <all="" agent:="" application="" manager="" usage="">Application Usage Manager Agent: <a>Application U</all>	INVNHOUR	Inventory Hour of Day [00-23]	00
	INVNMIN	Inventory Minute of Day [00-59]	00
	V ENABLED	Inventory Enabled [Y/N]	Y
Configuration-Entire Enterprise	FSIGMODE	Inventory - File Scan Mode [S/H/M]	S
Inventory - Sundays at Midnight Collection - Entire Enterprise			
Collection - Entire Enterprise			
HTTP - CMIS_IP_ADDR:Port\URL			
All Apps - Except Base OS Apps			
Application Usage Mgr Agent Install Only - No Co			
Application Packages (PACKAGE)			
	1		- I

11 If you want to adjust the inventory time, double-click **Inventory – Sundays at Midnight**. Table 4 below describes each inventory parameter.

 Table 4
 Default Inventory Parameters (UMINVENT)

Attribute	Default Value	Description
NAME	Default Inventory Parameters	Friendly Name
INTERVAL	Weekly	When each inventory will take place. [Monthly/ Weekly/ Daily/Collect/None]
DAYOFMON	1	The day of the month to begin the inventory. [0-31]
DAYOFWK	1	Day of the week each inventory will take place. [1-7] (1=Sunday).
INVNHOUR	00	The hour of the day at which the inventory will take place. [00-23]
INVNMIN	00	The minute at which the inventory will take place. [00-59]
ENABLED	Y	Whether or not inventory is enabled.

Attribute	Default Value	Description
FSIGMODE	S	Three levels of scanning depth for executables inventoried on each agent device are available. The type of scan defined here can determine the amount of time a collection may take.
		S File Sizes Only. Faster, less comprehensive (default)
		H Entire Module Header. Slower, more comprehensive
		M Complete MD5 Signature. Slowest, most comprehensive
CMETHOD	CMETHOD.UMINVENT	The inventory method.

These parameters can be adjusted to adhere to your specific needs. The default inventory will begin on the first of the month and repeat once a week every Sunday at midnight.

- 12 Connect the **Application Usage Mgr Agent Install Enterprise Collection** service to the appropriate users or workgroups using the Admin CSDB Editor. For example, to connect this service to the default Administrator User, follow the steps below:
 - a Login to the Database Editor.
 - b Expand the PRIMARY file, USAGE domain and Application (ZSERVICE) class.
 - c Select Application Usage Mgr Agent Install Enterprise collection and drag-and-drop it on the default user instance under PRIMARY\POLICY\Users\Administrator.

The Application Usage Manager Agent Installation using an HPCA environment

To install the Agent for Application Manager or Application Self-Service Manager

Installation requirements, as well as instructions for installing the Client Automation agent, are documented in the *HP Client Automation Application Manager and Application Self-service Manager Installation and* Configuration Guide (Application Manager and Application Manager Selfservice Manager Guide).

To install the Application Usage Manager Agent

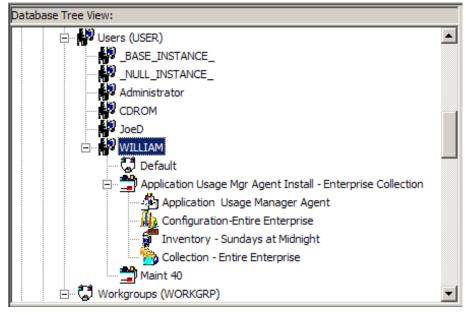
- 1 Open Application Self-Service Manager, in the list of software displayed.
- 2 Select HPCA Application Usage Manager Agent and right-click.

• • • • • • •			
Name	Status		
Amortize	Available		
HPCA Application Usage M	lanager Agent - 7.50	Size Compressed Size	3.06 MB 1.91 MB
Redbox Organizer Sales Information	Available Available		
cessfully		Connected	

3 Select **Install** from the shortcut menu to install the Application Usage Manager Agent.

After it is installed, you can also use the Application Selfservice Manager to **Update**, **Verify** and **Remove** the Application Usage Manager Agent. Refer to the *Application Manager and Application Self-service Manager Guide* for more information.

For implementation details regarding non-Client Automation environments refer to Appendix A, Implementing Application Usage Manager in a Non-HPCA Environment.



During the next agent connect to the Configuration Server, the service will be installed, and based on your settings, collection will begin.

Filters

By default, the Application Usage Manager collects usage information for every executable installed on the agent computer. To collect only specific executable information, filters can be defined and attached to the collection instance. Because all executable information is collected by default, the **Exclude All** filter rule must be included with any filters you use.

The USAGE Domain contains classes associated with creating filters for your usage data. This enables you to collect specific information based on parameters you define. The filter related classes are:

- Filter Criteria
- Filter Rule
- Filter Set

Each of these classes contains configurable instances you can use to define your filter.

Criteria, Rule, and Set

To help you define filter parameters, the Application Usage Manager uses filter criteria, rules, and sets.

Criteria

Criteria are specific attributes that an application may contain, such as "member of the Microsoft family of applications."

• Rule

When multiple criteria are combined, they form a rule. A rule is a simple way of grouping criteria, making it easier to apply the same set of criteria to multiple services.

• Set

When multiple rules are grouped into one instance, a set is created. A set is the highest level of criteria collection containing multiple rules, which in turn may contain multiple criteria.

Filter Criteria Class (UMFLTCRI)

🖉 File Edit View Window Help				_ 8 :	
2 <u>X DEX D</u> II <u> </u>	2				
atabase Tree View:	Filter Criteria (U	Filter Criteria (UMFLTCRI) Class Instances:			
🗄 📊 USAGE	▲ Name		Instance Name	Туре	
	CCM_1147	292934	CCM_1147292934	USAGE.UMFLTCRI In	
- 🏰 Application Packages (PACKAGE)	CCM_1147	293430	CCM_1147293430	USAGE.UMFLTCRI In	
🍅 Collection (UMCOLLCT)	CCM_1147	293431	CCM_1147293431	USAGE.UMFLTCRI In	
- 🏨 Configuration (UMCONFIG)	■ ③ CCM_1147	293447	CCM_1147293447	USAGE.UMFLTCRI In	
📴 Database (UMDBASE)	● CCM 1147	293487	CCM 1147293487	USAGE.UMFLTCRI In	
Destination Point (UMDESTPT)	Compag Co	rporation	COMPAQ CORPORATION	USAGE.UMFLTCRI In	
File Resources (FILE)	Creative Su	rround Mixer	MS_CREATIVE_SURROUND_MIXER	USAGE.UMFLTCRI In	
File Root (FILEROOT)	🛞 Default Filte	r Criteria Params	_BASE_INSTANCE_	USAGE.UMFLTCRI In	
🖻 🐵 Filter Criteria (UMFLTCRI)	InstallShield	Corporation	INSTALLSHIELD	USAGE.UMFLTCRI In	
	Internet Exc	blorer	CCM 1148989588	USAGE.UMFLTCRI In	
Compaq Corporation Screative Surround Mixer	McAfee Viri	usScan	MCAFEE VIRUS SCAN	USAGE.UMELTCBLIn	
Creative Surround Mixer Default Filter Criteria Params	Microsoft .N	IET Framework	MICROSOFT DOTNET FRAMEWORK	USAGE.UMFLTCBI In	
 Default Filter Criteria Params InstallShield Corporation 	Microsoft A	CCBSS	CCM 1147293463	LISAGE LIMELTOBLIN	
 Instalishield Corporation Internet Explorer 	Microsoft A	udioHQ	MICROSOFT AUDIOHQ	LISAGE LIMELTCBLIN	
McAfee VirusScan	Microsoft C	uster Server	MICROSOFT CLUSTER SERVER	USAGE UMELTCBUIN	
Microsoft NET Framework		onnection Manager	MICROSOFT_CONNECTION_MGR	USAGE.UMFLTCRI In	
Microsoft Access		ata Access Components	MDAC	USAGE.UMFLTCRI In	
Microsoft AudioHQ	 Microsoft D 		MICROSOFT DIRECTX	USAGE.UMFLTCRI In	
Microsoft Cluster Server	 Microsoft D 		MICROSOFT DTC	USAGE.UMFLTCRI In	
Microsoft Connection Manager	Microsoft E		MICROSOFT EXCHANGE	USAGE.UMFLTCRI In	
Microsoft Data Access Components	 Microsoft E Microsoft Fi 	2	MICROSOFT FRONTPAGE	USAGE.UMFLTCRI In	
- \varTheta Microsoft DirectX	 Microsoft II Microsoft II 		MICROSOFT IIS	USAGE.UMFLTCRI In	
🐵 Microsoft DTC		, etMeeting - Var 1	MICROSOFT_IIS	USAGE.UMFLTCRI In	
😔 Microsoft Exchange		etMeeting - Var 2	MICROSOFT_NETMEETING_VAR_2	USAGE.UMFLTCRI In	
😣 Microsoft FrontPage	 Microsoft N Microsoft N 		MICROSOFT_NETSHOW	USAGE.UMFLTCRI In	
🐵 Microsoft IIS	Microsoft N		ODBC	USAGE.UMFLTCRI In	
🐵 Microsoft NetMeeting - Var 1	Microsoft U		MICROSOFT OFFICE 2000	USAGE.UMFLTCRI In	
😌 Microsoft NetMeeting - Var 2		IIICE 2000	MICHOSOFI_OFFICE_2000	USAGE.OMFLICKIIN	
7 Filter Criteria instance(s) displayed			UTF-8 8/14/200	6 4:24 PM	

Figure 6 Filter Criteria Class (UMFLTCRI) pre-defined instances

The Filter Criteria Class contains various instances that reflect vendorspecific applications. Use these to attach a filter criterion using one of the included applications. The instances include filter criteria for Compaq, McAfee, Microsoft, and InstallShield, as well as many others.

Filter Rule Class (UMFLTRUL)

File Edit View Window Help		न्त		<u>_6 ×</u>
A DE CARA DE LE ELEMENT		Filter Rule (UMFLTRUL) Class Instances:		
🗄 📊 USAGE		Name	Instance Name	Туре
Application (ZSERVICE)		CCM Filter Rules	CCM_FILTERRULE	USAGE.UMFLTRUL I
- 🍰 Application Packages (PACKAGE)		Default Filter Rule Parameters	_BASE_INSTANCE_	USAGE.UMFLTRULI
- Collection (UMCOLLCT)		Excl - Microsoft OS Files - 1	EXCL_MICROSOFT_OS_FILES_1	USAGE.UMFLTRULI
— 🦺 Configuration (UMCONFIG)		Excl Windows OS Add-on Prods - 1	EXCL_WINDOWS_OS_ADD_ON_PR	USAGE.UMFLTRUL I
🧾 Database (UMDBASE)		Excl Windows OS Add-on Prods - 2	EXCL WINDOWS OS ADD ON PR	USAGE.UMFLTRUL I
🔤 🖓 Destination Point (UMDESTPT)		Exclude All	EXCLALL	USAGE.UMFLTRUL I
File Resources (FILE)		Exclude Microsoft System Folder	EXCL MICROSOFT SYSTEMFOLDER	USAGE.UMFLTRUL I
File Root (FILEROOT)		Exclude Microsoft WindowsFolder	EXCL MICROSOFT WINDOWSFOLD	USAGE.UMFLTRUL I
Filter Criteria (UMFLTCRI)		Include All	INCLALL	USAGE.UMFLTRULI
Filter Rule (UMFLTRUL)		Include MS Licensed Apps - 1	MICROSOFT_LICENSED_APPS_1	USAGE.UMFLTRUL I
(@) CCM Filter Rules (@) Default Filter Rule Parameters		Include MS Office Products	MICROSOFT_OFFICE_PRODUCTS	USAGE.UMFLTRULI
Orault Filter Fulle Parameters Sector Microsoft OS Files - 1		Include MS Server Products	INCLUDE MS SERVER PRODUCTS	USAGE.UMFLTRULI
Excl Windows OS Add-on Prods - 1		Include Novadigm Apps		USAGE.UMFLTRULI
Excl Windows 05 Add-on Prods - 2		Include Other Vendor Apps - 1	OTHER VENDOR APPLICATIONS 1	USAGE.UMFLTRUL
Exclude All				
Exclude Microsoft System Folder				
Exclude Microsoft WindowsFolder				
Include All				
Include MS Licensed Apps - 1				
Include MS Office Products				
Include MS Server Products				
- include Novadigm Apps				-
a Instude Other Vender Appen 1	-		UTF-8 8/14/2006	

Figure 7 Filter Rule Class (UMFLTRUL) pre-defined instances

The Filter Rule Class contains pre-configured rules using common vendorspecific parameters. For example, Include MS Office Products will include all Microsoft Office applications, and Exclude Microsoft Windows will exclude all Microsoft Windows files.

This Filter Rule Class connects to the usage filtering criteria. The filter type determines whether it is an inclusion or exclusion Filter Rule and its priority determines its importance when compared with other Filter Rules in a Filter Set (Zero is the lowest priority). In the event priorities are equal within a Filter Set, inclusion filters take precedence over exclusion filters.

If no criteria are specified for an inclusion filter, than all usage information is captured in the collection file. If no criteria are specified for an exclusion filter, then all usage is excluded.

Filter Set Class (UMFLTSET)

🔯 File Edit View Window Help			
			_ 8 ×
🕺 <u>X BEX 🔁 II 9555</u>	2		
Database Tree View:	Filter Set (UMFLTSET) Class Instances:		
😴 Database	Name	Instance Name	Туре
🚰 LICENSE	🚳 All Apps - Except Base OS Apps	ALL_APPS_EXCL_BASE_OS_AP	USAGE.UMFLTS
🖻 💾 PRIMARY	🚳 CCM Filter Set	CCM_FILTERSET	USAGE.UMFLTS
🗄 🔄 ADMIN	🐵 Concurrency - Novadigm Apps	CONCURR_INCL_NOVADIGM_A	USAGE.UMFLTS
🗄 🔜 AUDIT	🐵 Default Filter Set Parameters	_BASE_INSTANCE_	USAGE.UMFLTS
🕀 📰 CLIENT	🐵 Inventory Only - Incl. All Files	INVENTORY_INCLUDE_ALL_FIL	USAGE.UMFLTS
🗈 🥨 NOVADIGM	Microsoft Licensed Applications	MICROSOFT_LICENSED_APPLI	USAGE.UMFLTS
ia Patch	💷 Usage - Include All Files	USAGE_INCLUDE_ALL_FILES	USAGE.UMFLTS
in the second s			
🖶 🔞 SOFTWARE			
Application (ZSERVICE)			
Collection (UMCOLLCT)			
Configuration (UMCONFIG)			
Database (UMDBASE)			
🔏 Destination Point (UMDESTPT)			
File Resources (FILE)			
File Root (FILEROOT)			
Filter Criteria (UMFLTCRI)			
Filter Rule (UMFLTRUL)			
Filter Set (UMFLTSET)			
🚥 🚳 All Apps - Except Base OS Apps			
🚳 CCM Filter Set			
🕺 Concurrency - Novadigm Apps Only			
🚳 Default Filter Set Parameters			
🚳 Inventory Only - Incl. All Files			
🚥 Microsoft Licensed Applications			
🔤 🚥 Usage - Include All Files			
- 🐖 Inventory (UMINVENT)			
Path (PATH)	•		Þ
7 Filter Set instance(s) displayed		UTF-8 8/14/2006 4	:25 PM

Figure 8 Filter Set Class (UMFLTSET) pre-defined instances

A Filter Set is comprised of one, or a collection of, Filter Rules. The Filter Set class contains pre-configured Filter Sets you can use to collect or exclude vendor-specific information.

Once a Filter Set has been created, or you decide which existing Filter Set to use, connect it to a Collection class (UMCOLLCT) instance to enable the filter. Only Filter Sets may be connected to a collection class. All criteria associated with that Filter Set are then processed. By connecting the Filter Set to a Collection class instance, each data collection can then contain specific filtering.

Attribute	Default Value	Description
NAME	Default Filter Set Parameters	Filter Set Friendly Name
INCLUSAG	Yes	Determines whether or not to include usage data as well as inventory data in the collection.
CONCURR	No	Defines whether to collect concurrent usage data. See Using Concurrency on page 80 for more information.
CMETHOD	CMETHOD.UMFLTSET	Client method used to process Filter Set class instances
FLTRUL##		Filter Rules connections

Table 5Default filter set parameters

Using Filters

Filters can be applied to Collection class instances. Use the existing Filter Set instances, or create your own using the filter classes provided. The following exercises explain how to apply a filter as well as how to create a new filter based on parameters you define.

Filter Set Class Instances

The Filter Set Class (UMFLTSET) contains a few default Filter Sets that can be used for generic data collections. Each class instance collects a specific type or set of data. Table 6 below describes each class instance in detail.

Table 6Filter set class (UMFLTSET) instances

Instance Name	Description	
All Apps – Except Base OS Apps	Collects data for all installed applications with the exception of base operating system applications.	

Instance Name	Description
CCM Filter Set	Collects data for the Microsoft and Internet Explorer applications defined in the Filter Criteria connections.
Concurrency – Novadigm Apps Only	Collects concurrency data. This default setting collects data for all HPCA applications. HPCA applications were formerly known as Novadigm and Radia applications, as well as HP OpenView CM applications.
Default Filter Set Parameters	Contains the default Filter Set instance values and is used to create custom Filter Sets.
Inventory Only – Incl All Files	Collects inventory data for installed applications - no usage data is collected.
Microsoft Licensed Applications	Collects data for Microsoft applications as defined in each Filter Criteria connection.
Usage – Include All Files	Collects all usage data.

Applying Filters

Filters can be applied to Collection class instances by simply dragging the Filter Set instance onto the appropriate Collection class instance.

To apply a filter to a Collection Class

- 1 Start the Admin CSDB Editor and navigate to the PRIMARY File, USAGE Domain.
- 2 Connect the appropriate Filter Set to the connection class you would like to apply the filter to.
- 3 Click **Copy** and accept the changes.

Creating Filters

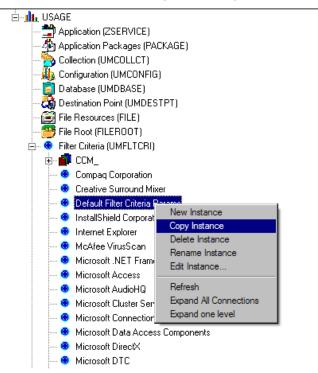
Creating a Filter is comprised of three basic steps:

- 1 Create or select a Filter Criteria instance.
- 2 Create or select a Filter Rule instance and attach the Filter Criteria instance.
- 3 Create or select a Filter Set instance and attach the Filter Rule instance.

The following example demonstrates how to create a filter that will collect usage information for Adobe Acrobat.

To create a Filter Criteria instance

- 1 Start the Admin CSDB Editor and navigate to the PRIMARY File, USAGE Domain.
- 2 Double-click Filter Criteria (UMFLTCRI).



3 To create a new instance right-click **Default Filter Criteria Params**, and from the shortcut menu select **Copy Instance**. The Copy Instance dialog box opens.

- 4 Rename the new instance Adobe Acrobat, and then click **OK**.
- 5 In the tree view of the Admin CSDB Editor, double-click the newly created instance.

The Editing Instance dialog box opens.

i, Editing Adobe Act - Company Name	robat Instance - Last Update	:: - 04/02/03 11:42:08	<u>?</u>]
Name	Attribute Description	Value	
	Friendly Name	Adobe Acrobat	
	File Root Connection		
V FILEPATH	File Path		
V FILENAME	File Name		
V COMPNAME	Company Name		
V PRODNAME	Product Name		
V PRODVER	Product Version		
V FILEDESC	File Description		•
•			
			OK Cancel Restore

6 Use the attributes defined in the following table to define your filter criteria.

	Table 7	Filter	criteria	attributes
--	---------	--------	----------	------------

Attribute	Description
NAME	Friendly Name
ROOTCONN	Compares for applications that reside in any of the predefined shell folder names, such as ProgramFilesFolder, WindowsFolder, or SystemsFolder. These can be used to filter based on a well-known folder, such as TempFolder.
DESCRIPT	Description of filter criteria.
ENABLED	Whether or not this filter is enabled. [Y/N] Default is Y.
FILEROOT	Defines the file root path, or the base location of a file without any extended path information. Can be a drive, like C: or a well known folder location, like ProgramFiles folder.

Attribute	Description
FILEPATH	Defines the suffix of the path name that is appended to the file root path. For example, this would contain the characters \Microsoft Office regardless if the installation for the Microsoft Office application was to the ProgramFilesFolder\Microsoft Office path or to the TempFilesFolder\Microsoft Office path.
FILENAME	The application file name executable, for example winword.exe.
COMPNAME	The vendor name defined in the executable's header.
PRODNAME	The product name defined in the executable's header.
PRODVER	The product version defined in the executable's header.
FILEDESC	The file description defined in the executable's header.
FILEVER	The internal file version defined in the executable's header.
ORIGNAME	The original file name defined in the executable's header. This string does not change if the file is renamed.
MD5HASH	The MD5 hash file signature that uniquely identifies the contents of the file. Any change to a file results in it being assigned a unique MD5 hash signature.
CMETHOD	The client method used to process Filter Criteria instances.

- 7 In the Editing Instance dialog box (see the figure on page 76) double-click the **COMPNAME** attribute and in the text box provided and type **Adobe**.
- 8 Click the **PRODNAME** attribute and type Acrobat.
- 9 Click **OK** and save the changes.

You have successfully created a new Filter Criteria instance.

To create the Filter Rule instance

- 1 In the tree view of the Admin CSDB Editor, double-click Filter Rule (UMFLTRUL).
- 2 Right-click **Default Filter Rule Parameters.**
- 3 In the shortcut menu, select **Copy Instance**. The Copy Instance dialog box opens.
- 4 Rename the new Filter Rule instance Adobe Apps, and click **OK**.
- 5 In the Admin CSDB Editor window, connect the Filter Criteria instance you created, Adobe Acrobat, to the newly created Adobe Apps Filter Rule instance.

atabase Tree View:		Filter Rule class Adobe	Apps Instance Attributes:	
Remedy Corporation		Name	Attribute Description	Value
🐵 RoboHELP		W NAME	Friendly Name	Adobe Apps
🐵 Sun Microsystems		V TYPE	Filter Type [Include/Exclude]	Include
🐵 Trend Micro Inc		V PRIORITY	Filter Bule Priority	0
📀 Windows 2000 OS		A CMETHOD	Filter Rule Client Method	CMETHOD.UMFLTRUL
- 😌 Windows Disk Defragmenter		TA FLTCRI01	Filter Criteria Connection	USAGE.UMFLTCRI.AD0BE_ACR0BA1
😌 Windows Installer		A FLTCRI02	Filter Criteria Connection	_
😁 Windows NT OS		DA FLTCRI03	Filter Criteria Connection	
🐵 Windows DS - Variation 1		A FLTCRI04	Filter Criteria Connection	
😌 Windows DS - Variation 2		DA FLTCRI05	Filter Criteria Connection	
Windows DS - Variation 3		A FLTCRI06	Filter Criteria Connection	
Windows DS - Variation 4		A FLTCRI07	Filter Criteria Connection	
🔮 Windows Script Host		A FLTCRIOS	Filter Criteria Connection	
- \varTheta WinZip		A FLTCRI09	Filter Criteria Connection	
Filter Rule (UMFLTRUL)			Filter Criteria Connection	
🖨 🛞 Adobe Apps		A FLTCRI10	Filter Unteria Connection	
- Elter Rule Method				
Adobe Acrobat				
- 🛞 Default Filter Rule Parameters				
🕘 Excl - Microsoft OS Files - 1				
- 🥘 Excl Windows OS Add-on Prods - 1				
Excl Windows DS Add-on Prods - 2				
Exclude All				
Exclude Microsoft System Folder				
() Exclude Microsoft WindowsFolder				
🛞 Include All				
Include MS Office Products				
Include MS Server Products				
Include Other Vendor Apps - 1				
Include Radia Apps				
Filter Set (UMFLTSET)				
Inventory (UMINVENT)				
Inventory (UMINVENT) A Path (PATH)	-1			

- 6 Click **Copy** and accept the changes by clicking **Yes**, and then **OK**. The Filter Criteria instance is now connected to a Filter Rule instance.
- 7 In the list view of the Admin CSDB Editor (right pane), double-click the PRIORITY instance attribute and set the value to **1** to ensure this rule will be applied before any default rules may be used. (Zero is the lowest possible priority as well as the default value.)

1			
Name	Attribute Description	Value	
V NAME	Friendly Name	Adobe Apps	
🕖 TYPE	Filter Type [Include/Exclude]	Include	
🕖 PRIORITY	Filter Rule Priority	1	
A СМЕТНОD	Filter Rule Client Method	CMETHOD.UMFLTRUL	
A FLTCRI01	Filter Criteria Connection		
A FLTCRI02	Filter Criteria Connection		
A FLTCRI03	Filter Criteria Connection		
A FLTCRI04	Filter Criteria Connection		

The Filter Rule instance is now complete.

To create the Filter Set instance

- 1 In the Admin CSDB Editor window, double-click **Filter Set (UMFLTSET)**.
- 2 Right-click Default Filter Set Parameters.
- 3 In the shortcut menu select, **Copy Instance**. The Copy Instance dialog box opens.
- 4 Rename the new Filter Set instance Adobe Licensed Applications.
- 5 Connect the Filter Rule instance you created earlier, Adobe Apps to the newly created Adobe Licensed Applications Filter Set instance.
- 6 Also connect the existing Filter Rule instance, Exclude All, to the newly created Filter Set instance. This ensures that only usage data for the specific executable defined in your criteria, Adobe Acrobat, will be collected.

By default the priority setting for this instance is 0, the lowest possible. By setting the priority for the Adobe Apps rule to 1 earlier, you have given priority to that Filter Rule instance, ensuring it will be applied before any default rules.

C 1:cs001 - 1	Filter Set class Adobe L	icensed Applications Instance Attributes:		
Windows 05 - Variation 2	Nome	Attribute Description	Volue	
Windows DS - Valation 3	NAME	Friendly Name	Adobe Licensed Applications	
Windows DS - Valation 4	INCLUSAG	Include Usage Data (Yes/No)	Yes	
Windows Scrint Host	CONCURR	Collect Concurrency Data [Yes/No]	No	
 WinZip 	CONCORN	Filter Set Client Method		
R-() Filter Rule (UMFLTRUL)	ELTRULO1	Filter Bule Connection	CMETHOD.UMFLTSET	
R Adobe Acos		I MARTING CONTROLING	USAGE.UMFLTRULADOBE_APPS	
Default Filter Rule Parameters	INTLTNUL02	Filter Rule Connection	USAGE.UMPLTDUL.EXCLALL	
Excl - Microsoft 03 Files - 1	A FLTRUL03	Filter Rule Connection		
Excl Windows OS Add-on Prods - 1	AFLTRUL04	Filter Rule Connection		
Excl Windows OS Add-on Prods - 2	A LTUTOLOS	Filter Rule Connection		
Exclude All	A FLTRULOS	Filter Rule Connection		
— Exclude Microsoft System Folder	A FLTRUL07	Filter Rule Connection		
— Exclude Microsoft WindowsFolder	A PLTNUL00	Filter Flule Connection		
- (Include All	AFLTRUL09	Filter Rule Connection		
— O Include MS Licensed Apps - 1	A FLTRUL10	Filter Rule Connection		
Include MS Office Products	DA FLTHUL11	Filter Dule Connection		
— Include MS Server Products	AFLTRUL12	Filter Rule Connection		
— Include Other Vendor Apps - 1	A FLTRUL13	Filter Rule Connection		
Include Radia Apps	CARLTNUL14	Filter Dule Connection		
Filter Set (UMFLTSET)	AFLTRUL15	Filter Rule Connection		
Adobe Licensed Applications	A FLTRUL16	Filter Rule Connection		
- Elter Set Method	AFLTOUL17	Filter Rule Connection		
- 🥥 Adobe Apps	AFLTRUL18	Filter Rule Connection		
Exclude All	A FLTRUL19	Filter Rule Connection		
— I All Apps - Except Base OS Apps	DA FLTRUL20	Filter Rule Connection		
 Concurrency - Novadigm Apps Only 	DAFLTRUL21	Filter Rule Connection		
 Default Filter Set Parameters 	A FLTRUL22	Filter Rule Connection		
- Inventory Only - Incl. All Files	DA FLTDUL23	Filter Rule Connection		
Microsoft Licensed Applications Usage - Include All Files	DAFLTRUL24	Filter Rule Connection		
Urage - Include All Files	A FLTRUL25	Filter Rule Connection		
Path (PATH)	Con Street			
A contract	-			

The Filter Set instance is complete. You are now ready to apply the filter to a collection instance. See the section Applying Filters on page 74 for more information.

Using Concurrency

Data usage collection is available either on a daily basis or on a more specific basis using concurrency. Concurrent data collection is enabled at the Filter Set level (UMFLTSET) in the CONCURR instance attribute.

Database Tree View:		Filter Set class All Apps	- Except Base OS Apps Instance Attributes:	
		Name	Attribute Description	Value
🕀 📲 Application (ZSERVICE)		V NAME	Friendly Name	All Apps - Except Base OS Apps
Application Packages (PACKAGE)		V INCLUSAG	Include Usage Data [Yes/No]	Yes
Client Methods (CMETHOD)		V CONCURR	Collect Concurrency Data [Yes/No]	No
Collection (UMCOLLCT)		FLTRUL01	Filter Rule Connection	USAGE.UMFLTRUL.INCLALL
Configuration (UMCONFIG)		AFLTRUL02	Filter Rule Connection	USAGE.UMFLTRUL.EXCL_MICROSOFT_OS_FILES_1
Database (UMDBASE)		IA FLTRUL03	Filter Rule Connection	USAGE.UMFLTRUL.EXCL_WINDOWS_OS_ADD_ON_P
Destination Point (UMDESTPT)		AFLTRUL04	Filter Rule Connection	USAGE.UMFLTRUL.EXCL_WINDOWS_OS_ADD_ON_P
File Resources (FILE)		A FLTRUL05	Filter Rule Connection	
File Root (FILEROOT)		A FLTRUL06	Filter Rule Connection	
 Filter Criteria (UMFLTCRI) Filter Rule (UMFLTRUL) 		AFLTRUL07	Filter Rule Connection	
□ · · · · · · · · · · · · · · · · · · ·		A FLTRUL08	Filter Rule Connection	
B All Apps - Except Base OS Apps		FLTRUL09	Filter Rule Connection	
Include All		AFLTRUL 10	Filter Rule Connection	
Excl - Microsoft OS Files - 1	-	ň		

To enable concurrency usage data collection

- 1 Navigate to an existing Filter Set instance (see To create the Filter Set instance on page 79 for details on how to create Filter Sets instances).
- 2 Double-click the **CONCURR** instance attribute.

No Yes N		
No Vo Name	Attribute Description	Value
V NAME	Friendly Name	All Apps - Except Base OS Apps
V INCLUSAG	Include Usage Data [Yes/No]	Yes
V CONCURR	Collect Concurrency Data [Yes/	No
А СМЕТНОД	Filter Set Client Method	CMETHOD.UMFLTSET
FLTRUL01	Filter Rule Connection	USAGE.UMFLTRUL.INCLALL
FLTRUL02	Filter Rule Connection	USAGE.UMFLTRUL.EXCL_MICROSOFT_OS_FILES_1
FLTRUL03	Filter Rule Connection	USAGE.UMFLTRUL.EXCL_WINDOWS_OS_ADD_ON_PRO
FLTRUL04	Filter Rule Connection	USAGE.UMFLTRUL.EXCL_WINDOWS_OS_ADD_ON_PRO

3 From the drop-down list select **Yes**, and then click **OK**. Click **Yes** to save your changes.

Concurrency usage data collection has been enabled. Concurrent usage data will now be collected for the appropriate applications in fifteenminute intervals, by default.



Concurrent usage data collection generates a large amount of data. Make sure you have enough available resources before you begin collecting this type of data.

Initiating Inventory and Usage Collections

The executables, USDBINVN.exe and USDBColl.exe can be used to initiate the collection of inventory and usage data respectively. After a default installation, these files are located in the \Program Files\Hewlett-Packard\HPCA\AUM Agent\bin\ folder.

Initiating Inventory Data Collection

The executable usdbinvn.exe, collects current inventory data on a target machine. Run this executable to force inventory collection for any machine with the Application Usage Manager Agent installed. No parameters are required. The inventory information is stored within the history.usdbase file, on the local machine at the root of the \Usage Manager \ directory.

Configuring Usage Data Collection

The executable, usdbcoll.exe, is responsible for configuring the Application Usage Manager data collection environment on the agent device.

Defining a Database Collection Point

A database definition contains the information required to send the collected usage data to a specific collection point in the backend infrastructure. It has a unique name and associated parameters.

Database entries can be configured in the Configuration Server Database in the PRIMARY File USAGE Domain. Default database and associated configuration parameters are shipped with the Application Usage Manager. To manually define a database collection point, run the following command:

USDBCOLL.EXE /i DatabaseName=SQL_database_name

The /i parameter indicates an **install database** operation.

Initiating a Usage Data Collection Request

Execute the USDBColl.exe module to initiate a data collection request. It can be launched by the Application Usage Manager internal scheduler, by an HPCA service or Notify request, or otherwise. Any filtering is applied during the collection process.

To launch a collection, run the following command for the specific database name defined in the command line:

USDBCOLL.EXE DatabaseName=SQL_database_name

Initiating a Usage Data Re-collection Request

Once data has been collected, it is not sent to the server again during a normal collection request.



Consider the consequences before recollecting usage data. Recollection may result in duplicate data or a corrupted SQL database if not done within strict guidelines and without the consent of HP Technical Support.

To initiate a re-collection of data (data already sent to the server), execute the usdbcoll.exe module using the following command line options:

USDBCOLL.EXE DatabaseName=SQL_database_name, RecollectMode=3

See Table 13 on page 117, for a description of the ${\tt USDBCOLL}$. EXE parameter values.

 Table 8
 USDBCOLL.EXE Command Line Parameters

Parameter	Description
DatabaseName=Uniq ueSQLDatabaseName	Defines a unique SQL database name for collection purposes.

Parameter	Description
RecollectMode=Value	Defines the type of data to be re-collected. Value can be 1, 2, or 3 as defined below.
	1 – Signatures - all file signature data is re- collected for all files that meet the collection filter. This includes the data for the FileSignatures and FileSignatureProperties tables.
	2- Files - all Windows file data is recollected for all files that meet the collection filter. This includes all of the data collected in Signature mode as well as data for the WindowsFiles and WindowsFileInstances tables.
	3 – Usage - all Windows file usage data is re- collected for all files that meet the collection filter. This includes all of the data collected in File mode as well as data for the WindowsFileUsage table.

Enabling Privacy

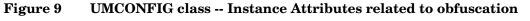
The Application Usage Manager allows for the obfuscation of certain data attributes in order to ensure privacy, if required. The following information can remain undisclosed:

- **User Name** The user name is reported as [AnyUser].
- **Computer Name** The computer name is reported as a random set of alphanumeric values.
- Domain Name

The domain name is reported as a random set of alphanumeric values.

• Usage Times

The executable file usage times and launch counts are all reported as zero values.



abase Tree View:	Filter Set class All Apps	- Except Base OS Apps Instance Attributes:	
	▲ Name	Attribute Description	Value
Application (ZSERVICE)	NAME	Friendly Name	All Apps - Except Base OS Apps
Application Packages (PACKAGE)	INCLUSAG	Include Usage Data [Yes/No]	Yes
Client Methods (CMETHOD)	CONCURR	Collect Concurrency Data [Yes/No]	No
Collection (UMCOLLCT)	FLTRUL01	Filter Rule Connection	USAGE.UMFLTRUL.INCLALL
Configuration (UMCONFIG)	FLTRUL02	Filter Rule Connection	USAGE.UMFLTRUL.EXCL_MICROSOFT_OS_FILES_1
Database (UMDBASE)	FLTRUL03	Filter Rule Connection	USAGE.UMFLTRUL.EXCL_WINDOWS_OS_ADD_ON_P
Destination Point (UMDESTPT)	FLTRUL04	Filter Rule Connection	USAGE.UMFLTRUL.EXCL_WINDOWS_OS_ADD_ON_P
	A FLTRUL05	Filter Rule Connection	
Filter Criteria (UMFLTCRI)	AFLTRUL06	Filter Rule Connection	
Filter Rule (UMFLTRUL)	- AFLTRUL07	Filter Rule Connection	
	AFLTRUL08	Filter Rule Connection	
All Apps - Except Base OS Apps	A FLTRUL09	Filter Rule Connection	
Include All	AFLTRUL 10	Filter Rule Connection	
Excl - Microsoft OS Files - 1	A	and a second second	

• Four attributes in the UMCONFIG Class directly relate to this information. Set these values to Y to hide the related data.

Attribute	Description
OBFSUSER	Set this value to Y to obfuscate user name data.
OBFSCOMP	Set this value to Y to obfuscate computer name data.
OBFSDOMN	Set this value to Y to obfuscate domain name data.
OBFSUSAG	Set this value to Y to obfuscate user usage time data.

Table 9 Obfuscation attributes of the UMCONFIG class

Internet Explorer Usage Counts for Windows Vista

When the Internet Explorer is running on Windows Vista (x64) with the "Enable Protected Mode" selected (from the Tools \rightarrow Internet Options \rightarrow Security menu), each launch of the application will result in a usage count of two.

This is because when the user launches Internet Explorer, it first runs IEUser.exe, which runs at the default medium-integrity level. IEUser.exe then spawns a low-integrity level executable, IExplorer.exe, which is the program the user sees and interacts with. Hence the usage count will always be two for each launch of the Internet Explorer.

5 Viewing Application Manager Usage Reports

At the end of this chapter, you will:

- Know how to access and use the Reporting Server to view the usage information obtained from agent computers.
- Be able to navigate through the information collected by clicking hyperlinks embedded within any table.
- Alternatively, know how to access and use a Web browser to view the usage information obtained from agent computers.

Accessing the Reporting Server

To access the Reporting Server

• Open a Web browser and type the following address:

```
http://<hostname>/reportingserver
```

Where <hostname> is the host name of the Apache web server on which the Reporting Server was installed and where reportingserver is the alias assigned to Reporting Server during its installation.



Reporting is optimized for display screen area setting 1024 x 768 or greater.



For better performance, stop the **HPCA Knowledge Base Server** before viewing usage reports from the Reporting Server. Refer to Starting and Stopping the KB Server on page 47 for more information.

Viewing Usage Information Using the Reporting Server

The Reporting Server provides web-based reports for Application Usage Manager. For installation and configuration instructions for the Reporting Server, refer to the *Reporting Server Guide*. The Reporting Server installation media is included with the Infrastructure media.



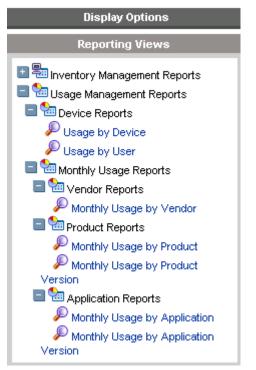
Usage reports may need to be enabled. This is done using the Reporting Server configuration file (setup.tcl). Refer to the *Reporting Server Guide* for more details.

Reporting Views for Usage Reports

To view the reports, first access your Reporting Server. Then, under Reporting Views, click **Usage Management Reports** to expand the list of reports.

There are different types of inventory reports:

- Device Reports Summaries
- Monthly Usage Reports





Filtering Usage Management Reports with Reporting Server

Reporting Server provides extensive filtering capabilities. To access the filters, expand Usage Management Related in the Search Options section of the Reporting Server page.

Filter types include:

- Device Related
- OS Related
- Software Related
- Interval Related

Figure 11 Usage Management Related Data Filters



Expand each individual Usage Management Related Data Filter to refer to the available filters you can apply to the current Reporting View.

For more information on creating filters and using the Reporting Server in general, refer to the *Reporting Server Guide*.

6 Using the Application Usage Manager Administrator

Use the Application Usage Manager Administrator to create specific search criteria to be implemented when you are generating your usage monitoring reports. Creating these criteria allow you to supplement the existing search options and create better reports based on your individual organization's needs. The Application Usage Manager Administrator is installed as part of the Application Usage Manager.

To access the Application Usage Manager Administrator

- From the Start menu, go to HP Client Automation Application Usage Manager → Application Usage Manager Admin.
- 2 Select the name of the DSN you will be using and type your User Name and Password in the text boxes provided.
- 3 When finished, click **OK**.

The Application Usage Manager Admin consists of four tabs you can use to define criteria, rules, rule sets, and rule set groups.

Application Usage Manager Admin Search Function

After selecting criteria, rule, rule set, or rule set group, click the **Search** button near the bottom of the window to preview your query results. Query results are displayed in a table at the bottom of the Application Usage Manager Admin window.

The search function can be used at any stage of the rule creation process.

Creating Criteria, Rules, Rule Sets, and Rule Set Groups

Use the Application Usage Manager Admin to create criteria, rules, rule sets, and rule set groups that can then be used when you generate usage reports.

Operators AND versus OR

There are two types of criteria, rules, rule sets, and rule set groups you can create: AND and OR. Before creating the rule, decide which type you would like to create and select the appropriate operator from the Operator drop-down list.

Figure 12 Operator drop-down list

Criteria Rules Rule Sets Rule Set Groups	
Rule Set Groups	
Microsoft Office and Internet Applications Operator: OR	Add Delete
AND	
Rule Sets	
🗹 Internet Apps - All	

Microsoft Office All Versions

Creating a criterion using the AND operator specifies that in order for a record to match that criterion, all of the properties specified must be true. For example, a criterion designed with

Vendor property	=	Equals Microsoft
Application property	=	Like WinWord
Operator	=	AND

will return only Microsoft Word records.

If the OR operator was selected in the above example, all applications with Vendor Microsoft will be returned.

The AND operator is most effective when creating criteria only. The OR operator is more appropriate for creating rules, rule sets, and rule set groups.

Criteria Tab

Use the Criteria tab to define specific application criteria you will use to display collected information when generating usage monitoring reports.

Property	Condition	Value(s)	Description	
<u>S</u> earch (Esc to can	cel) <u>C</u> opy SQL	to Clipboard		

Figure 13 Criteria tab

Before you select application criteria, you can use the Criteria drop-down list to check if any of the existing applications can be used.

Figure 14 Choose an existing application to define criteria

Criteria Rules Rule Sets Rule Set Groups	
Criteria	
Microsoft Excel	-
License Compliance Wizard	
McAfee VirusScan	
_ microsoft	
Microsoft (R) .NET Framework	
Microsoft (R) Network Monitor	
- Microsoft .NET Framework Microsoft Access	
Microsoft Agent Server	
Microsoft Clip Gallery	
Microsoft Data Access Components	
Microsoft Distributed Transaction Coordinator	
Microsoft Equation Editor	
Microsoft Excel	
Microsoft Exchange	
Microsoft IME 2000 Microsoft Map	
Microsoft Office 2000	
Microsoft Office XP	
Microsoft Open Database Connectivity	
Microsoft Organization Chart	-

Once you select an application from this list, check a Property box to add that to the Criteria.

Figure 15	Select a property	to include	in the criteria
-----------	-------------------	------------	-----------------

Microsoft Excel - All Versions	3		▼ Operator: AND ▼ Add Delete		
Property	Condition	Value(s)	Description		
Vendor			Vendor who created the file		
Product Name			Product Name that uses the file		
Product Version			Product version number in Ver.Rel.Mod.Build for		
Application	Equals	excel.exe	Application file name		
Application Version			Application version number in Ver.Rel.Mod.Build		
Application Description			Application file description		
🗖 Original File Name			Original file name - if renamed		
Root Logical Folder			Root folder name - i.e. ProgramFilesFolder or Sys		
Path Suffix			Remainder of path name after Logical Root - i.e		
MD5 Hash			Calculated MD5 hash value		
Mod CRC			Calculated module header CBC value		

Double-click any row in the Condition or Value columns to add a condition and value to the criteria. As an example, the steps below describe how to create rule criteria where the Vendor property is equal to Microsoft.

Microsoft			Operator: AND Add Delete
Property	Condition	Value(s)	Description
✓ Vendor	Like	Microsoft	Vendor who created the file
Product Name			Product Name that uses the file
Product Version			Product version number in Ver.Rel.Mod.Build for
Application			Application file name
Application Version			Application version number in Ver.Rel.Mod.Build
Application Description	Cr	iteria : ¥endor	
Original File Name			
Root Logical Folder		Condition: Like	
Path Suffix		Value: Microsoft	
MD5 Hash		Value: Microsoft	
Mod CRC			OK Cancel

Figure 16 Select a criteria condition and value

To create a criterion

1 To the right of the Criteria drop-down box, click the **Add** button to create new criteria. Enter a name for the criteria in the dialog box that opens.

Criteria Rules Rule Sets H Criteria Microsoft	Rule Set Groups		Operator: AND Add Delete	,
Property	Condition	Value(s)	Description	_
☑ Vendor	Like	Microsoft	Vendor who created the file	
Product Name			Product Name that uses the file	
Product Version			Product version number in Ver.Rel.Mod.Build for	
Application			Application file name	
Application Version			Application version number in Ver.Rel.Mod.Build	
Application Description			Application file description	
Original File Name Add Co	riteria			×
Root Logical Fold				OK
Path Suffix				
MD5 Hash				Cancel
Mod CRC				
,				_
Search Cop	y SQL to Clipboard			

Names are sorted in the report pages in ascending sequence so frequently used names should be prefixed with a character that places them at the top of the sort sequence.

- 2 Click **OK** to close the Add Criteria dialog box.
- 3 Double-click on the **Vendor** attribute row.
- 4 In the dialog box that opens, select **Equals** in the Condition text box.
- 5 In the Value text box, type Microsoft. Note that this value is used in a SQL command and must conform to SQL syntax rules.

The typed text must conform to SQL Server query rules, for example, you can select the **LIKE** clause and type text such as **Microsoft*** to define a criterion for any application whose Vendor definition contains the character string Microsoft.

Criteria : ¥	endor				×
Condition:	Equals			-	
Value:					
		OK	Cancel		

The use of LIKE clauses with preceding % may cause lengthy search times during reporting. We strongly recommend that you use the EQUALS clause.

6 Test the criteria by clicking **Search** to retrieve all entries in the Application Usage Manager Knowledge Base that match the criteria you defined. Entries are displayed in the table at the bottom of the window.

All Applicatio	ons			▼ Operator: △	ND <u>A</u> dd	Delete		
Property		Condition	Value(s)	Description				
✓ Vendor		Equals	Microsoft	Vendor who created t	he file			
Product Na	ame			Product Name that us	es the file			
Product Ve	rsion			Product version numb	er in Ver.Rel.Mod.Bu	uild for		
				Application file name				
	Version			Application version nu	umber in Ver.Rel.Mod	.Build		
	Description			Application file descrip	ation			
Original File				Original file name - if n				
Root Logic				Root folder name - i.e		or Sue		
Dath Cuffig.								
				Remainder of path na	~	u - i.e		
Path Suffix MD5 Hash Mod CRC				Calculated MD5 hash Calculated module he	value	▼		
MD5 Hash Mod CRC Search	Copy S	QL to Clipboard	Application	Calculated MD5 hash Calculated module he	value ader CRC value		Product Name	6
MD5 Hash Mod CRC Search sSignature_id	Copy S	d Application	Application	Calculated MD5 hash Calculated module he	value	Device	Product Name	<u>A</u>
MD5 Hash Mod CRC Search	Copy S		xe 2.0.0.1	Calculated MD5 hash Calculated module he	value ader CRC value		Product Name Microsoft uncol	
MD5 Hash Mod CRC Search Signature_id 5 77	Copy S WindowsFile_ 16454	d Application Gprswizard.E		Calculated MD5 hash Calculated module he Versi Vendor Microsoft	value ader CRC value	Device Device005		A A U U
MD5 Hash Mod CRC Search Signature_id 5 5 77 22	Copy S WindowsFile 16454 5477 12208 21994	d Application Gprswizard.E Uncol.Exe Uncol.Exe Robocopy.E:	xe 2.0.0.1 1.0.0.0 1.0.0.0 xe 4.0.1.96	Calculated MD5 hash Calculated module he Versi Vendor Microsoft Microsoft Microsoft Microsoft	value ader CRC value	Device Device005 Device003 Device004 Device027	Microsoft uncol Microsoft uncol Microsoft Roboc	U
MD5 Hash Mod CRC Search Signature_id 5 77 37 2 2	Copy S WindowsFile_ 16454 5477 12208 21994 17811	d Application Gprswizard.E Uncol.Exe Uncol.Exe Robocopy.E Robocopy.E	xe 2.0.0.1 1.0.0.0 1.0.0.0 xe 4.0.1.96 xe 4.0.1.96	Calculated MD5 hash Calculated module he Versi Vendor Microsoft Microsoft Microsoft Microsoft Microsoft	value ader CRC value	Device Device005 Device003 Device004 Device027 Device028	Microsoft uncol Microsoft uncol Microsoft Roboc Microsoft Roboc	UUU
MD5 Hash Mod CRC Search Signature_id 5 7 37 2 2 2 2	Copy S WindowsFile 16454 5477 12208 21994 17811 8432	d Application Gprswizard.E Uncol.Exe Robocopy.E Robocopy.E Robocopy.E	xe 2.0.0.1 1.0.0.0 1.0.0.0 xe 4.0.1.96 xe 4.0.1.96 xe 4.0.1.96	Calculated MD5 hash Calculated module he Versi Vendor Microsoft Microsoft Microsoft Microsoft Microsoft	value ader CRC value	Device Device005 Device003 Device027 Device027 Device028 Device05	Microsoft uncol Microsoft uncol Microsoft Roboc Microsoft Roboc Microsoft Roboc	U U rc rc rc
MD5 Hash Mod CRC Signature_id 5 77 57 2 2 2 2 2	Copy S WindowsFile 16454 5477 12208 21994 17811 8432 15233	d Application Gprswizard.E Uncol.Exe Robocopy.E: Robocopy.E: Robocopy.E: Robocopy.E:	xe 2.0.1 1.0.0 1.0.0 xe 4.0.1.96 xe 4.0.1.96 xe 4.0.1.96 xe 4.0.1.96	Calculated MD5 hash Calculated module he Versi Vendor Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft	value ader CRC value	Device Device005 Device003 Device027 Device028 Device03	Microsoft uncol Microsoft uncol Microsoft Roboc Microsoft Roboc Microsoft Roboc Microsoft Roboc	U U rc rc rc rc
MD5 Hash Mod CRC Search Signature_id 5 5 7 2 2 2 2 2 2 2 2 2	Copy S WindowsFile_ 5477 12208 21994 17811 8432 15233 15166	d Application Gprswizard E Uncol Exe Nobocopy E Robocopy E Robocopy E Robocopy E Robocopy E	xe 2.0.0.1 1.0.0.0 1.0.0.0 xe 4.0.1.96	Calculated MD5 hash Calculated module he Versi Vendor Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft	value ader CRC value	Device Device005 Device005 Device004 Device027 Device005 Device038 Device044	Microsoft uncol Microsoft uncol Microsoft Roboc Microsoft Roboc Microsoft Roboc Microsoft Roboc	U U rc rc rc rc rc rc
MD5 Hash Mod CRC Signature_id 5 57 22 2 2 2 2 2 2 2 2 2 2 2 2 2 2	Copy S WindowsFile 16454 5477 12208 21994 17811 8432 15233 15166 9578	d Application Gprswizard.E Uncol.Exe Uncol.Exe Robocopy.E: Robocopy.E: Robocopy.E: Robocopy.E: Robocopy.E:	xe 2.0.0.1 1.0.0.0 1.0.0.0 xe 4.0.1.96 xe 4.0.1.96	Calculated MD5 hash Calculated module he Wersi Vendor Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft	value ader CRC value	Device Device005 Device003 Device027 Device028 Device038 Device038 Device044 Device03	Microsoft uncol Microsoft uncol Microsoft Roboc Microsoft Roboc Microsoft Roboc Microsoft Roboc Microsoft Roboc Microsoft Roboc	U U rc rc rc rc rc rc rc
MD5 Hash Mod CRC Search Signature_id 5 77	Copy S WindowsFile_ 5477 12208 21994 17811 8432 15233 15166	d Application Gprswizard E Uncol Exe Nobocopy E Robocopy E Robocopy E Robocopy E Robocopy E	ixe 2.0.0.1 1.0.0.0 1.0.0.0 1.0.0.0 1.0.0.0 xe 4.0.1.96 xe 4.0.1.96	Calculated MD5 hash Calculated module he Versi Vendor Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft	value ader CRC value	Device Device005 Device005 Device004 Device027 Device005 Device038 Device044	Microsoft uncol Microsoft uncol Microsoft Roboc Microsoft Roboc Microsoft Roboc Microsoft Roboc	U U rc rc rc rc rc

The new criterion is complete and ready to be used in any rules you generate.

Rules Tab

Rules are a combination of Criteria. Use the Rules tab to define rules based on the criteria you selected in the Criteria tab.

Criteria Rules Rule Sets Rule Set Groups
Rules Operator: OR Add Delete
Criteria
Show All

Figure 17 Rules tab

Use the Rules drop-down list box to select any default rules. Once a rule is selected, the criteria that are part of that rule are displayed.

Figure 18 Criteria for each rule is displayed

riteria Rules Rule Sets Rule Set Groups Rules Microsoft Office Professional - All Versions	Operator: OR <u>Add</u>
Criteria	
Microsoft Frontpage - All Versions	
Microsoft Outlook - All Versions	
Microsoft Powerpoint - All Versions	
Microsoft Access - All Versions	
Microsoft Excel - All Versions	
Microsoft Word - All Versions	
Show All	
SHOW AI	

To create a new Rule

1 Click **Add** to define a new rule. Enter a name for the rule in the dialog box that opens.

Add Rule	×
[OK
,	Cancel

- 2 Click OK.
- 3 Select any criteria you would like to include in the new rule by clicking the check box to the left of the criterion name.

Rules Microsoft Apps	T	Operator: OR	▼ <u>A</u> dd	Delete
Criteria				▲
All Applications				
Countrywide				
Microsoft Office 2000 Only				
FileNet Corporation				
FileNet LTS Executable				
Filenet Dispimg Executable				
Microsoft Internet Explorer - All Versions				
🗖 WinZip				
Microsoft Windows Explorer				-
1				

4 Test the rule by clicking **Search**. All matching records are displayed in the table at the bottom of the window.

Microsoft App	8						
Criteria						_	
All Applica	ations_						
Countrywide	e						
Microsoft 0	ffice 2000 Only						
FileNet Corp							
FileNet LTS							
	img Executable						
	iternet Explorer - All Ve						
	Remot Explorer - All Vi	ersions					
 ↓ WinZip		ersions					
☐ WinZip ☑ Microsoft W	/indows Explorer	ersions					
 ↓ WinZip						_	
☐ WinZip ☑ Microsoft W ◀						▼	
☐ WinZip ☑ Microsoft W		ersions				• •	
WinZip Microsoft W ✓ Show All	/indows Explorer					▼ ▶	
WinZip Microsoft W ✓ Show All <u>S</u> earch	/indows Explorer	to Clipboard		[
WinZip Microsoft W ✓ Show All <u>S</u> earch	/indows Explorer	to Clipboard	Application Versi	Vendor	Domain	Device	Product Name
WinZip Microsoft \\ Microsoft \\ Show All Search sSignature_id	Vindows Explorer	to Clipboard Application	5.51.4807.2300	Microsoft Corpor	Domain	Device040	Microsoft(R) Win
WirZip ☑ Microsoft W ◀ ☑ Show All <u>S</u> earch sSignature_id	/indows Explorer	to Clipboard Application lexplore.Exe lexplore.Exe	5.51.4807.2300 5.51.4807.2300	Microsoft Corpor Microsoft Corpor	Domain	Device040 Device010	Microsoft(R) Win Microsoft(R) Win
WirZip Wicrosoft W ✓ Show All <u>S</u> earch sSignature_id	/indows Explorer Copy SQL t WindowsFile_id 4450 3306 676	to Clipboard Application Lexplore.Exe Lexplore.Exe Lexplore.Exe	5.51.4807.2300 5.51.4807.2300 5.0.2920.0	Microsoft Corpor Microsoft Corpor Microsoft Corpor	Domain	Device040 Device010 Device002	Microsoft(R) Win Microsoft(R) Win Microsoft(R) Win
WinZip Microsoft W Show All Signature_id	/indows Explorer Copy SQL t WindowsFile_id 4450 3906 676 1569	to Clipboard Application lexplore.Exe lexplore.Exe lexplore.Exe Explore.Exe	5.51.4807.2300 5.51.4807.2300 5.0.2920.0 5.0.3315.2846	Microsoft Corpor Microsoft Corpor Microsoft Corpor Microsoft Corpor	Domain	Device040 Device010 Device002 Device017	Microsoft(R) Win Microsoft(R) Win Microsoft(R) Win Microsoft(R) Win
WinZip Microsoft W Show All Search Signature_id	/indows Explorer <u>Copy SQL t</u> <u>VindowsFile_id</u> 4450 3906 676 676 1569 7000	to Clipboard Application Iexplore. Exe Iexplore. Exe Explorer. Exe Explorer. Exe Explorer. Exe	5.51.4807.2300 5.51.4807.2300 5.0.2920.0 5.0.3315.2846 5.0.3315.2846	Microsoft Corpor Microsoft Corpor Microsoft Corpor Microsoft Corpor Microsoft Corpor	Domain	Device040 Device010 Device002 Device017 Device024	Microsoft(R) Win Microsoft(R) Win Microsoft(R) Win Microsoft(R) Win Microsoft(R) Win
Wirzīp ✓ Microsoft W ✓ Show All Signature_id • •	/indows Explorer Copy SQL t VindowsFile_id 4450 3906 676 676 1569 7000 6264	to Clipboard Application lexplore Exe lexplore Exe lexplore Exe Explorer Exe Explorer Exe Explorer Exe	5.51.4807.2300 5.51.4807.2300 5.0.2920.0 5.0.3315.2846 5.0.3315.2846 5.0.3315.2846	Microsoft Corpor Microsoft Corpor Microsoft Corpor Microsoft Corpor Microsoft Corpor Microsoft Corpor	Domain	Device040 Device010 Device002 Device017 Device024 Device043	Microsoft(R) Win Microsoft(R) Win Microsoft(R) Win Microsoft(R) Win Microsoft(R) Win Microsoft(R) Win
WinZip Microsoft W ✓ Show All <u>S</u> earch	/indows Explorer <u>Copy SQL t</u> <u>VindowsFile_id</u> 4450 3906 676 676 1569 7000	to Clipboard Application Iexplore. Exe Iexplore. Exe Explorer. Exe Explorer. Exe Explorer. Exe	5.51.4807.2300 5.51.4807.2300 5.0.2920.0 5.0.3315.2846 5.0.3315.2846	Microsoft Corpor Microsoft Corpor Microsoft Corpor Microsoft Corpor Microsoft Corpor	Domain	Device040 Device010 Device002 Device017 Device024	Microsoft(R) Win Microsoft(R) Win Microsoft(R) Win Microsoft(R) Win Microsoft(R) Win

The new rule is complete and ready for inclusion in any Rule Sets you generate.

Rule Sets Tab

A Rule Set is a grouping of Rules. Use the Rule Sets tab to define which rules you would like to combine to form a Rule Set instance.

Figure 19 Rule Sets tab

teria Rules Rule Sets Rule Set Groups Rule Sets	Operator: AND Add Delete	
Rules		
Show All		

Use the Rule Sets drop-down list to select any existing Rule Sets. Once a Rule Set is selected, the rules that make up that Rule Set are displayed.

Figure 20	Rules included in the Rule Set are displayed.	
Criteria Rules Rule S	ets Rule Set Groups	_

RuleSet Test					<u>▼</u> <u>A</u> dd		
,							
Rules							
Microsoft A	pps						
Microsoft OI	ffice Standard - All Ve	rsions					
Microsoft OI	ffice Professional - All	Versions					
	ieous Vendors						
** Immediate	e Interest Applications	2					
	e morest Appliedione						
_							
Z Show All							
		er u ul					
Show All	Copy SQL t	o Clipboard					
<u>S</u> earch	Copy SQL t	o Clipboard	Application Versi	Vendor	Domain	Device	Product Name
<u>S</u> earch	WindowsFile_id 4450	<u> </u>	Application Versi 5.51.4807.2300	Vendor Microsoft Corpor	Domain	Device Device040	Product Name
<u>S</u> earch	WindowsFile_id 4450 3906	Application lexplore.Exe lexplore.Exe	5.51.4807.2300 5.51.4807.2300	Microsoft Corpor Microsoft Corpor	Domain	Device040 Device010	Microsoft(R) Win Microsoft(R) Win
<u>S</u> earch	WindowsFile_id 4450 3906 676	Application lexplore.Exe lexplore.Exe lexplore.Exe	5.51.4807.2300 5.51.4807.2300 5.0.2920.0	Microsoft Corpor Microsoft Corpor Microsoft Corpor	Domain	Device040 Device010 Device002	Microsoft(R) Win Microsoft(R) Win Microsoft(R) Win
<u>S</u> earch	WindowsFile_id 4450 3906 676 1569	Application lexplore.Exe lexplore.Exe	5.51.4807.2300 5.51.4807.2300	Microsoft Corpor Microsoft Corpor	Domain	Device040 Device010	Microsoft(R) Win Microsoft(R) Win
<u>S</u> earch	WindowsFile_id 4450 3906 676 1569 7000	Application lexplore.Exe lexplore.Exe Explore.Exe Explore.Exe Explorer.Exe	5.51.4807.2300 5.51.4807.2300 5.0.2920.0 5.0.3315.2846 5.0.3315.2846	Microsoft Corpor Microsoft Corpor Microsoft Corpor Microsoft Corpor Microsoft Corpor	Domain	Device040 Device010 Device002 Device017 Device024	Microsoft(R) Win Microsoft(R) Win Microsoft(R) Win Microsoft(R) Win Microsoft(R) Win
<u>S</u> earch	WindowsFile_id 4450 3906 676 1569 7000 6264	Application lexplore.Exe lexplore.Exe Explore.Exe Explorer.Exe Explorer.Exe Explorer.Exe Explorer.Exe	5.51.4807.2300 5.51.4807.2300 5.0.2920.0 5.0.3315.2846 5.0.3315.2846 5.0.3315.2846	Microsoft Corpor Microsoft Corpor Microsoft Corpor Microsoft Corpor Microsoft Corpor Microsoft Corpor	Domain	Device040 Device010 Device002 Device017 Device024 Device043	Microsoft(R) Win Microsoft(R) Win Microsoft(R) Win Microsoft(R) Win Microsoft(R) Win Microsoft(R) Win
	WindowsFile_id 4450 3906 676 1569 7000 6264 6181	Application lexplore.Exe lexplore.Exe Explore.Exe Explorer.Exe Explorer.Exe Explorer.Exe Explorer.Exe	5.51.4807.2300 5.51.4807.2300 5.0.2320.0 5.0.3315.2846 5.0.3315.2846 5.0.3315.2846 5.0.3315.2846	Microsoft Corpor Microsoft Corpor Microsoft Corpor Microsoft Corpor Microsoft Corpor	Domain	Device040 Device010 Device02 Device017 Device024 Device043 Device030	Microsoft(R) Win Microsoft(R) Win Microsoft(R) Win Microsoft(R) Win Microsoft(R) Win Microsoft(R) Win
<u>S</u> earch	WindowsFile_id 4450 3906 676 1569 7000 6264	Application lexplore.Exe lexplore.Exe Explore.Exe Explorer.Exe Explorer.Exe Explorer.Exe Explorer.Exe	5.51.4807.2300 5.51.4807.2300 5.0.2920.0 5.0.3315.2846 5.0.3315.2846 5.0.3315.2846	Microsoft Corpor Microsoft Corpor Microsoft Corpor Microsoft Corpor Microsoft Corpor Microsoft Corpor	Domain	Device040 Device010 Device002 Device017 Device024 Device043	Microsoft(R) Win Microsoft(R) Win Microsoft(R) Win Microsoft(R) Win Microsoft(R) Win Microsoft(R) Win

To create a new Rule Set

- 1 Click **Add** to define a new Rule Set. Enter a name for the Rule Set in the dialog box that opens.
- 2 Click OK.
- 3 Select any rules you would like to include in the new Rule Set by clicking the check box to the left of the rule name.

Criteria Rules Rule Sets Rule Set Groups - Rule Sets		
	Operator: OR Add Delete	
Microsoft Office All Versions	Operator: OR <u>Add</u> <u>Delete</u>	
Rules		
Microsoft Office Standard - All Versions		
Microsoft Office Professional - All Versions		
🔲 Show All		

4 Test the Rule Set by clicking **Search**. All matching records are displayed in the table at the bottom of the Application Usage Manager Admin window.

I MICrosoft Uffi	ce All Versions		•	Operator: OR	▼ <u>A</u> dd	Delete	
Rules							
Microsoft A	pps						
Microsoft O	ffice Standard - All Ve	ersions					
Microsoft O	ffice Professional - All	Versions					
🔲 ** Miscellar	eous Vendors						
	e Interest Application:	\$					
		-					
Chave All							
Show All							
Show All	Copy SQL 1	to Clipboard					
<u>S</u> earch	<u>C</u> opy SQL I WindowsFile_id	to Clipboard	Application Versi	Vendor	Domain	Device	Product Name
<u>S</u> earch leSignature_id			Application Versi 5.51.4807.2300	Vendor Microsoft Corpor	Domain	Device Device040	Product Name Microsoft(R) Win
<u>S</u> earch eSignature_id 1	WindowsFile_id	Application			Domain		
<u>S</u> earch leSignature_id 11	WindowsFile_id 4450	Application lexplore.Exe	5.51.4807.2300	Microsoft Corpor	Domain	Device040	Microsoft(R) Win
<u>S</u> earch eSignature_id 1 1 4 9	WindowsFile_id 4450 3906 676 1569	Application lexplore.Exe lexplore.Exe lexplore.Exe Explore.Exe	5.51.4807.2300 5.51.4807.2300 5.0.2920.0 5.0.3315.2846	Microsoft Corpor Microsoft Corpor Microsoft Corpor Microsoft Corpor	Domain	Device040 Device010 Device002 Device017	Microsoft(R) Win Microsoft(R) Win Microsoft(R) Win Microsoft(R) Win
<u>S</u> earch eSignature_id 1 1 4 9 9	WindowsFile_id 4450 3906 676 1569 7000	Application lexplore.Exe lexplore.Exe Explore.Exe Explorer.Exe Explorer.Exe	5.51.4807.2300 5.51.4807.2300 5.0.2920.0 5.0.3315.2846 5.0.3315.2846	Microsoft Corpor Microsoft Corpor Microsoft Corpor Microsoft Corpor Microsoft Corpor	Domain	Device040 Device010 Device002 Device017 Device024	Microsoft(R) Win Microsoft(R) Win Microsoft(R) Win Microsoft(R) Win Microsoft(R) Win
<u>Search</u> leSignature_id 1 1 4 9 9 9 9	WindowsFile_id 4450 3906 676 1569 7000 6264	Application lexplore.Exe lexplore.Exe lexplore.Exe Explore.Exe	5,51,4807,2300 5,51,4807,2300 5,0,2920,0 5,0,3315,2846 5,0,3315,2846 5,0,3315,2846	Microsoft Corpor Microsoft Corpor Microsoft Corpor Microsoft Corpor Microsoft Corpor Microsoft Corpor	Domain	Device040 Device010 Device002 Device017 Device024 Device043	Microsoft(R) Win Microsoft(R) Win Microsoft(R) Win Microsoft(R) Win Microsoft(R) Win Microsoft(R) Win
<u>Search</u> leSignature_id 1 1 4 9 9 9 9 9	WindowsFile_id 4450 3906 676 1569 7000 6264 6181	Application lexplore.Exe lexplore.Exe Explore.Exe Explorer.Exe Explorer.Exe	5.51.4807.2300 5.51.4807.2300 5.0.2920.0 5.0.3315.2846 5.0.3315.2846 5.0.3315.2846 5.0.3315.2846	Microsoft Corpor Microsoft Corpor Microsoft Corpor Microsoft Corpor Microsoft Corpor Microsoft Corpor Microsoft Corpor	Domain	Device040 Device010 Device002 Device017 Device024 Device043 Device030	Microsoft(R) Win Microsoft(R) Win Microsoft(R) Win Microsoft(R) Win Microsoft(R) Win Microsoft(R) Win
	WindowsFile_id 4450 3906 676 1569 7000 6264	Application lexplore.Exe lexplore.Exe Explore.Exe Explorer.Exe Explorer.Exe Explorer.Exe	5,51,4807,2300 5,51,4807,2300 5,0,2920,0 5,0,3315,2846 5,0,3315,2846 5,0,3315,2846	Microsoft Corpor Microsoft Corpor Microsoft Corpor Microsoft Corpor Microsoft Corpor Microsoft Corpor	Domain	Device040 Device010 Device002 Device017 Device024 Device043	Microsoft(R) Win Microsoft(R) Win Microsoft(R) Win Microsoft(R) Win Microsoft(R) Win Microsoft(R) Win

The new Rule Set is complete and ready for inclusion in any Rule Set Groups you may generate.

Rule Set Groups Tab

If you want to combine multiple Rule Sets, create a Rule Set Group instance.

Figure 21 Rule Set Groups tab

		Operator: AND	Add De	elete	
Rule Sets					

Use the Rule Set Groups drop-down list to select any existing Rule Set Groups. Once a Rule Set Group is selected, all of the Rules Sets that make up that Rule Set Group are displayed.

Figure 22 Rule Sets included in the Rule Set Group are displayed

iteria Rules Rule Sets Rule Set Groups Rule Set Groups Microsoft Office and Internet Applications	•	Operator: OR	▼ _Add	Delete	_	
Rule Sets						
Internet Apps - All						
Microsoft Office All Versions						
RuleSet Test						
Show All						

To create a new Rule Set Group

- 1 Click **Add** to define a new Rule Set Group. Enter a name for the Rule Set Group in the dialog box that opens.
- 2 Click OK.
- 3 Select any Rule Sets you would like to include in the new Rule Set Group by clicking the check box to the left of the Rule Set name.

Rule Set Groups Microsoft Office and Internet Applications	•	Operator: OR	▼ <u>A</u> dd	Delete
Rule Sets				
🗹 Internet Apps - All				
Microsoft Office All Versions				
RuleSet Test				

4 Test the Rule Set Group by clicking **Search**. All matching records are displayed in the table at the bottom of the Application Usage Manager Admin window.

Rule Set Grou	E (A):			I San Marine		1		
Microsoft Offic	ce and Internet Applic	ations	<u>•</u>	Operator: OR	<u>▲</u> dd	Delete		
Rule Sets								
Internet App	ps - All							
Microsoft 0	ffice All Versions							
RuleSet Te	st							
Show All								
✓ Show All <u>S</u> earch	Copy SQL t	to Clipboard						
<u>S</u> earch	<u>Copy SQL</u>	to Clipboard	Application Versi	Vendor	Domain	Device	Product Name	A
<u>S</u> earch eSignature_id 93	WindowsFile_id	Application Winword Exe	9.0.0.3822	Microsoft Corpor	Domain	Device020	Microsoft Office	M
<u>S</u> earch eSignature_id 93 93	WindowsFile_id 19180 21138	Application Winword.Exe Winword.Exe	9.0.0.3822 9.0.0.3822	Microsoft Corpor Microsoft Corpor	Domain	Device020 Device016	Microsoft Office Microsoft Office	M
<u>S</u> earch eSignature_id 93 93 93	WindowsFile_id 19180 21138 12187	Application Winword.Exe Winword.Exe Winword.Exe	9.0.0.3822 9.0.0.3822 9.0.0.3822	Microsoft Corpor Microsoft Corpor Microsoft Corpor	Domain	Device020 Device016 Device004	Microsoft Office Microsoft Office Microsoft Office	M M M
<u>S</u> earch eSignature_id 93 93 93 93 93	WindowsFile_id 19180 21138 12187 22459	Application Winword Exe Winword Exe Winword Exe Winword Exe	9.0.0.3822 9.0.0.3822 9.0.0.3822 9.0.0.3822 9.0.0.3822	Microsoft Corpor Microsoft Corpor Microsoft Corpor Microsoft Corpor	Domain	Device020 Device016 Device004 Device058	Microsoft Office Microsoft Office Microsoft Office Microsoft Office	M M M M
<u>S</u> earch eSignature_id 93 93 93 93 93	WindowsFile_id 19180 21138 12187 22459 24592	Application Winword Exe Winword Exe Winword Exe Winword Exe Winword Exe	9.0.0.3822 9.0.0.3822 9.0.0.3822 9.0.0.3822 9.0.0.3822 9.0.0.3822	Microsoft Corpor Microsoft Corpor Microsoft Corpor Microsoft Corpor Microsoft Corpor	Domain	Device020 Device016 Device004 Device058 Device034	Microsoft Office Microsoft Office Microsoft Office Microsoft Office Microsoft Office	M M M M M
<u>Search</u> 93 93 93 93 93 93 93 93	WindowsFile_id 19180 21138 12187 22459 24592 8937	Application Winword.Exe Winword.Exe Winword.Exe Winword.Exe Winword.Exe Winword.Exe	9.0.0.3822 9.0.0.3822 9.0.0.3822 9.0.0.3822 9.0.0.3822 9.0.0.3822 9.0.0.3822 9.0.0.3822	Microsoft Corpor Microsoft Corpor Microsoft Corpor Microsoft Corpor Microsoft Corpor Microsoft Corpor	Domain	Device020 Device016 Device004 Device058 Device034 Device030	Microsoft Office Microsoft Office Microsoft Office Microsoft Office Microsoft Office Microsoft Office	M M M
<u>Search</u> eSignature_id 93 93 93 93 93 93 93 93 92	WindowsFile_id 19180 21138 12187 22459 24592	Application Winword Exe Winword Exe Winword Exe Winword Exe Winword Exe	9.0.0.3822 9.0.0.3822 9.0.0.3822 9.0.0.3822 9.0.0.3822 9.0.0.3822 9.0.0.3822 9.0.0.3822	Microsoft Corpor Microsoft Corpor Microsoft Corpor Microsoft Corpor Microsoft Corpor	Domain	Device020 Device016 Device004 Device058 Device034	Microsoft Office Microsoft Office Microsoft Office Microsoft Office Microsoft Office	M M M M M
<u>Search</u> eSignature_id 93 93 93 93 93 93 93 93 92	WindowsFile_id 19180 21138 12187 22459 24592 8937	Application Winword.Exe Winword.Exe Winword.Exe Winword.Exe Winword.Exe Winword.Exe	9.0.0.3822 9.0.0.3822 9.0.0.3822 9.0.0.3822 9.0.0.3822 9.0.0.3822 9.0.0.3822 9.0.0.3822	Microsoft Corpor Microsoft Corpor Microsoft Corpor Microsoft Corpor Microsoft Corpor Microsoft Corpor	Domain	Device020 Device016 Device004 Device058 Device034 Device030	Microsoft Office Microsoft Office Microsoft Office Microsoft Office Microsoft Office Microsoft Office	M M M M M
Search eSignature_id 93 93 93 93 93 93 93 92 92	WindowsFile_id 19180 21138 12187 22459 24592 8937 19178	Application Winword Exe Winword Exe Winword Exe Winword Exe Winword Exe Winword Exe Powerpht Exe	9.0.0.3822 9.0.0.3822 9.0.0.3822 9.0.0.3822 9.0.0.3822 9.0.0.3822 9.0.0.3822 9.0.0.3822	Microsoft Corpor Microsoft Corpor Microsoft Corpor Microsoft Corpor Microsoft Corpor Microsoft Corpor Microsoft Corpor	Domain	Device020 Device016 Device004 Device058 Device034 Device030 Device020	Microsoft Office Microsoft Office Microsoft Office Microsoft Office Microsoft Office Microsoft Office Microsoft Office	M M M M M M M M
Search eSignature_id 93 93 93 93 93 93 93 93 93 92 92 92 92	WindowsFile_id 19180 21138 12187 22459 24592 8937 19178 17647	Application Winword Exe Winword Exe Winword Exe Winword Exe Winword Exe Winword Exe Powerpht Exe Powerpht Exe	9.0.0.3822 9.0.0.3822 9.0.0.3822 9.0.0.3822 9.0.0.3822 9.0.0.3822 9.0.0.3822 9.0.0.3821	Microsoft Corpor Microsoft Corpor Microsoft Corpor Microsoft Corpor Microsoft Corpor Microsoft Corpor Microsoft Corpor Microsoft Corpor	Domain	Device020 Device016 Device004 Device058 Device034 Device030 Device020 Device013	Microsoft Office Microsoft Office Microsoft Office Microsoft Office Microsoft Office Microsoft Office Microsoft Power	M M M M M M M M
✓ Show All Search Besignature_id 93 93	WindowsFile_id 19180 21138 12187 24592 24592 8937 19178 17647 17731	Application Winword Exe Winword Exe Winword Exe Winword Exe Winword Exe Winword Exe Powerpnt Exe Powerpnt Exe Powerpnt Exe	9.0.0.3822 9.0.3822 9.0.3822 9.0.3822 9.0.3822 9.0.3822 9.0.3822 9.0.3821 9.0.3821 9.0.3821	Microsoft Corpor Microsoft Corpor Microsoft Corpor Microsoft Corpor Microsoft Corpor Microsoft Corpor Microsoft Corpor Microsoft Corpor Microsoft Corpor	Domain	Device020 Device016 Device004 Device058 Device030 Device030 Device020 Device013 Device016	Microsoft Office Microsoft Office Microsoft Office Microsoft Office Microsoft Office Microsoft Office Microsoft Power Microsoft Power	

The new Rule Set Group is complete.

Now that you have finished creating criteria, rules, rule sets, and rule set groups, you can generate reports based on your own specifications using the report generator options Include Rule and Exclude Rule. For more information, refer to Viewing Application Manager Usage Reports on page 86.

A Implementing Application Usage Manager in a Non-HPCA Environment

The Application Usage Manager agent can operate independently of an HPCA environment. This implementation is often used by organizations to determine priorities for application or operating system migrations.

Included with the Application Usage Manager media is an MSI-based program to install and configure the Application Usage Manager agent.

These files are located in your Application Usage Manager media in the \Agent Install\Setup\ directory and are described in Table 10 below.

Filename	Description
AUMAgent.msi	Agent installation program.
USDBColl.ini	Collection configuration file

 Table 10
 Application Usage Manager Agent files

Application Usage Manager Configuration: Non-HPCA Infrastructure

To configure your Application Usage Manager components for this environment, refer to Chapter 2, Configuring Your Environment on page 25. Once your Application Usage Manager components are configured, you are ready to configure and install the agent and collection parameters.

Installing and Configuring the Application Usage Manager Agent

The Application Usage Manager agent is installed by either an HPCA service, independently through any distribution methodology, or by running the Agent Installation Wizard.



Non-HPCA implementation does not support filters inherently. Specific Registry keys must be configured.

Using the Installation Wizard

To install the Application Usage Manager agent using the Installation Wizard

1 From the media location for Application Usage Manager, navigate to the \Agent Install\Setup folder, and double-click AUMAgent.msi.

The Installation Wizard for the Application Usage Manager Agent opens.

- 2 Click Next. The License Agreement window opens.
- 3 After reading and accepting the license agreement, click **Next**. The installation configuration options window opens.

HP Client Automation Application Usage Manager Agent 7.50 Setup	<u>_ ×</u>
Select the installation configuration options	
Usage Collection Database path	
C:\Program Files\Hewlett-Packard\HPCA\AUM Agent\Usage Manager\	Browse
Number of daily logs to keep on each managed device	
Number of months to save history data on each managed device 12	
<u> </u>	Cancel

Use this window to specify a Usage Collection Database Path, how many daily logs to keep, and how many months of data to save on each managed device.

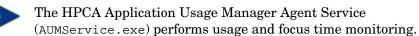
- In the Usage Collection Database Path area, specify a local path where the agent will be installed and usage data history and monitoring files will be stored. The default location is SystemDrive:\Program Files\Hewlett-Packard\HPCA\AUM Agent. If you want to select a different path, click Browse and then navigate to an appropriate local folder.
- In the Number of daily logs to keep text box, type the maximum number of daily log files to be maintained in the \Log folder. The default is 7.
- In the Number of months to save history data text box, type the number of months to maintain data in the History.USDBase file. Old data is automatically aged out of the file after the specified retention period.



The History data file serves as a backup location for monitored data in case it needs to be recollected. (For example, in case the KB Server is faulty.) 4 Click Next.

The Usage Monitoring Options window opens. Select the monitoring options to be enabled for this Agent.

- Leave Enable Usage Monitoring checked to monitor application usage, or remove the check-mark to disable it.
- Leave Enable Focus Time Monitoring checked to monitor the application focus time, or remove the check-mark to disable it.



5 Click **Next**. The Data Obfuscation Options window opens.

Select data obfuscation op This option allows for the obfuscation of the following data attributes in order to ensure end-user privacy.
Obfuscate Domain Names Check to store and report domain names as an alphanumeric alias names
Obfuscate Computer Names Check to store and report computer names as an alphanumeric alias names
Obfuscate User Names Check to store and report user names as 'AnyUser'
Obfuscate Usage Data Check to store and report usage times and counts as zero values
< <u>B</u> ack <u>N</u> ext > Cancel

The Application Usage Manager allows for the obfuscation of certain data attributes in order to ensure privacy, if required.

6 Select from the following obfuscation options to have that type of data remain undisclosed:

— Obfuscate Domain Names

When selected, the domain name is reported as a random set of alphanumeric values.

Obfuscate Computer Names

When selected, the computer name is reported as a random set of alphanumeric values.

— Obfuscate User Names

When selected, the user name is reported as [AnyUser].

— Obfuscate Usage Data

When selected, the executable file usage times and launch counts are all reported as zero values.

7 Click Next. The Select Inventory Options window opens.

Scan Interval: Weekly Day of Month: 1 Day of Week: Sunday Hour: 0 Minute: 0 File Signature Mode: File Size Delay Minutes: 0	
Hour: 0 Minute: 0 File Signature Mode: File Size Delay Minutes: 0	*
File Signature Mode: File Size Clay Minutes: 0	*
	*
Inventory monitoring should be enabled by default between the hours of 12:00 midnight a 6:00 am on Saturday or Sunday mornings	ind

- 8 Leave Enable Inventory Monitoring checked to perform a software and hardware inventory scan on the Agent machine on a regular basis. Remove the check-mark to disable inventory monitoring.
- 9 If inventory monitoring is enabled, specify a scan schedule as follows:
 - Use the Scan Interval drop-down box to select an interval of Daily, Weekly, or Monthly.
 - For a Daily scan, also select an Hour and Minute for the scan to run.
 - For a Weekly scan, also select a **Day of Week**, **Hour** and **Minute** for the scan to run.
 - For a Monthly scan, also select a **Day of Month**, **Hour** and **Minute** for the scan to run.

- 10 In the **Delay Minutes** text box, optionally type a maximum delay period, in minutes, to use to randomize the inventory collection time. Valid values are 0 (no randomized collection) to 720 minutes (collection is randomized between the specified hours and minutes and 12 hours later).
- 11 Select one of the following File Signature Mode options:
 - **File Size** (Default).
 - File Header. Scans the entire file header. Slower than File Size scans.
 - **MD5 Signature**. Most complete scan and slowest.
- 12 Click Next. The Ready to Install the Application window opens.
- 13 Click Next to begin the installation. The installation takes place.

After installation, a final window opens to indicate the Application Usage Manager Agent has been successfully installed.

14 Click **Finish** to close the Installation Wizard.

Silent Installation using a Command Line

Alternatively, use the following command to install the Application Usage Agent silently.

msiexec.exe /i AUMAgent.msi /lv* optional_parameters

Refer to Table 11 on page 110 for the list of optional parameters and their default values.

- Space separate parameter entries.
- Enclose all parameter values in quotation marks, as shown in the command sample below.

Sample Command

The following command shows a sample silent installation of the Application Usage Manager Agent.

```
msiexec.exe /i AUMAgent.msi /lv* <LogFilePath>
NOVADIGM_PATH=<NovadigmPath> LOCAL_PATH="\[NovadigmFolder\]"
ENABLED="1" ENABLE_FOCUS_TIME="1" HISTORY_SAVE_MONTHS="12#"
LOG_COUNT="7" OBFUSCATE_USER="0" OBFUSCATE_COMPUTER="0"
OBFUSCATE_DOMAIN=0 OBFUSCATE_USAGE="0"
```

Silent Installation Configuration Parameters

Parameter and Values	Description
<logfilepath></logfilepath>	Defines an alternate path for storing Log files. The default location is the \Log subdirectory of the UM_LocalPath value.
NOVADIGM_PATH =[ProgramFilesF older]\Hewlett-Packard\HPCA\AUM Agent\	Defines the root directory of where the Application Usage Manager agent binaries are to be installed on the agent machine. The binaries are stored in the \bin folder under this folder. The path must be a local drive; it cannot be a network drive.
LOCAL_PATH=[<u>ProgramFilesFolder</u>]] <u>\Hewlett-Packard\HPCA\AUM</u> <u>Agent\</u> <u>Usage Manager\</u>	Defines where the active usage monitoring and history files are stored on the agent machine. This path must be a local drive; it cannot be a network drive.
ENABLED= 0 or <u>1</u>	Defines whether application usage profiling is installed as active . If set to 0, then application usage is not monitored for any application.
ENABLE_FOCUS_TIME= 0 or <u>1</u>	Defines whether application focus time is monitored and reported on. If set to 0, then focus time is not monitored.

 Table 11
 Silent installation parameters for AUMAgent.msi

Parameter and Values	Description
FILE_SIGNATURE_MODE= S H M representing File <u>Sizes</u> File Header MD5 Signature	Determines the scanning depth for executables inventoried on each agent device. The type of scan defined here can determine the amount of time a collection may take.
	 S = File Sizes. Scans only file sizes. This is faster, but less comprehensive (default) H=File Header. Scans entire Module Header. Slower, more comprehensive. M=MD5 Signature. Slowest, most comprehensive.
HISTORY_SAVE_MONTHS= 0 - nnn Default is <u>12</u>	Defines the number of months to maintain data in the history file, History.usdbase. Old data is automatically aged out of the file. Default is 12.
INVENTORY_INTERVAL = 0 1 <u>2</u> 3 representing No Inventory Monthly <u>Weekly</u> Daily	Defines when the current executable inventory for the machine is run.
INVENTORY_DAY_OF_MONTH = 1 - 31	If the Inventory Interval is 1 [monthly], defines the relative day of the month that the current executable inventory should be run.
INVENTORY_DAY_OF_WEEK = $1-7$	If the Inventory_Interval is 2 [weekly], defines the relative day of the week that the current executable inventory should be run. 1 = Sunday, 7 = Saturday.
INVENTORY_HOUR= 00 – 23 where 13 is 01:00 pm	If the Inventory_Inventory is non- zero, defines what hour of the day the current executable inventory for the machine is run.

Parameter and Values	Description
INVENTORY_MINUTE = 00 - 59	Defines what minute of the hour the current executable inventory for the machine is run.
INVENTORY_RANDOM_MINUTE = 0 - 720	Defines a maximum period, in minutes, to use to randomize the inventory collection time. If non- zero, randomizes the collection process to occur anytime from the start time through a randomly generated number of minutes later. [0-720]
LOG_COUNT= 0 - nn	Maximum number of log files to be maintained in the \Log folder. Default is 7.
OBFUSCATE_COMPUTER = 0 1	Obfuscate computer name to conform to privacy laws. 1 = Yes 0 = No
OBFUSCATE_DOMAIN = 0 1	Obfuscate domain name to conform to privacy laws. 1 = Yes 0 = No
OBFUSCATE_USAGE = 0 1	Obfuscate usage information to conform to privacy laws. 1 = Yes 0 = No
OBFUSCATE_USER = 0 1	Obfuscate user name to conform to privacy laws. 1 = Yes 0 = No

Configuring the Application Usage Manger Agent for SSL Communications with a Secured Portal

The Application Usage Manager (AUM) Agent can support communications with a secured Portal or Integration Server using HTTPS.

To configure the AUM Agent for this support, do the following:

- 1 Stop the AUM Agent Service.
- 2 Create the following \HPCA\Agent directory on the machine where the AUM Agent is installed:

[ProgramFilesFolder]\Hewlett-Packard\HPCA\Agent

3 Locate the AUM Agent folder on the HPCA media and copy the \CACertificates folder and its contents to the \Agent directory created in Step 2:

[ProgramFilesFolder]\Hewlett-Packard\CM\Agent\CACertificates

- 4 Locate the file for the Server's certificate, located at: CM Server Path\etc\Certificates\ Server-hostname.netcert.pem
- 5 Copy the contents from the line that begins::

-----BEGIN CERTIFICATE

until

-----END CERTIFICATE

- 6 Paste this contents into the end of the cacert.pem file, located in the \CACertificates folder on the agent machine
- 7 Save your changes.
- 8 Use Regedit to modify the Registry information for the AUM Agent collection point.
- 9 Modify the URL from http to https and modify the port number to include the secured port, such as 443:

https://xxx.xxx.xxx:443/KB_Mgr1_Usage/

10 Restart the AUM Agent Service.

Modifying the Application Usage Manager Agent

After the installation of the Application Usage Manager Agent, rerun the AUMAgent.msi program to modify it. Following modification, you must restart the service for the **HPCA Application Usage Manager Agent** to put the changes into effect.

1 Double-click **AUMAgent.msi** on the installation media. The Application Maintenance window opens.

- 2 Select **Modify** and click **Next**. Complete the prompts to modify the AUM Agent.
- 3 After modifying the AUM Agent, you must restart the HPCA Application Usage Manager Agent Service.

Removing the Application Usage Manager Agent

After the installation of the Application Usage Manager Agent, rerun the AUMAgent.msi program to delete it.

- 1 Double-click **AUMAgent.msi** on the installation media. The Application Maintenance window opens.
- 2 Select **Remove** and click **Next**. The Uninstall window opens.
- 3 Confirm you want to remove the agent and click Next.
- 4 The agent is removed. Click **Finish** when it is complete.

Silent Removal of the Agent

Use the following command to remove the Application Usage Manager agent silently:

msiexec.exe /i AUMAgent.msi /x

Common Files Required by Application Usage Manager Agent

Once the Application Usage Manager agent is installed, three files must be copied to the same directory where you installed the agent, for example, Drive:\ProgramFilesFolder\Hewlett-Packard\HPCA\AUM Agent\. These files are included with the Application Usage Manager media and are listed below:

• gzip.exe

Located in the <code>\Agent Install\Setup\GZIP</code> folder, the GZIP (generic zip) utility is used by the Application Usage Manager Agent and Knowledge Base Server to compress and decompress data during transfer to and from a SQL database.

• Readme.txt

Located in the Agent <code>Install\Setup\GZIP</code> directory, the <code>Readme.txt</code> file explains where to obtain the following files, also needed by the Agent in a non-HPCA environment:

- nvdkit.exe
 Collection of components used by the Application Usage Manager.
- hide.exe
 Hides the nvdkit.exe user interface from the process.

Collecting Data

The Usage Database Collection is installed using the USDBColl.exe program, which is placed in the \Application Extensions\Bin folder of the agent's base installation directory. By default, the USDBColl.exe file is location in:

```
C:\Program Files\Hewlett-Packard\HPCA\AUM Agent\Bin.
```

Configuring Collection Parameters

Collect usage data by first defining collection parameters. Optionally, these parameters can be placed within a file USDBColl.ini and then named during the batch program to install the collection.

The collection parameters are installed when USDBColl.exe is executed.

Table 12, below, lists the collection configuration parameters used to define your usage data collection. They can be placed in a file named USDBColl.ini, if desired.

Parameter	Description
DatabaseName	Name of your Application Usage Manager database.
CollectionEnabled	Enable or disable collection. [Y/N].
CollectionInterval	When to process collections, monitor only (no collection), monthly, weekly, daily. $[0 1 2 3]$ Default is Daily (3).
CollectionDayOfMonth	When the interval is monthly, day of the month to process collection. [01-31]
CollectionDayOfWeek	When the interval is weekly, day of the week to process collection. Default is Sunday (1). [1-7].

 Table 12
 Collection Configuration File (USDBColl.ini)

Parameter	Description
CollectionHour	Hour to begin data collection process. [00-23] Default is Midnight (00).
CollectionMinute	Minute to begin data collection process. [00 – 59] Default is 00.
CollectionRandom	Randomizes collection process to occur anytime from the start time through a randomly generated number of minutes later. $[0 - 720]$
CollectionPoint	The IP address and port number of the associated Integration Server or Portal. Supports an SSL- secured server (requires the URL to specify HTTPS and the secure port number, such as 443).

Command to Install Usage Database Collection

Open a batch window and execute one of the following commands to install usage collection. You can either specify all collection parameters directly on the command line, or place the parameters in a configuration file named USDBCOLL.INI, and then name that file when you run USDBColl.exe.

USDBColl.exe /I <collection_parameter_list>

or

```
USDBColl.exe /I USDBCOLL.INI
```

To run USDBColl.exe using a parameter list

- 1 Open a command prompt, go to the InstallDir\AUM Agent\Bin.
- 2 Execute the following command:

```
USDBColl.exe /I DatabaseName=Usage_Database CollectionEnabled=1
CollectionInterval=3 CollectionDayOfMonth=1 CollectionDayOfWeek=1
CollectionHour=0 CollectionMinute=0 CollectionRandom=0
CollectionPoint=http://<<IS_Server_IP_Address:3466>>/KB_Mgr1_Usag
e/
```



Specify a secured Collection Point using the format:

CollectionPoint=https://<<IS_Server_IP_Address:443>>/K B_Mgr1_Usage

Configuring Database Specific Collection

The executable usdbcoll.exe initiates the data collection process and can be launched by an HPCA service or otherwise. Two command-line parameters are passed that indicate the SQL database specific configuration parameters to use when copying the information from the inventory and active monitoring files to the database specific collection file, for example:

USDBCOLL.EXE /i DatabaseName=SQL_database_name

See Table 13 below for a description of the USDBCOLL. EXE parameter values.

Re-collecting Usage Data

In the event you need to collect lost or damaged usage data, USDBCOLL.EXE supports the recollection of data with the /r parameter. To initiate recollection, use the /r parameter and define the **RecollectMode** value on the command line. For example:

USDBCOLL.EXE /r RecollectMode=1 DatabaseName=MyDatabase

See Table 13 below for a description of the different RecollectMode values.

Parameter	Description
DatabaseName= UniqueSQLDatabaseName	Defines a unique SQL database name for collection purposes.
RecollectMode=Value	Defines the type of data to be re-collected. Value can be 1, 2, or 3 as defined below.
	1 – Signatures: All file signature data is re-collected for all files that meet the collection filter. This includes the data for the FileSignatures and FileSignatureProperties tables.
	2 – Files: All Windows file data is recollected for all files that meet the collection filter. This includes all of the data collected in Signature mode as well as data for the WindowsFiles and WindowsFileInstances tables.
	3 – Usage: All Windows file usage data is re-collected for all files that meet the collection filter. This includes all of the data collected in File mode as well as data for the WindowsFileUsage table.

 Table 13
 USDBCOLL.EXE command line parameters

Generating Reports

Once the Application Usage Manager agent and collection parameters are installed, refer to Chapter 5, Viewing Application Manager Usage Reports on page 86 to learn about generating reports to view your usage data.

Installing the Application Usage Manager Agent and Collection Parameters

After you have configured your Application Usage Manager agent and configuration parameters using the two .ini files, you are ready to install the components to your agent computers.

These files will install the Application Usage Manager agent as well as the collection parameters you defined within each .ini file.

A sample batch file, AUMAgent.bat, is supplied with the Application Usage Manager media in the \Samples\ AUM Agent - Batch Install\ directory. The directory also contains these files:

- AUMAgent.bat
- AUMAgent.msi
- Collect.bat
- Sleep.exe
- USDBColl.ini

Run AUMAgent.bat to install the Application Usage Manager agent as well as the collection parameters you defined within each .ini file.

After the Application Usage Manager agent and collection parameters are installed, refer to Chapter 5, Viewing Application Manager Usage Reports on page 86 to learn about generating reports to view your usage data.

Index

A

accessing Reporting Server, 53, 86 active monitoring file, 22 active usage data, 22 All Apps – Except Base OS Apps instance, 73 Application Class, 59 Application instance, 61 Application Packages Class, 59 application usage data, 26 Application Usage Manager benefits, 12 configuration without HPCA infrastructure, 105 data collection types, 14 description, 12 installation options, 59 inventory scan, 60 packages, 59 processing, 15 services, 59 system requirements, 14 Application Usage Manager Admin Search Function, 90 Application Usage Manager Administrator, 90 accessing, 90 Application Usage Manager Administrator, installing, 41 Application Usage Manager agent installing, 105 Application Usage Manager Agent, 18 configuring, 61 HPCA install, 66 uninstalling, 114 Application Usage Manager Database, 27 Application Usage Manager Knowledge Base, 41

Archive subdirectory, 63 AUMAgent.msi, 104 AutoImport directories, 21, 42 Automated Import, 21 automated import server, 42

С

CCM Filter Set instance, 74 Client Automation infrastructure requirements, 17 Client Methods Class. 59 CM Extensions for WI, 26 **CMETHOD** attribute, 77 **CMETHOD Class**, 59 CMETHOD instance, 64, 66, 73 **COLLCNCT** instance, 64 Collection Class, 59, 72 Collection class instances, 60 applying filters, 74 Collection instance, 61 collection point, 39 secured with SSL, 39 **COLLHOUR** instance, 63 **COLLMIN** instance, 63 **COLLRAND** instance, 64 common infrastructure, 16 **COMPNAME** attribute, 77 **CONCURR** instance, 73 concurrency, 80 Concurrency – Incl Novadigm Apps instance, 74 concurrency usage, 14

concurrency usage data collection, 81 Configuration Class, 59 Configuration instance, 61 Criteria tab, 92

D

data collection requests, 22 data collection types, 14 Database Class, 59 DAYOFMON instance, 63, 65 DAYOFWK instance, 63, 65 DB_OWNER, 47 DBASCONN instance, 64 DBReconnect (msecs), 46 Default Filter Criteria Params, 75 Default Filter Set Parameters instance, 74 default filter sets, 73 DESCRIPT attribute, 76 DESTCONN instance, 64 Destination Point Class, 59

E

ENABLED attribute, 76 ENABLED instance, 64, 65 Exclude All filter rule, 68 Exclude All instance, 79 exclusion filter, 60, 71 executable file inventory scan, 22 export directories, 42

F

FILE Class, 59 File Resources Class, 59 File Root Class, 59 FILEDESC attribute, 77 FILENAME attribute, 77 FILEPATH attribute, 77 FILEROOT attribute, 76 FILEROOT class, 59 **FILEVER** attribute, 77 Filter class instances, 60 Filter Criteria class. 68 Filter Criteria Class, 59, 70 Filter Criteria, creating, 75 Filter Rule class, 68 Filter Rule Class, 60, 71 Filter Rule instance, creating, 78 Filter Set. 72 Filter Set class, 68, 72 Filter Set Class, 60, 73 Filter Set instance, 64 filter, applying to a Collection Class, 74 filtering usage management reports, 88 FLTRUL## instance, 73 FLTSET01 instance, 64 FLTSET02 attribute, 64 focus time, 22 FSIGMODE instance, 66

G

gzip.exe, 114

Η

hide.exe, 115 history file, 19 history.usdbase, 82 HP passport registration, 7 HPCA KB Server configuration control panel, 42 HPCA KB Server configuration control panel, 42 HPCA KB Server Configuration icon, 42

Implementing Application Usage Manager in a Non-HPCA Environment

hpkbmanager.exe, 47 HTTP_PUT request, 39

INCLUSAG instance, 73 inclusion filter, 60, 71 infrastructure requirements, 16 installation wizard installing Application Usage Manager agent, 105 installing Application Usage Manager agent Installation Wizard, 105 Internet Explorer usage counts doubled, 85 INTERVAL instance, 63, 65 Inventory Class, 60 inventory data, 14 initiating a collection, 82 Inventory instance, 61 Inventory Manager, 26 Inventory Only - Incl All Files instance, 74 **INVNHOUR** instance, 65 **INVNMIN** instance, 65

Κ

KB Server SQL server requirements, 47 starting and stopping, 47

Knowledge Base Server, 41 configuring autoimport directories, 43 installing, 42

L

Log Path, 46

Μ

MD5HASH attribute, 77

Microsoft Licensed Applications instance, 74

Ν

NAME attribute, 76 NAME instance, 63, 65, 73 nvdkit.exe, 115

0

OBFSCOMP, 85 OBFSDOMN, 85 OBFSUSAG, 85 OBFSUSER, 85 obfuscation, 84, 107 Operator drop-down list, 91 Operators, 91 Oracle database schema, configuring, 29 Oracle DBA SQL Plus Worksheet, 29 Oracle DBA Studio, 31 ORIGNAME attribute, 77

Ρ

PACKAGE Class, 59 PACKAGE instance, 61 Packager for Windows Installer, 42 passport registration, 7 Patch Manager, 42 PATH Class, 60 PRIORITY instance attribute, 78 privacy, 84 PRODNAME attribute, 77 PRODVER attribute, 77 put.cfg file, 37, 38

R

RADPIMGR.exe, 41 Reporting Server filtering usage management reports, 88 ROOTCONN attribute, 76 Rule Set Groups tab, 100 Rule Sets tab, 98 Rules tab, 96 rumclient.bat, 118

S

software configurations, 18 state file data, 26 state files, 42

U

UMCOLLCT Class, 20, 59, 72 UMCOLLCT instance, 61 UMCOLLCT object, 39 UMCOLLCT.EXE, 117 UMCONFIG Class, 59 UMCONFIG instance, 61 UMDBASE Class, 59 UMDESTPT Class, 59 UMFLTCRI class, 59, 75 UMFLTCRI Class, 70 UMFLTRUL class, 60 UMFLTRUL Class, 71 UMFLTSET class, 60, 73, 80 **UMFLTSET Class**, 72 UMINVENT instance, 61 UNINVENT class, 60

Usage - Include All Files instance, 74 usage collection files, 59 usage data, 14, 59 initiating a collection, 83 usage database files, 38 USAGE Domain, 39 adding to database, 47 classes, 59 definition, 58 usage files active application monitoring, 19 collection files, 20 history file, 19 usage filtering criteria, 59, 60, 71 usage monitoring data, 22 usage reports, 87 usage.cfg file, 40 configuring, 40 usage_Oracle.cfg, 40 usage_SQL_Server.cfg, 40 usdbcoll.exe, 82 USDBColl.exe, 82, 83 USDBColl.ini, 115 USDBColl.ini file, 104 usdbinvn.exe, 82 USDBInvn.exe, 82

Ζ

ZOBJID, 20 ZSERVICE Class, 59