HP Universal CMDB

for the Windows and Linux operating systems

Software Version: 9.04

Deployment Guide

Document Release Date: September 2011
Software Release Date: September 2011

Legal Notices

- This product includes OpenLDAP code from OpenLDAP Foundation (http://www.openldap.org/foundation/).

- This product includes GNU code from Free Software Foundation, Inc. (http://www.fsf.org/).

- This product includes JiBX code from Dennis M. Sosnoski.

- This product includes the XPP3 XMLPull parser included in the distribution and used throughout JiBX, from Extreme! Lab, Indiana University.

- This product includes the Office Look and Feels License from Robert Futrell (http://sourceforge.net/projects/officelnfs).

- This product includes JEP - Java Expression Parser code from Netaphor Software, Inc. (http://www.netaphor.com/home.asp).

Documentation Updates

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

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

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

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

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

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

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

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

Support

Visit the HP Software Support web site at:

http://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 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 web site to:

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

Most of the support areas require that you register as an HP Passport user and sign in. Many also require a support contract. To register for an HP Passport ID, go to:

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

To find more information about access levels, go to:

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

Table of Contents

Table of Contents

Welcome to This Guide

Welcome to the HP Universal CMDB Deployment Guide. This guide introduces you to HP Universal CMDB, provides information on getting started, describes server installation, server hardening, and details the upgrade process.

This chapter includes:

➤ How This Guide Is Organized on page 15

➤ Who Should Read This Guide on page 16

➤ HP Universal CMDB Online Documentation on page 17

➤ Additional Online Resources on page 20

➤ Documentation Updates on page 21

How This Guide Is Organized

This guide contains the following parts:

Part I   Introduction

Introduces the components that are installed during HP Universal CMDB installation, and provides the installation workflow and deployment choices.

Part II   UCMDB Server Installation

Describes the installation procedure for the HP Universal CMDB server, including database configuration.

Part III   Data Flow Probe Installation

Describes the installation procedure for the Data Flow Probe.

Part IV   Upgrading HP Universal CMDB from Version 8.0x to 9.0x

Explains the procedures for upgrading (migrating) HP Universal CMDB to version 9.04, and for migrating packages from version 8.0x to 9.04.

Part V   High Availability and Capacity Planning

Describes the installation, startup, and configuration procedures so that HP Universal CMDB version 9.04 can be run in a high availability environment.

Part VI   Hardening HP Universal CMDB

Explains the procedures for hardening the HP Universal CMDB Server and the Data Flow Probe.

Part VII   Disaster Recovery

Describes the basic principles and guidelines on how to set up a Disaster Recovery system.

Part VIII   Getting Started With HP Universal CMDB

Includes information on logging in to HP Universal CMDB for the first time immediately following installation, and the Start menu. Also includes information on accessing UCMDB through the IIS Web server.

Who Should Read This Guide

This guide is intended for the following users of HP Universal CMDB:

➤ HP Universal CMDB administrators

➤ HP Universal CMDB platform administrators

➤ HP Universal CMDB application administrators

➤ HP Universal CMDB data management administrators

Readers of this guide should be knowledgeable about enterprise system administration, have familiarity with ITIL concepts, and be knowledgeable about HP Universal CMDB.

HP Universal CMDB Online Documentation

HP Universal CMDB includes the following online documentation:

Readme. Provides a list of version limitations and last-minute updates. From the HP Universal CMDB DVD root directory, double-click **readme.html**. You can also access the most updated readme file from the HP Software Support Web site.

What's New. Provides a list of new features and version highlights. In HP Universal CMDB, select **Help** > **What's New**.

Printer-Friendly Documentation. Choose **Help** > **UCMDB Help**. The following guides are published in PDF format only:

➤ the *HP Universal CMDB Deployment Guide* PDF. Explains the hardware and software requirements needed to set up HP Universal CMDB, how to install or upgrade HP Universal CMDB, how to harden the system, and how to log in to the application.

➤ the *HP Universal CMDB Database Guide* PDF. Explains how to set up the database (MS SQL Server or Oracle) needed by HP Universal CMDB.

➤ the *HP Universal CMDB Discovery and Integration Content Guide* PDF. Explains how to run discovery to discover applications, operating systems, and network components running on your system. Also explains how to discover data on other data repositories through integration.

HP Universal CMDB Online Help includes:

➤ **Modeling Guide**. Enables you to manage the content of your IT Universe model.

➤ **Data Flow Management Guide**. Explains how to integrate HP Universal CMDB with other data repositories and how to set up HP Universal CMDB to discover network components.

➤ **Administration Guide**. Explains how to work with HP Universal CMDB.

➤ **Developer Reference Guide**. For users with an advanced knowledge of HP Universal CMDB. Explains how to define and use adapters and how to use APIs to access data.

Online Help is also available from specific HP Universal CMDB windows by clicking in the window and clicking the **Help** button.

Online books can be viewed and printed using Adobe Reader, which can be downloaded from the Adobe Web site (www.adobe.com).

Topic Types

Within this guide, each subject area is organized into topics. A topic contains a distinct module of information for a subject. The topics are generally classified according to the type of information they contain.

This structure is designed to create easier access to specific information by dividing the documentation into the different types of information you may need at different times.

Three main topic types are in use: **Concepts**, **Tasks**, and **Reference**. The topic types are differentiated visually using icons.

Topic Type	Description	Usage
Concepts	Background, descriptive, or conceptual information.	Learn general information about what a feature does.
Tasks	**Instructional Tasks.** Step-by-step guidance to help you work with the application and accomplish your goals. Some task steps include examples, using sample data. Task steps can be with or without numbering: ➤ **Numbered steps.** Tasks that are performed by following each step in consecutive order. ➤ **Non-numbered steps.** A list of self-contained operations that you can perform in any order.	➤ Learn about the overall workflow of a task. ➤ Follow the steps listed in a numbered task to complete a task. ➤ Perform independent operations by completing steps in a non-numbered task.
	Use-case Scenario Tasks. Examples of how to perform a task for a specific situation.	Learn how a task could be performed in a realistic scenario.

Topic Type	Description	Usage
Reference	**General Reference**. Detailed lists and explanations of reference-oriented material.	Look up a specific piece of reference information relevant to a particular context.
	User Interface Reference. Specialized reference topics that describe a particular user interface in detail. Selecting **Help on this page** from the Help menu in the product generally open the user interface topics.	Look up specific information about what to enter or how to use one or more specific user interface elements, such as a window, dialog box, or wizard.
Troubleshooting and Limitations	**Troubleshooting and Limitations**. Specialized reference topics that describe commonly encountered problems and their solutions, and list limitations of a feature or product area.	Increase your awareness of important issues before working with a feature, or if you encounter usability problems in the software.

Additional Online Resources

Troubleshooting & Knowledge Base accesses the Troubleshooting page on the HP Software Support Web site where you can search the Self-solve knowledge base. Choose **Help** > **Troubleshooting & Knowledge Base**. The URL for this Web site is http://h20230.www2.hp.com/troubleshooting.jsp.

HP Software Support accesses the HP Software Support Web site. This site enables you to browse the Self-solve knowledge base. You can also post to and search user discussion forums, submit support requests, download patches and updated documentation, and more. Choose **Help** > **HP Software Support**. The URL for this Web site is www.hp.com/go/hpsoftwaresupport.

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

To find more information about access levels, go to:

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

To register for an HP Passport user ID, go to:

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

HP Software Web site accesses the HP Software Web site. This site provides you with the most up-to-date information on HP Software products. This includes new software releases, seminars and trade shows, customer support, and more. Choose **Help** > **HP Software Web site**. The URL for this Web site is www.hp.com/go/software.

Documentation Updates

HP Software is continually updating its product documentation with new information.

To check for recent updates, or to verify that you are using the most recent edition of a document, go to the HP Software Product Manuals Web site (http://h20230.www2.hp.com/selfsolve/manuals).

Part I

Introduction

1

Introduction to HP Universal CMDB

This chapter includes:

Concepts

➤ HP Universal CMDB Overview on page 26

➤ HP Universal CMDB on VMware on page 31

➤ Migrating from Previous Versions on page 32

Tasks

➤ Change Memory Allocation for Applets on page 33

Concepts

HP Universal CMDB Overview

This chapter introduces HP Universal CMDB, the main stages of the HP Universal CMDB installation, presents the installation workflow, provides prerequisite hardware, software, and configuration information, and helps you to get started.

This section includes the following topics:

About HP Universal CMDB

HP Universal CMDB consists of a rich business-service-oriented data model with built-in discovery of configuration items (CIs) and configuration item dependencies, visualization and mapping of business services, and tracking of configuration changes.

HP Universal CMDB enables you to manage all the CIs contained in a managed world. A managed world refers to any self-contained environment that can be described using a topology model (defined with HP's Topology Query Language (TQL)). For example, the IT infrastructure of a large business represents a managed world, where the topology comprises multiple layers such as networks, protocols, databases, operating systems, and so on. You manage views to view the information in exactly the format you require.
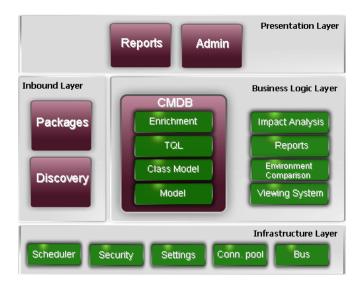
Additionally, the information contained in the results of each TQL is updated automatically with the latest data entering the configuration management database (CMDB). As a result, once a TQL and View have been defined, they continue to provide up-to-date information about the current state of your managed world. Views are displayed in multi-level maps that enable you to identify key CIs, as required. You can also create reports (in HTML, Excel or table format) about information collected by the system.

HP Universal CMDB addresses the following operational and functional needs:

➤ **IT resources and application alignment.** Automatic discovery of IT resources and their interdependencies from a business service perspective.

➤ **Problem resolution.** Understanding the causal relationships between CIs to locate and address the root cause of infrastructure problems and reduce troubleshooting time.

➤ **Asset and change management control.** Automatic detection of infrastructure changes, to enable automatic updating of all the relevant sub-systems.

➤ **Customized state management (performance, change).** Ability to define a CI management state.

➤ **Performance management and capacity planning.**

➤ **Architecture and infrastructure planning.**

➤ **Federation and reconciliation data.** Retrieved from existing repositories and other CMDBs.

HP Universal CMDB System Architecture
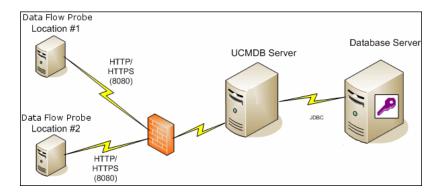
The following diagram provides a graphical overview of the HP Universal CMDB system architecture:

To set up an LDAP authentication method for logging in, see "HP Universal CMDB Login Authentication" on page 389.

HP Universal CMDB Deployment

The following diagram provides a graphical overview of a typical deployment of the HP Universal CMDB system.

The Configuration Management Database (CMDB)

The CMDB is the central repository for the configuration information gathered by HP Universal CMDB and the various third-party applications and tools.

The CMDB contains CIs and relationships that are created automatically from the discovery process or inserted manually. The CIs and relationships together represent a model of the components of the IT world in which your business functions.

The CMDB also stores and handles the infrastructure data collected and updated by Data Flow Management.

The IT model can be very large, containing thousands of CIs. To facilitate the management of these CIs, you work with the CIs in a view that provides a subset of the overall components in the IT world.

You use views (factory views supplied with HP Universal CMDB or defined in the Topology Map) to display and manage the CIs and relationships in the CMDB. The views enable you to focus on specific IT areas.

The CMDB also contains the TQL query definitions that are used to query and retrieve data from the CMDB for presentation in:

➤ pattern views (views based on TQLs)

➤ the configuration item type (CIT) model (a repository for all CI types and relationship definitions)

Note: You can connect to the CMDB from other HP products. For details, refer to the product's installation documentation.

Data Flow Management Mapping

The discovery process is the mechanism that enables you to collect data about your system by discovering the IT infrastructure resources and their interdependencies (relationships). Data Flow can discover such resources as applications, databases, network devices, different types of servers, and so on. Each discovered IT resource is delivered and stored in the configuration management database (CMDB), where it is represented as a managed configuration item (CI).

Topology Query Language (TQL)

TQL is a language and tool for discovering, organizing, and managing IT infrastructure data. TQL is used to create queries that retrieve specific data from the CMDB and display that data.

TQL queries constantly search the CMDB for changes that occur in the state of managed resources, and inform and update the relevant subsystems.

TQL extends the traditional query languages by adding two important capabilities:

➤ TQL enables HP Universal CMDB to draw conceptual relationships between CIs, which represent their actual interdependencies. Using predefined operators, the different types of interconnections that exist between CIs can be established, and consequently the infrastructure design and performance are more accurately represented. This representation serves as a basis and a model for the discovery, arrangement, query, and management of complex infrastructures.

➤ TQL has a graphical aspect, consisting of visual symbols and syntax that represent the resources and their interconnections. This visualization of an IT infrastructure simplifies the understanding, monitoring, and managing of the IT business operations.

Document Conventions

➤ The HP Universal CMDB documentation assumes that the HP Universal CMDB Server and Data Flow Probe are installed in the default location, that is, **C:\hp\UCMDB\UCMDBServer** and **C:\hp\UCMDB\DataFlowProbe**.

➤ Instructions for accessing components of the application always give the path from the left menu—for example, to view the Active Directory Topology query: **Modeling** > **Modeling Studio** > **Resources** > **Root** > **Application** > **Active Directory**.

HP Universal CMDB on VMware

If you are deploying HP Universal CMDB on a VMware platform, the sizing guidelines for a regular installation are not applicable. The following general limitations and recommendations are applicable to a VMware installation:

➤ Performance of HP Universal CMDB on VMware ESX can be expected to be somewhat slower than with a direct installation on a physical server. For Enterprise deployments, you must verify that your server configuration provides proper performance under realistic operational constraints. For deployment requirements, see "Server Hardware Requirements" on page 36.

➤ HP Universal CMDB capacities and performance vary according to the various server resources, such as CPU, memory, and network bandwidth, allocated to HP Universal CMDB components.

➤ ESX Server versions 3.5 to 4.0 should be used.

➤ A Gigabit network card should be used.

➤ It is highly recommended that you do not run a database server containing HP Universal CMDB databases on VMware if the database files reside on a VMware virtual disk.

➤ VMWare is the only virtualization technology supported by HP Universal CMDB for Windows.

The following HP Universal CMDB components are supported on VMware ESX Server versions 3.5 to 4.0:

➤ HP Universal CMDB

➤ Data Flow Probe

Migrating from Previous Versions

For details on upgrading HP Universal CMDB from version 8.0x to 9.04, see "Upgrading HP Universal CMDB from Version 8.0x to 9.04" on page 175.

For details on upgrading HP Universal CMDB from version 7.0x and 7.5x to 8.0x, refer to the version 8.04 documentation.

Tasks

🔧 Change Memory Allocation for Applets

Note: This section is relevant only if you are connecting to the HP Universal CMDB from a client machine using JRE 6u9 or earlier.

To work correctly the HP Universal CMDB applets may require more memory than is allocated by default, especially when you view very large topology maps or use the applet for a long time without restarting the browser.

To change the memory allocation, modify a file on the client machine (on the machine of the user who is using the applet):

1 On Windows machines, open the file: **...\Documents and Settings\ %userprofile%\ApplicationData\Sun\Java\Deployment\ deployment.properties**.

2 Change the line with the latest Java version by adding the text **-XmxYYYm** to the end of it, where **YYY** is the amount of memory (in megabytes) to be allocated to the Java applet. For example:

```
deployment.javapi.jre.6u10.args=-Xmx256m
```

allocates 256 MB of memory to the applet.

The default value (if no **-Xmx** parameter exists) is 64 MB. You can experiment with the values 128 MB and 256 MB. It is recommended that you do not use more than 256 MB. If Java is unable to acquire the specified memory, it fails to load. In this case, set the memory allocation value to a lower value.

You can also make this change by selecting **Start** > **Settings** > **Control Panel**. Double-click the Java icon and click the **Java** tab. Click the **View** button for Runtime settings are used when an applet is executed. Make changes in the Java Runtime Parameters field according to the above instructions.

Note:

➤ Due to a technological limitation, when switching modes (for example, from Admin to Application) or Managers before all applets have been downloaded to the browser, you may encounter a **Fatal Error** error message. In this case, clear the Java cache.

➤ To view the progress of the applet jars download, in the Java Console window, enter **5**.

➤ For details on installing or updating Java on the client machine, see "Updating the Java Configuration" on page 44.

2

HP Universal CMDB Support Matrix

This chapter includes:

Reference

Reference

🔍 Server Hardware Requirements

Computer/processor	**Windows/Linux:**
	To fulfill the CPU requirements, you must have one of the following:
	➤ Intel Dual Core Xeon Processor 2.4 GHz or higher
	➤ AMD Opteron Dual Core Processor 2.4 GHz or higher
	In addition to the above requirements, you must have the following number of CPU Cores, depending on your deployment configuration:
	➤ Small deployment: 1 CPU
	➤ Standard deployment: 4 CPU
	➤ Enterprise deployment: 8 CPUs
	Note: As HP Universal CMDB performance is dependent upon processor speed, to ensure proper HP Universal CMDB performance, it is recommended that you use the fastest possible processor speed.
Memory	**Windows/Linux:**
	➤ Small deployment: 4 GB RAM
	➤ Standard deployment: 8 GB RAM
	➤ Enterprise deployment: 16 GB RAM
Virtual memory/ Memory swap file	**Windows:**
	➤ Small deployment: 6 GB (Supported)
	➤ Standard deployment: 12 GB
	➤ Enterprise deployment: 24 GB
	Linux:
	➤ Small deployment: 4 GB (Supported)
	➤ Standard deployment: 8 GB
	➤ Enterprise deployment: 16 GB
	Note:
	➤ The virtual memory for Windows should be at least 1.5 times the physical memory size.
	➤ The Linux swap file size should be equal to the physical memory size.

Free hard disk space	Minimum 30 GB (for logs, memory dumps, and so on)
Display	**Windows:** Color palette setting of at least 256 colors (recommended: 32,000 colors)

📌 Server Software Requirements

Hardware Platform	OS Type	OS Version and Edition	Supported	Recommended
x86-64	Windows 2003	Enterprise SP2 and R2 SP2, 64-bit	Yes	
x86-64	Windows 2008	Enterprise SP2, R2, and R2 SP1, 64-bit	Yes	Yes
x86-64	Red Hat Linux 5	Enterprise/Advanced, 64-bit	Yes	
Any	SUSE Linux 9, 10, 11	Enterprise	No	
x86	Windows 2000, 2003/2008		No	64-bit required
Sun SPARC	Solaris 8, 9 or 10		No	
Any	Red Hat Linux 3, 4	Enterprise	No	
Itanium 64	Red Hat Linux 5	Enterprise/Advanced	No	

Note:

➤ Unsupported configurations are listed to ensure that there is no ambiguity on the scope of the Support Matrix.

➤ It is recommended that Dr. Watson be enabled and configured in automatic mode (after running Dr. Watson, Drwtsn32.exe, at least once). To set up automatic mode, search for **\\HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\AeDebug** in the Windows Registry and set the value of the Auto parameter to **1**.

➤ Installation of HP Universal CMDB is not supported on 32-bit machines.

🔍 Server Supported Virtual Environments

Virtual Environment	OS Version and Edition	Supported	Recommended
VMware ESX 4.0	➤ Windows 2003 Enterprise SP2 and R2 SP2, 64-bit ➤ Windows 2008 Enterprise SP2, R2, and R2 SP1, 64-bit ➤ Red Hat Linux 5 Enterprise/Advanced, 64-bit	Yes	Yes
VMware ESX version 3.5 or version 3.x	➤ Windows 2003 Enterprise SP2 and R2 SP2, 64-bit ➤ Windows 2008 Enterprise SP2, R2, and R2 SP1, 64-bit ➤ Red Hat Linux 5 Enterprise/Advanced, 64-bit	Yes	Older ESX 3.x versions may not provide adequate performance and may not be supported on all OS versions.
MS Hyper-V Server 2008 v1 and R2	Any	No	
Xen Hypervisor 3.x	Any	No	
ESXi	Any	No	

🔍 Server Database Requirements

This section describes the database servers supported for working with HP Universal CMDB.

This section includes the following topics:

➤ "Oracle System Requirements" on page 39

➤ "Microsoft SQL Server System Requirements" on page 41

Oracle System Requirements

The following table lists the Oracle Servers supported for working with HP Universal CMDB. A supported option means that HP quality assurance personnel have successfully performed basic tests on that option.

(*****) 10.2.0.4 or higher in the 10.2.0.X versions.

Database Version	Standard Edition	Enterprise Edition	RAC Enterprise Edition	System Type
Oracle 10.2*		✔	✔	64-bit
Oracle 11.1.0.7		✔		64-bit
Oracle 11.2 (11g R2)	✔	✔	✔	64-bit

Note:

➤ It is strongly recommended to apply the latest critical Oracle patches per your operating system. For details, consult the Oracle documentation.

➤ Consult the Oracle documentation for supported platforms.

➤ The Standard Edition of Oracle Server is supported by the HP Universal CMDB server when the latter is deployed without the UCMDB Configuration Manager component.

➤ When the HP Universal CMDB server is deployed in combination with the UCMDB Configuration Manager component, the Enterprise Edition of Oracle and the Oracle Partitioning option are required.

➤ If you previously deployed the HP Universal CMDB server with the Standard Edition of Oracle 11.2, and you intend to add the UCMDB Configuration Manager component to your installation, you must first convert your Standard Edition database to an Enterprise Edition database with the Partitioning option enabled.

➤ It is strongly recommended that the UCMDB server(s) be located in the same LAN with the database servers (without a proxy and firewalls between them). Otherwise, your system's performance may be impacted.

➤ If you are using an Oracle version prior to 10.2.0.5, you must apply the Oracle patch that fixes Oracle defect # 5866410. For more details, see the Oracle website for information related to this defect number.

Examples of Tested Deployments

The following table details the deployment environments that have been rigorously tested by HP quality assurance personnel.

Database Release		Operating System
Version	**System Type**	
Oracle 11.2 (11g R2) Enterprise Edition	64-bit	Linux Enterprise Edition RHEL 5
Oracle 11.2 (11g R2) RAC Enterprise Edition	64-bit	Linux Enterprise Edition RHEL 5
Oracle 10.2.0.4 Enterprise Edition	64-bit	Linux Enterprise Edition RHEL 5
Oracle 11.2 (11g R2) Enterprise Edition	64-bit	Solaris 10

Microsoft SQL Server System Requirements

The following table lists the Microsoft SQL Servers supported for working with HP Universal CMDB. A supported option means that HP quality assurance personnel have successfully performed basic tests on that option.

Database Version	Standard Edition	Enterprise Edition	System Type	Service Packs
Microsoft SQL Server 2005		✔	32-bit or 64-bit	SP3 or SP4
Microsoft SQL Server 2008	✔	✔	32 bit or 64-bit	SP1 or SP2

Note:

➤ Only supported service packs should be installed, with latest patches.

➤ Support for SQL Server 2008 Service Pack 1 ends on Oct. 11, 2011 . Future UCMDB service packs will not support SQL server 2008 SP1.

➤ Support for SQL 2005 Service Pack 3 ends on Jan. 10, 2012. Future UCMDB service packs will not support SQL server 2005 SP3.

➤ Consult the Microsoft documentation for supported platforms.

Examples of Tested Deployments

The following table details the deployment environments that have been rigorously tested by HP quality assurance personnel.

Database Release			Operating System
Version	**System Type**	**Service Pack**	
Microsoft SQL Server 2008 Enterprise Edition	32-bit	Service Pack 1	Windows 2008 Enterprise Edition Service Pack 1
Microsoft SQL Server 2008 Enterprise Edition	64-bit	Service Pack 1	Windows 2008 Enterprise Edition Service Pack 1 (64-bit)
Microsoft SQL Server 2008 Enterprise Edition	32 BIT	Service Pack 2	Windows 2008 Enterprise Edition Service Pack 1
Microsoft SQL Server 2008 Enterprise Edition	64 BIT	Service Pack 2	Windows 2008 Enterprise Edition Service Pack 1 (64-bit)

🔍 Client Software Requirements

Screen resolution	Minimal resolution: 1024x768. It is recommended that you use 1280x1024. For wide screens (for example, for 15.4" laptops) the best resolution is 1600x1050.
Java Runtime Environment (for applet viewing)	**1.6 family**: The recommended version is 6u26 and the required version is 6u10 or later. 6u19 is not recommended because on every applet load a pop-up appears with a message that the applet contains a mix of signed and unsigned code.
	Note: The recommended JRE version is 6u26, which is also included on the UCMDB Server itself for local network download.
	To change the locally available JRE:
	1 Place a new JRE deployment executable file in: **C:\hp\UCMDB\UCMDBServer\deploy\ucmdb-ui\static\JRE**
	2 Restart the server.
	For details on working with applets, see "Change Memory Allocation for Applets" on page 33.
	If you are using Microsoft Internet Explorer, you can download the Sun JRE from the Java Web site (**http://java.com/**).
	After installation, verify that the browser is using the correct Java version. Click the **Tools** > **Internet Options** > **Advanced** tab, and select the **Java (Sun)** check box. Click **OK**, then close the browser and reopen it.
Java caching	Enable Java caching on the client machine: **Control Panel** > **Java** > **General tab** > **Temporary Internet Files** > **Settings** > **Keep temporary files on my computer**.
Applet tag support	UCMDB applets support applet tag deployment only.
	To verify that the client machine supports applet tags, open the Java Control Panel. Click the **Advanced** tab and open **Default Java for browsers**. Verify that Microsoft Internet Explorer is selected.
Flash Player (to view charts in reports)	Acrobat Flash 8 or later.

Microsoft Excel (to view exported data)	Versions 2003, 2007, and 2010
Adobe PDF (to view exported data)	Versions 7.0, 8.1, and 9.1

🔍 Client Browser Requirements

Browser	OS Version and Edition	Supported	Recommended
Internet Explorer 7	Windows XP 32/64-bit Windows Vista 32/64-bit Windows 7 32/64-bit Windows 2003 32/64-bit Windows 2008 32/64-bit	Yes	
Internet Explorer 8	Windows XP 32/64-bit Windows Vista 32/64-bit Windows 7 32/64-bit Windows 2003 32/64-bit Windows 2008 32/64-bit	Yes	Yes
Internet Explorer 9	Windows Vista 32-bit with Service Pack 2 (SP 2) or higher Windows Vista 64-bit with Service Pack 2 (SP 2) or higher Windows 7 32-bit RTM or higher Windows 7 64-bit RTM or higher Windows Server 2008 32-bit with Service Pack 2 (SP 2) or higher Windows Server 2008 64-bit with Service Pack 2 (SP 2) or higher Windows Server 2008 R2 64-bit	Yes	
Google Chrome	Windows XP Windows Vista Windows 7	Yes	

Browser	OS Version and Edition	Supported	Recommended
Firefox 3.5, 4, and 5	Windows XP Windows Vista Windows 7 Windows 2003 Linux	Yes	
Safari 4.x	Windows	No	
Internet Explorer 6	Windows	No	

Capacity Planning Requirements

For details, see "HP Universal CMDB Large Capacity Planning" on page 285.

3

Licensing Model for HP Universal CMDB

This chapter includes:

Concepts

Tasks

Reference

Concepts

🎲 Licensing Model – Overview

HP Universal CMDB's licensing model is based on three complementary types of license, or licensing levels. The first one, known as the UCMDB Foundation License, is granted free of charge to eligible customers. The other two levels (the UCMDB Integration Only License and the DDM Advanced Edition License) are fee based.

This section includes the following topics:

➤ "Licensing Levels" on page 48

➤ "Units of Measure" on page 49

Licensing Levels

➤ **UCMDB Foundation License**

This license grants the rights to use UCMDB as the backbone component of select BTO products.

➤ **UCMDB Integration Only License**

This license grants the right to integrate third-party (non-HP) products with UCMDB using various types of integrations.

➤ **DDM Advanced Edition License**

This license grants the rights to:

➤ Use all Discovery and Dependency Mapping (DDM) capabilities to populate UCMDB

➤ Integrate BTO and third-party (non-HP) products with UCMDB, using any type of integration

The following table provides an overview of what is permitted with the various licenses:

License/Integration	Integrations with other BTO products	Integrations with third-party products	Custom Discovery-like integrations	All Discovery capabilities
UCMDB Foundation	Permitted	No	No	No
UCMDB Integration Only	Permitted	Permitted	No	No
DDM Advanced Edition	Permitted	Permitted	Permitted	Permitted

Units of Measure

➤ **OS Instance**

Each implementation of the bootable program that can be installed onto a physical system or a partition within the physical system. A physical system can contain multiple Operating System instances.

➤ **Managed Server**

A computer system or computer system partition where a bootable program is installed, but not including personal computers or computers primarily serving a single individual.

Note: Printers and network devices are not counted as Managed Servers.

☸ UCMDB Foundation License

This is a no charge entitlement license for the UCMDB product, which is automatically granted to any HP customer who purchases HP Discovery and Dependency Mapping (DDM), HP Service Manager (SM), or HP Asset Manager (AM).

This section also includes:

Standard BTO Integrations

With this license, you are entitled to integrate the following BTO products with UCMDB:

➤ HP Business Service Management

➤ HP Universal CMDB

➤ HP Asset Manager

➤ HP Service Manager

➤ HP DDM Inventory

➤ HP Network Node Manager

➤ HP Storage Essentials

➤ HP Systems Insight Manager

Data flows between these products are implemented by means of adapters provided out-of-the-box with HP Universal CMDB or bundled under the SACM solution. Most adapters can leverage the Data Flow Probe infrastructure of HP Universal CMDB - except those supporting a federation data flow or the push data flow from UCMDB to SM, due to a technical restriction.

Note: The data flow from UCMDB to Asset Manager relies on a Connect-It connector, which is licensed free of charge to AM customers.

The right granted by the UCMDB Foundation license to integrate BTO products with UCMDB does not remove the need for customers to properly license these products in the first place.

Other Integrations

With this license, you are also entitled to integrate BTO products with UCMDB using:

➤ Standard integrations provided by HP partners (additional charges may apply)

➤ Custom data exchange integrations (that is, the Generic DB Adapter, the Generic Push Adapter and customer-developed Java adapters)

➤ The HP Universal CMDB Web Service API and the HP Universal CMDB API (Java)

Number of CIs and Relationships

The UCMDB Foundation License does not restrict the number of CIs and relationships that can be stored in UCMDB or exchanged between UCMDB and other BTO products. The only limitation is physical capacity and performance.

Number of UCMDB Instances

The UCMDB Foundation License does not restrict the number of UCMDB instances that can be deployed in a customer environment for the purpose of implementing development, test, production, HA and/or DR platforms. However, technical limitations may apply regarding how data can be managed and exchanged in a multi-instance installation. Servers that are discovered with DDM or sourced from a third-party product only need to be counted once under the DDM Advanced Edition license or the UCMDB Integration Only license, even if they appear in several UCMDB instances for the purpose of operational management.

Number of Data Flow Probe instances

The UCMDB Foundation License does not restrict the number of Data Flow Probe instances that can be deployed in a customer environment for the purpose of hosting discovery or integration adapters. However, technical limitations may apply regarding the maximum number of probes that can be used with UCMDB. Also, as mentioned above, some adapters cannot be hosted by a probe.

Particular Case of BSM

Customers who purchase HP Application Performance Manager (APM) version 9.0x or later are automatically granted a no-charge license to use the embedded UCMDB component labeled as Run-time Service Model (RTSM) and to integrate BTO products with RTSM. As a result, APM customers do not have and do not need a UCMDB Foundation license.

Note: APM was formerly known as HP Business Availability Center version 8.0x (BAC) and RTSM as the Operational Database (ODB).

UCMDB Integration Only License

This license is based on the Managed Server unit of measure (for details, see "Units of Measure" on page 49). An appropriate quantity of that license must be acquired by customers who need to integrate third-party products with UCMDB.

This section also includes:

➤ "Licensing Rule" on page 54

➤ "Valid Types of Integrations" on page 53

Licensing Rule

One License To Use (LTU) must be purchased for each Managed Server that is defined in a third-party product and whose definition then gets copied to UCMDB to be recorded in the form of CIs. The UCMDB Integration Only license requires an initial minimum purchase of 100 LTUs.

Valid Types of Integrations

With this license, you can integrate third-party products with UCMDB using:

➤ Standard integrations provided by HP

➤ Standard integrations provided by HP partners (additional charges may apply)

➤ Custom data exchange integrations (that is, the Generic DB Adapter, the Generic Push Adapter and customer-developed Java adapters)

➤ The HP Universal CMDB Web Service API and the HP Universal CMDB API (Java)

➤ But not Discovery-like integrations (that is, those created using Jython adapters)

Note: HP Universal CMDB provides out-of-the-box adapters for third-party products such as Microsoft SCCM and BMC Atrium CMDB.

DDM Advanced Edition License

This license is based on the OS Instance unit of measure (for details, see "Units of Measure" on page 49). An appropriate quantity of that license must be acquired by customers who need access to all the Discovery and Dependency Mapping capabilities of DDM.

This section also includes:

➤ "Licensing Rule" on page 54

➤ "Discovery and Dependency Mapping" on page 54

➤ "Integrations" on page 55

➤ "DDM Inventory No Charge Entitlement with DDM Advanced Edition" on page 55

Licensing Rule

One License To Use (LTU) must be purchased for each OS Instance that is discovered by DDM and gets recorded in UCMDB in the form of CIs. The DDM Advanced Edition license requires an initial minimum purchase of 100 LTUs.

Example: A VMware ESX Server hosting one virtual machine requires two licenses to use (LTUs).

Servers that are both discovered by DDM and sourced from a third-party product (to collect additional data) do not need to be counted under the UCMDB Integration Only license. The DDM Advanced Edition license covers that usage scenario.

Discovery and Dependency Mapping

With this license, you can use the Discovery Control Panel and other related functions to take advantage of all the discovery content available out of the box. In addition, you can create new Jython adapters to discover other resources.

Integrations

With this license, you can use the Integration Studio to create integration points with BTO and third-party products using Discovery-like integrations (custom Jython adapters).

DDM Inventory No Charge Entitlement with DDM Advanced Edition

For each LTU purchased under the DDM Advanced Edition license for a given server, you are granted a free DDM Inventory license to collect inventory data on the same server.

Tasks

🛠 Upgrade to the Integration Only or DDM Advanced Edition License

When you install HP Universal CMDB, you receive the Universal CMDB Foundation license. To obtain the file needed to upgrade to the Integration Only or DDM Advanced Edition license, contact HP Software Support, then perform the following procedure:

To upgrade your license:

1 Obtain the appropriate file from HP Software Support.

2 Replace the **ucmdb_license.xml** file in the C:\hp\UCMDB\UCMDBServer\conf\ folder. The name of the file must be ucmdb_license.xml.

3 Use the JMX console to force a license change:

   a Launch the Web browser and enter the server address, as follows: **http://<UCMDB Server Host Name or IP>:8080/jmx-console**.

   b When prompted, enter the JMX Console authentication credentials (if you do not have these credentials, contact your system administrator). The default user name and password are **sysadmin**/**sysadmin**.

   c Under **UCMDB**, click **service=Server Services** to open the Operations page.

   d Locate **getLicense** and enter the following information:

   In the Value box for the **customerID** parameter, enter **1**.

   Click **Invoke**.

   Information about the license type, customer name, permitted packages, and whether any applications are blocked is displayed.

Reference

🔍 Troubleshooting and Limitations

This section describes troubleshooting and limitations for UCMDB licensing.

➤ **Problem**: When integrating UCMDB with HP Storage Essentials, unable to run the **SE Integration by SQL** job with the Foundation license.

Solution: Perform the SE Oracle Database discovery described in the *HP Universal CMDB Discovery and Integration Content Guide* PDF.

➤ **Problem**: When integrating UCMDB with HP Network Node Manager (NNMi), unable to run the **Layer2 by NNM** job with the Foundation license.

Solution: For details, see *"Network Node Manager (NNMi) Integration"* in the *HP Universal CMDB Discovery and Integration Content Guide* PDF.

4

Getting Started with HP Universal CMDB

This chapter includes:

Concepts

➤ Predeployment Planning on page 60

Tasks

➤ Get Started on page 63

➤ Basic Administration Tasks on page 64

Concepts

🟦 Predeployment Planning

Deploying HP Universal CMDB in an enterprise network environment is a process that requires resource planning, system architecture design, and a well-planned deployment strategy. The following checklist describes some of the basic issues that should be considered prior to installation. For comprehensive best practices documentation on deployment planning, consult with HP Professional Services.

Use the following checklist to review the basic issues that your organization should consider when planning the HP Universal CMDB deployment.

✔	Step
	Define the goals of the project.
	Define the protocols to be used for Data Flow Management (DFM) and ensure that the protocols are available for use.
	Verify that you have access rights for the protocols to be used for DFM. Ask the system administrator for the user name and password for the relevant protocols.
	Define the speed and utilization of the network subnets to be discovered. You may find that you need to increase timeouts for some of the protocols.
	Verify whether the following applications use the default ports. If they are not using the default ports, check which ports they are using. ➤ FTP ➤ IBM HTTP Server ➤ IIS ➤ Microsoft SQL Server ➤ Oracle Server ➤ SAP ➤ SNMP ➤ Siebel ➤ WebLogic ➤ WebSphere
	Identify the components to be discovered: ➤ Server hardware platform ➤ Server operating system and version ➤ Network device types
	Install the following tools and utilities to help analyze discovery processes: ➤ SNMP tool ➤ WMI tool ➤ LDAP browser ➤ Log file tailer (for example, BareTail for Windows or a UNIX tail utility)

✔	Step
	Define what you want to do with HP Universal CMDB: ➤ System component mapping ➤ Root cause analysis ➤ Impact analysis ➤ Data center relocation/consolidation
	Analyze the IT processes and organizational structure and culture that can affect, or be affected by, the deployment.
	Analyze the organization's goals and identify the key IT-enabled business processes to achieve these goals.
	Identify the target users (those with a vested interest in the business processes), such as executives, LOB managers, application owners, system administrators, and security auditors.
	Align the project with current performance management practices.
	Define the project deliverables, including setting expectations regarding measurements, features, the deployment scope, and maturity levels.
	Identify the appropriate HP Universal CMDB functionality.
	Build a deployment roadmap.
	Define success criteria for the project.
	Decide how often you want to run DFM. For details, see "Discovery Scheduler Dialog Box" in the *HP Universal CMDB Data Flow Management Guide*.

Tasks

🔧 Get Started

This section provides a basic, step-by-step roadmap for getting started with HP Universal CMDB.

 1 Read about where to get help.

Learn about the various sources of assistance, including HP Professional Services and HP Software Support, as well as HP Universal CMDB Documentation. For details, see "Welcome to This Guide" on page 15.

 2 Learn about the HP Universal CMDB components.

Learn about the components that power the HP Universal CMDB system. For details, see "HP Universal CMDB Overview" on page 26.

 3 Plan your HP Universal CMDB deployment.

Create a complete deployment plan prior to installing HP Universal CMDB. Use the Predeployment Planning checklist to assist you. For in-depth deployment planning best practices, consult your HP Professional Services representative. For details, see "Predeployment Planning" on page 60.

 4 Install HP Universal CMDB components.

Install the Server (on a Windows or Linux system) and Data Flow Probe. For details, see Part II, "UCMDB Server Installation."

 5 Log on to HP Universal CMDB.

Launch HP Universal CMDB. For details, see "Accessing HP Universal CMDB" on page 429.

 6 Initiate system administration.

Set up the HP Universal CMDB system. For details, see "Administration" in the *HP Universal CMDB Administration Guide*.

🔧 Basic Administration Tasks

This section provides a checklist for basic administration and configuration tasks. You use this checklist to review the basic administration tasks required to set up the HP Universal CMDB system.

 1 Set up Data Flow Management (DFM).

Licensed DFM users can run the discovery process to identify IT resources in the network infrastructure. For details, see the *HP Universal CMDB Data Flow Management Guide*.

 2 When setting up DFM, request the following from the system administrator:

➤ Operating system credentials

➤ Network protocol credentials

➤ Application credentials

 3 Set up users.

Define permissions for views. Permissions permit or deny users access to views, TQLs, and other components. For details, see "Setting Up and Working with Users" and "Security Manager" in the *HP Universal CMDB Administration Guide*.

 4 Configure recipients of scheduled reports, including method of delivery.

For details, see "Reports" in the *HP Universal CMDB Modeling Guide*.

 5 Manually build your IT universe model by defining configuration items (CIs) and CI relationships in the model.

Divide the model into views that represent logical subsets of the overall model. Add CIs based on discovered network resources or manually define infrastructure components.

For details, see:

➤ "IT Universe Manager" in the *HP Universal CMDB Modeling Guide*

➤ "Modeling Studio" in the *HP Universal CMDB Modeling Guide*

Part II

UCMDB Server Installation

5

Installation Procedure

This chapter includes:

Concepts

➤ Installation Procedure Overview on page 68

➤ Installation Stages on page 68

Concepts

🔷 Installation Procedure Overview

During installation, the following HP Universal CMDB components are installed:

➤ HP Universal CMDB server

➤ Configuration management database (CMDB)

➤ History database

➤ HP Universal CMDB packages

➤ Data Flow Management (DFM) Probe (if a suitable license is present – for details, see "Licensing Model for HP Universal CMDB" on page 47)

Important: HP Universal CMDB must **not** be installed more than once on a server, even if the instances are installed in different folders or are different versions.

🔷 Installation Stages

The installation workflow contains the following main stages:

1 Set up the CMDB and History databases.

You set up HP Universal CMDB either on Microsoft SQL Server or on Oracle Server.

For details, see "Deploying and Maintaining the Microsoft SQL Server Database" and "Deploying and Maintaining the Oracle Server Database" in the *HP Universal CMDB Database Guide* PDF.

2 Obtain the appropriate HP Universal CMDB license.

Place the license on a machine that is accessible from the machine on which you are installing HP Universal CMDB.

For details, see "Licensing Model for HP Universal CMDB" on page 47.

3 Install the HP Universal CMDB Server.

For details, see "HP Universal CMDB Installation on a Windows Platform" on page 71 or "HP Universal CMDB Installation on a Linux Platform" on page 87.

At the end of the Server installation, the installation procedure continues directly to the installation of the databases (CMDB and History). You can create a new database (Microsoft SQL Server) or schema (Oracle Server), or you can connect to an existing database or schema. For details, see "UCMDB Server Configuration" on page 105.

Note: Factory packages are deployed automatically only once on the first Server startup.

---

4 Install the collectors (Data Flow Probes). For details, see "Data Flow Probe Installation on the Windows Platform" on page 135 or "Data Flow Probe Installation on the Linux Platform" on page 157.

5 Set up access permissions for the UCMDB Server and Data Flow Probe.

For details, see Part VI, "Hardening HP Universal CMDB."

6 Set up the UCMDB Server Service authentication permissions.

7 Launch HP Universal CMDB.

For details, see "Access Commands for the UCMDB Server" on page 129.

6

HP Universal CMDB Installation on a Windows Platform

Important: If you are installing a service pack version (such as 9.04), see the release notes for the most updated instructions. Also verify if a Cumulative Update Patch (CUP) is available for the version you are installing. If so, install it after the full installation or upgrade.

This chapter includes:

Concepts

➤ Installation Prerequisites on page 72

Tasks

➤ Install HP Universal CMDB - Full Installation on page 74

➤ Upgrade from UCMDB 9.0x to 9.04 on page 83

➤ Configure the UCMDB Mail Server on page 84

➤ Uninstall HP Universal CMDB on page 85

Concepts

Installation Prerequisites

Note the following prior to installing HP Universal CMDB:

➤ It is highly recommended that you thoroughly read the introduction to this guide before commencing installation. For details, see "Introduction to HP Universal CMDB" on page 25.

➤ Do not install HP Universal CMDB on a drive that is mapped to a network resource.

➤ Due to Web browser limitations, the names of server machines running the HP Universal CMDB server should consist only of alphanumeric characters (a-z, A-Z, 0-9), hyphens (-), and periods (.).

If the names of the machines running the HP Universal CMDB servers contain underscores, it may not be possible to log in to HP Universal CMDB. In this case, you should use the machine's IP address instead of the machine name.

➤ **Important:** HP Universal CMDB must **not** be installed more than once on a server even if the instances are installed in different folders or are different versions.

➤ Database user and password names can contain alphanumeric characters from the database character set as well as the underscore sign. Names must begin with an alphabetic character and should not exceed 30 characters.

➤ The HP Universal CMDB program directory cannot contain non-English characters.

➤ For details on licensing, see "Licensing Model for HP Universal CMDB" on page 47.

➤ For details on troubleshooting login, see "Available Troubleshooting Resources" on page 445.

➤ **Important:** If you are upgrading your current version to 9.04, read the chapter "Upgrading HP Universal CMDB from Version 8.0x to 9.04" on page 175 before uninstalling your current version. In that chapter, the section "Perform Post Upgrade Procedures" on page 182 explains how to avoid losing the adapter configuration files.

➤ Have the following information ready before beginning installation:

   ➤ Information for setting the CMDB and CMDB History database parameters. If you plan to set these databases during server setup, see "UCMDB Server Configuration" on page 105.

   ➤ If you plan to run the UCMDB server on a hardened platform (including using the HTTPS protocol), review the hardening procedures described in Part VI, "Hardening HP Universal CMDB."

   ➤ Administrator's e-mail address. (Optional)

   ➤ SMTP mail server name. (Optional)

   ➤ SMTP sender name. This name appears on alerts sent from UCMDB. (Optional)

Tasks

Install HP Universal CMDB - Full Installation
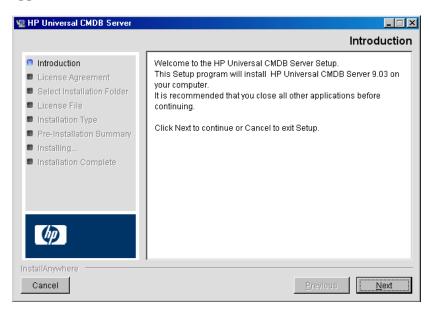
The following procedure explains how to install HP Universal CMDB.

1 If you are installing from a network drive, connect to it.

2 Locate the UCMDB executable file: **HPUCMDB_Server_904.exe**.

3 Double-click the file to open the splash screen.
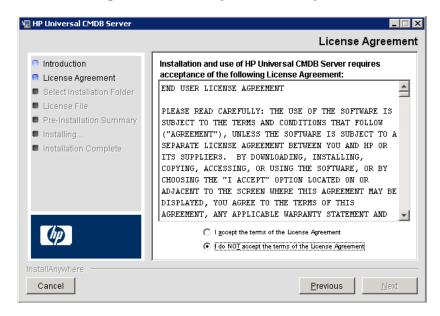
If the digital signature is valid, the splash screen appears:
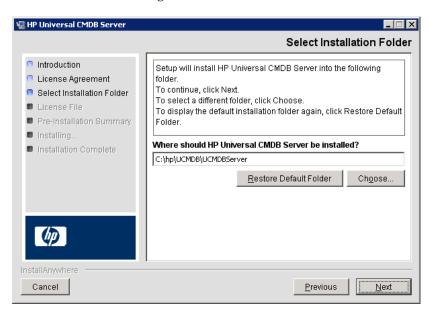
 4 Choose the locale language and click **OK**. The Introduction dialog box
 appears.

 5 Click **Next** to open the License Agreement dialog box.
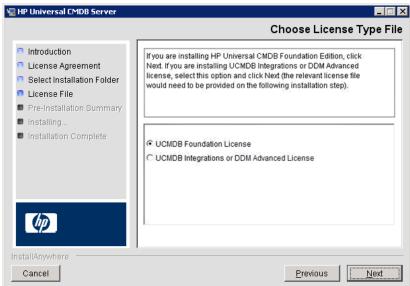
 6 Accept the terms of the license and click **Next** to open the Select
 Installation Folder dialog box.

 Accept the default entry or click **Choose** to display a standard Browse
 dialog box. To install to a different directory, browse to and select the
 installation folder. The installation path should not contain spaces.

 Tip: To display the default installation folder again, click **Restore Default
 Folder**.

 ---

 7 Click **Next** to open the Choose License Type File dialog box.
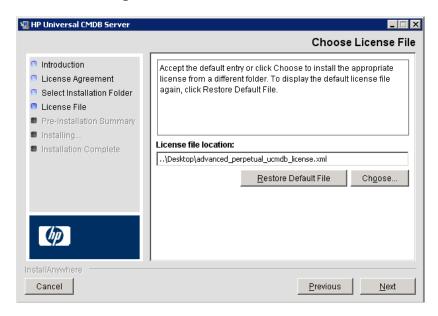
For details on licensing, see "Licensing Model for HP Universal CMDB" on page 47.

➤ To install the UCMDB Foundation License, accept the default entry, and then skip to step 8 on page 79.
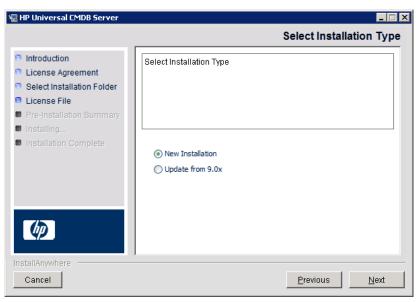
➤ To install the UCMDB Integration Only License or DDM Advanced Edition License, select **UCMDB Integration Only License** or **DDM Advanced Edition License**, and then click **Next** to open the Choose License File dialog box.
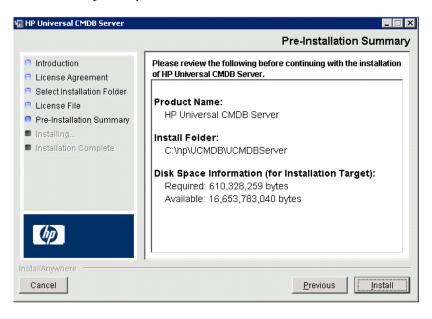
Accept the default entry or click **Choose** to display a standard Browse dialog box. Browse to and select the folder where the license file is located. Select the license file (**ucmdb_license.xml**).

Tip: To display the default installation folder again, click **Restore Default File**.
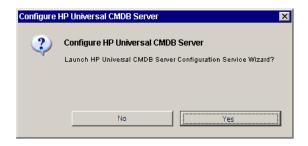
---

 8 Click **Next** to open the Select Installation Type dialog box. Select **New Installation**.

 9 Click **Next** to open the Pre-Installation Summary dialog box that lists the installation options you have selected.

 10 If you are satisfied with the summary, click **Install**. A message is displayed indicating that the installation is currently being performed.

 11 When the installation is complete, the Configure HP Universal CMDB Server message is displayed:
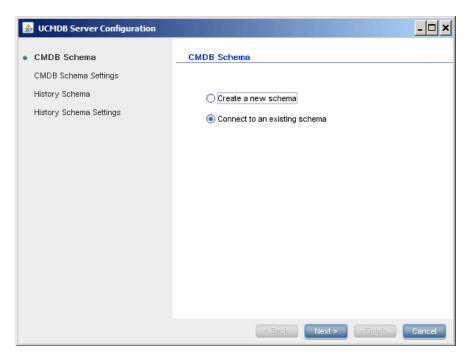
The next stage of the procedure is to launch the UCMDB Server Configuration Wizard (to set up the database or schema). Click **Yes** to continue with the configuration.

If you are performing an upgrade from version 8.0x to 9.04, click **No** and continue with the procedure in "Install the Version 9.04 Data Flow Probe" on page 183.

You can set up the database or schema later. In that case, access the UCMDB Server Configuration wizard from the Windows Start menu.

The UCMDB Server Configuration dialog box appears.

During the following stages, you choose between creating a new database or schema (Microsoft SQL Server or Oracle Server), or connecting to an existing database or schema. You would probably create a new database or schema for a new installation of HP Universal CMDB and would connect to an existing schema or database when reinstalling a server or installing an additional server.

➤ For the introduction to creating or connecting to a database, see "Choosing the Database or Schema" on page 106.

➤ For the procedure for creating a Microsoft SQL Server database, see "Create a Microsoft SQL Server Database" on page 110.

➤ For the procedure for creating an Oracle schema, see "Create an Oracle Schema" on page 116.

➤ For the procedure for connecting to an existing Microsoft SQL Server database, see "Connect to an Existing Microsoft SQL Server Database" on page 120.

➤ For the procedure for connecting to an existing Oracle schema, see "Connect to an Existing Oracle Schema" on page 120.

Note: When connecting to an existing schema, the CMDB schema version and the History schema version must match the server version. If the versions do not match, an error message is displayed and you must re-enter the schema settings.

---

12 After you have finished the configuration in the Configuration wizard, the Installation Complete dialog box appears. Click **Done** to complete the installation.

13 If you are installing a Data Flow probe, see "Install the Data Flow Probe" on page 136.

Note: When you start the server, it may take several minutes for the process to finish and for the server to be up and running. This period of time increases with the size of the DB schema.

Upgrade from UCMDB 9.0x to 9.04

The following procedure explains how to upgrade to HP Universal CMDB 9.04 if you currently have an earlier 9.0x version installed.

 1 Stop the UCMDB 9.0x server before starting the 9.04 installation.

 2 Run the UCMDB 9.04 installer for your operating system. For details, see "Install HP Universal CMDB - Full Installation" on page 74.

 3 On the Select Installation Folder page of the installer, select the existing 9.0x installation folder.

 4 On the Select Installation Type page of the installer, select **Update from 9.0x**.

Note: The wizard checks that you have UCMDB version 9.0x already installed on your machine. If not, the following error message is displayed:

If this error message appears, you must return to the previous step in the wizard and select **New Installation**.

---

 5 Complete the installation process.

 6 The minimum supported Discovery and Integration Content Pack version for UCMDB 9.04 is Content Pack 7.00. If you have an earlier content pack installed, the latest content pack version (Content Pack 9.01) will be automatically installed. If you have Content Pack 7.00 or later installed, you are given the option of upgrading to Content Pack 9.01.

Note: In Content Pack 9.01 all Jython-based integrations have moved from the Discovery Control Panel to the Integration Studio. If one of these integration jobs is active when installing Content Pack 9.01, the adapter does not change to an integration adapter.

---

7 If you imported authorization certificates in the 9.0x version, extract the certificates from the **C:\hp\UCMDB\UCMDBServer\old** folder and import them into the **C:\hp\UCMDB\UCMDBServer\bin\jre\lib\security\cacert** folder. For details, see "Enable SSL on the Client SDK" on page 309.

8 Start up the version 9.04 server. For details on server status, see "HP Universal CMDB Services" on page 126.

Note: You do not need to run the Configuration Wizard, since the system uses the schemas from the previous installation.

Configure the UCMDB Mail Server

Perform this procedure after HP Universal CMDB is installed.

To configure the UCMDB Mail server:

1 Select **Administration** > **Infrastructure Settings** > **Mail Settings**.

2 Define the **SMTP server** setting: enter the name of the SMTP server.

3 Edit the **SMTP server port** setting: the default value is 25.

4 As a backup for the main SMTP server, you can provide information about an alternative server. Repeat steps 2 and 3 but provide the name of the **Alternate SMTP server** and the **Alternate SMTP server port**.

5 Edit the setting for **Email sender** with the name to appear in reports that HP Universal CMDB sends.

6 To enable users to change the **Email sender** name inside the form that sends mail, change the value of **Sender editability** to **True**. Otherwise, leave its value as **False**.

Uninstall HP Universal CMDB

The following procedure explains how to uninstall HP Universal CMDB.

1 From the Start menu, choose **All Programs** > **HP UCMDB** > **Uninstall HP Universal CMDB Server.** The Uninstall HP Universal CMDB Server dialog box appears together with a message giving you the option of either removing the server configuration files or not: Should the installer remove the configuration files also? <root directory>/UCMDBServer/conf directory.

2 Click **Uninstall**.

 3 When uninstall is complete, a confirmation message is displayed. Click
 Done to complete the uninstall process.

7

HP Universal CMDB Installation on a Linux Platform

Important: If you are installing a service pack version (such as 9.04), see the release notes for the most updated instructions. Also verify if a Cumulative Update Patch (CUP) is available for the version you are installing. If so, install it after the full installation or upgrade.

This chapter includes:

Concepts

➤ Installation Prerequisites on page 88

Tasks

➤ Install HP Universal CMDB - Full Installation on page 90

➤ Upgrade from UCMDB 9.0x to 9.04 on page 99

➤ Configure the UCMDB Mail Server on page 100

➤ Uninstall HP Universal CMDB on page 101

Concepts

Installation Prerequisites

Note the following prior to installing HP Universal CMDB:

➤ It is highly recommended that you thoroughly read the introduction to this guide before commencing installation. For details, see "Introduction to HP Universal CMDB" on page 25.

➤ Due to Web browser limitations, the names of server machines running the HP Universal CMDB server should consist only of alphanumeric characters (a-z, A-Z, 0-9), hyphens (-), and periods (.).

If the names of the machines running the HP Universal CMDB servers contain underscores, it may not be possible to log in to HP Universal CMDB. In this case, you should use the machine's IP address instead of the machine name.

➤ **Important:** HP Universal CMDB must **not** be installed more than once on a server even if the instances are installed in different folders or are different versions.

➤ Apply the following configuration to the Linux machine:

  ➤ /etc/sysctl.conf. Add or update the **fs.file-max** value to
  fs.file-max = 300000

  ➤ /etc/security/limits.conf. At the end of the file, add:
  * soft nofile 20480
  * hard nofile 20480

Note: You probably need privileges to modify these files. You may need to restart the Linux machine for the changes to take effect.

➤ Database user and password names can contain alphanumeric characters from the database character set as well as the underscore sign. Names must begin with an alphabetic character and should not exceed 30 characters.

➤ The HP Universal CMDB program directory cannot contain non-English characters.

➤ For details on licensing, see "Licensing Model for HP Universal CMDB" on page 47.

➤ For details on troubleshooting login, see "Available Troubleshooting Resources" on page 445.

➤ Have the following information ready before beginning installation:

   ➤ Information for setting the CMDB and CMDB History database parameters. If you plan to set these databases during server setup, see "UCMDB Server Configuration" on page 105.

   ➤ If you plan to run the UCMDB server on a hardened platform (including using the HTTPS protocol), review the hardening procedures described in Part VI, "Hardening HP Universal CMDB."

Tasks

Install HP Universal CMDB - Full Installation
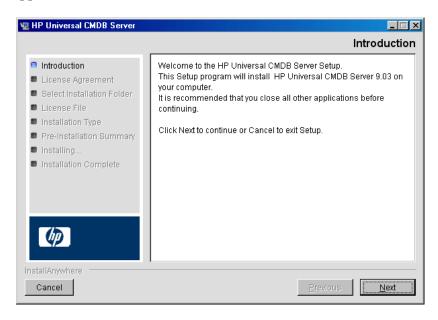
The following procedure explains how to install HP Universal CMDB.

 1 The HP Universal CMDB Linux installation works as a graphic-based installation. Before running the installer, configure the **DISPLAY** environment variable to point to a running instance of an X Windows Server.

 2 Locate the UCMDB executable file: **HPUCMDB_Server_904.bin**.

 3 Run the following executable: **sh <the path to the installation file>/HPUCMDB_Server_904.bin**.
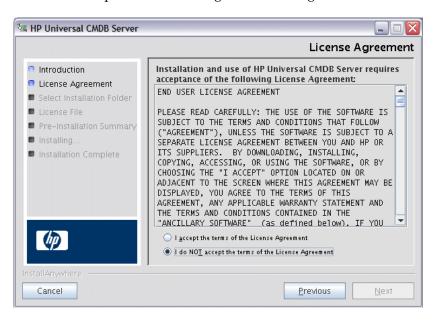
The splash screen appears:

4 Choose the locale language and click **OK**. The Introduction dialog box appears.

5 Click **Next** to open the License Agreement dialog box.
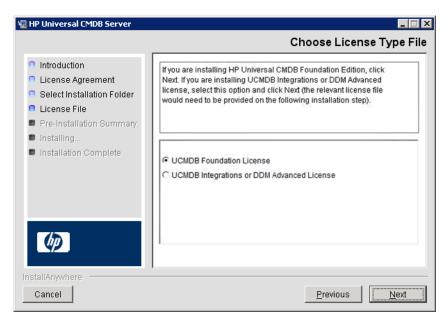
6 Accept the terms of the license and click **Next** to open the Select Installation Folder dialog box.

Enter a different path or click **Choose** to display a standard Browse dialog box. To install to a different directory, browse to and select the installation folder. The installation path should not contain spaces.

Tip: To display the default installation folder again, click **Restore Default Folder.**

---
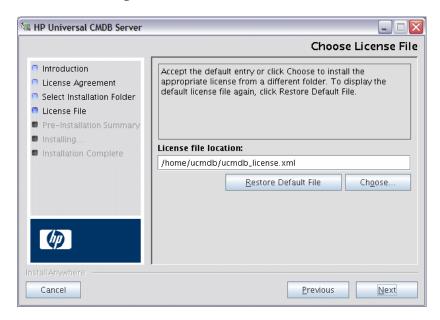
7 Click **Next** to open the Choose License Type File dialog box.
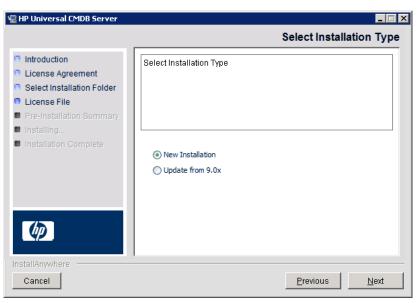
➤ To install the UCMDB Foundation License, accept the default entry, and then skip to step 8 on page 95.

➤ To install the UCMDB Integration Only License or DDM Advanced Edition License, select **UCMDB Integration Only License** or **DDM Advanced Edition License**, and then click **Next** to open the Choose License File dialog box.
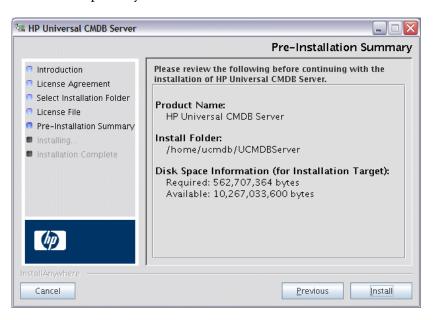
Click **Choose** to display a standard Browse dialog box. Browse to and select the folder where the license file is located. Select the license file (**ucmdb_license.xml**).

8 Click **Next** to open the Select Installation Type dialog box. Select **New Installation**.

9 Click **Next** to open the Pre-Installation Summary dialog box that lists the installation options you have selected.

 10 If you are satisfied with the summary, click **Install**. A message is displayed
   indicating that the installation is currently being performed.

 11 When the installation is complete, the Configure HP Universal CMDB
   Server message is displayed:

 12 Click **Yes** to continue with the configuration and open the Start HP
   Universal CMDB Server Configuration dialog box.
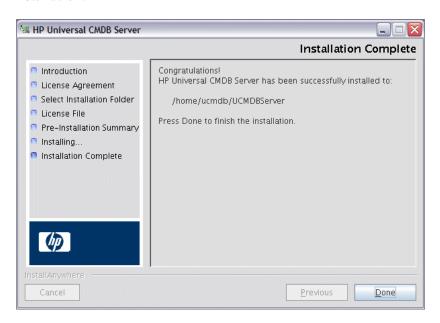
   If you prefer, you can set up the database or schema later. In that case, run
   the **configure.sh** script located in the **bin** subfolder of the installation
   folder.

During the following stages, you choose between creating a new database or schema (Microsoft SQL Server or Oracle Server), or connecting to an existing database or schema. You would probably create a new database or schema for a new installation of HP Universal CMDB and would connect to an existing schema or database when reinstalling a server or installing an additional server. For the introduction to creating or connecting to a database, see "Choosing the Database or Schema" on page 106.

➤ For the procedure for creating a Microsoft SQL Server database, see "Create a Microsoft SQL Server Database" on page 110.

➤ For the procedure for creating an Oracle schema, see "Create an Oracle Schema" on page 116.

➤ For the procedure for connecting to an existing Microsoft SQL Server database, see "Connect to an Existing Microsoft SQL Server Database" on page 120.

➤ For the procedure for connecting to an existing Oracle schema, see "Connect to an Existing Oracle Schema" on page 120.

Note: When connecting to an existing schema, the CMDB schema version and the History schema version much match the server version. If the versions do not match, an error message is displayed and you must re-enter the schema settings.

---

 13 After you have finished the configuration in the Configuration wizard the
   Installation Complete dialog box appears. Click **Done** to complete the
   installation.

 14 If you are installing a Data Flow probe, see "Install the Data Flow Probe"
   on page 158.

Note:

➤ You do not need to run the Configuration Wizard, since the system uses
  the schemas from the previous installation.

➤ When you start the server, it may take several minutes for the process to
  finish and for the server to be up and running. This period of time
  increases with the size of the DB schema.

Upgrade from UCMDB 9.0x to 9.04

The following procedure explains how to upgrade to HP Universal CMDB 9.04 if you currently have an earlier 9.0x version installed.

 1 Stop the UCMDB 9.0x server before starting the 9.04 installation.

 2 Run the UCMDB 9.04 installer for your operating system. For details, see "Install HP Universal CMDB - Full Installation" on page 90.

 3 On the Select Installation Folder page of the installer, select the existing 9.0x installation folder.

 4 On the Select Installation Type page of the installer, select **Update from 9.0x**.

Note: The wizard checks that you have UCMDB version 9.0x already installed on your machine. If not, the following error message is displayed:

If this error message appears, you must return to the previous step in the wizard and select **New Installation**.

---

 5 Complete the installation process.

 6 The minimum supported Discovery and Integration Content Pack version for UCMDB 9.04 is Content Pack 7.00. If you have an earlier content pack installed, the latest content pack version (Content Pack 9.01) will be automatically installed. If you have Content Pack 7.00 or later installed, you are given the option of upgrading to Content Pack 9.01.

7 Start up the version 9.04 server. For details on server status, see "HP Universal CMDB Services" on page 126".

Note: You do not need to run the Configuration Wizard, since the system uses the schemas from the previous installation.
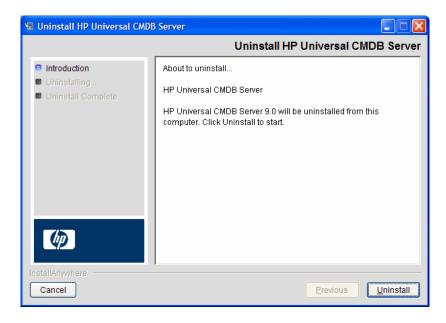

Configure the UCMDB Mail Server

1 Select **Administration** > **Infrastructure Settings** > **Mail Settings**.

2 Define the **SMTP server** setting: enter the name of the SMTP server.

3 Edit the **SMTP server port** setting: the default value is 25.

4 As a backup for the main SMTP server, you can provide information about an alternative server. Repeat steps 2 and 3 but provide the name of the **Alternate SMTP server** and the **Alternate SMTP server name**.

5 Edit the setting for **Email sender** with the name to appear in reports that HP Universal CMDB sends.

6 To enable users to change the **Email sender** name inside the form that sends mail, change the value of **Sender editability** to **TRUE**. Otherwise, leave its value as **FALSE**.

Uninstall HP Universal CMDB
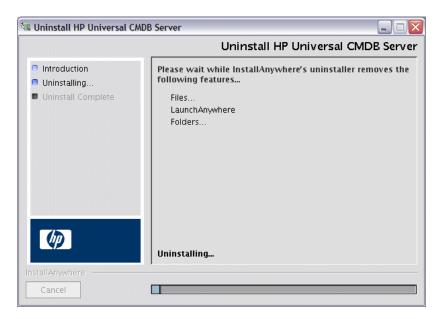
The following provides a procedure for uninstalling UCMDB.
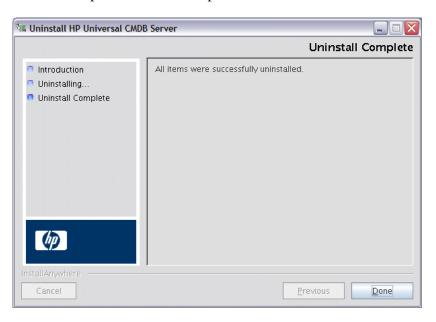
1 Execute the **Uninstall_UCMDBServer** script from the **UninstallerData** subfolder of the Installation folder. The Uninstall HP Universal CMDB Server dialog box appears together with a message giving you the option of either removing the server configuration files or not: Should the installer remove the configuration files also? <root directory>/UCMDBServer/conf directory.

2 From the same location, select **Uninstall** to uninstall the HP Universal CMDB Server.

 3 When uninstall is complete, a confirmation message is displayed. Click
   Done to complete the uninstall process.

8

UCMDB Server Configuration

This chapter includes:

Concepts

➤ Choosing the Database or Schema on page 106

➤ Required Information for Setting Database Parameters on page 107

Tasks

➤ Access the UCMDB Server Configuration Wizard on page 110

➤ Create a Microsoft SQL Server Database on page 110

➤ Create an Oracle Schema on page 116

➤ Connect to an Existing Microsoft SQL Server Database on page 120

➤ Connect to an Existing Oracle Schema on page 120

➤ Restart the Server on page 121

Concepts

Choosing the Database or Schema

This chapter describes the second stage of the installation procedure, which is to launch the UCMDB Server Configuration Wizard (to set up the database or schema). For details on the first stage of the installation, see "HP Universal CMDB Installation on a Windows Platform" on page 71 or "HP Universal CMDB Installation on a Linux Platform" on page 87.

Note: It is highly recommended that you thoroughly read the introduction to this guide before commencing installation. For details, see "Introduction to HP Universal CMDB" on page 25.

During installation, you must decide whether you want to create the database users or use predefined users. HP Universal CMDB enables you to make this choice at the same time as you choose on which database you want to run the application:

Choose to create a database or schema user in the following cases:

➤ There are no existing database users.

➤ There are existing database users, but you want to initialize the database default contents.

Choose to connect to an existing database or schema user in the following cases:

➤ You want to upgrade to a newer version of HP Universal CMDB, and to use the database contents you have from the previous version of HP Universal CMDB.

➤ You do not want to change the database's default contents, for example, because you have data in your database or schema from a previous installation of the same release. In this case, Setup updates the necessary server configuration files with the database details and updates the database scripts configuration file. For details, see the *HP Universal CMDB Database Guide* PDF.

➤ Your database administrator provides instructions for creating the database users in advance according to company policy. To manually create Microsoft SQL Server databases or Oracle schemas, see the *HP Universal CMDB Database Guide* PDF.

Required Information for Setting Database Parameters

Before setting CMDB and CMDB History database parameters, you should prepare the information described in the following sections.

Deploying Microsoft SQL Server

You need the following information for creating new databases and connecting to existing ones:

➤ **Host name.** The name of the machine on which Microsoft SQL Server is installed. If you are connecting to a non-default Microsoft SQL Server instance, enter the following: <host_name>\<instance_name>

➤ **Port.** The Microsoft SQL Server TCP/IP port. HP Universal CMDB automatically displays the default port, **1433**.

➤ **Database (schema) name.** The name of the existing database, or the name that you will give your new database (for example, UCMDB_History).

➤ **User name and Password.** (if you are using Microsoft SQL Server authentication) The user name and password of a user with administrative rights on Microsoft SQL Server. The default Microsoft SQL Server administrator user name is **sa**. Note that a password must be supplied.

You can create and connect to a database using Windows authentication instead of Microsoft SQL Server authentication. To do so, you must ensure that the Windows user running the HP Universal CMDB service has the necessary permissions to access the Microsoft SQL Server database. For information on assigning a Windows user to run the HP Universal CMDB service, see "Change the HP Universal CMDB Server Service User" on page 301. For information on adding a Windows user to Microsoft SQL Server, see "Using Windows Authentication to Access Microsoft SQL Server Databases" in the *HP Universal CMDB Database Guide* PDF.

Deploying Oracle Server

Before setting CMDB and CMDB History database parameters, ensure that you have created at least one default tablespace for each user schema for data persistency purposes, and that at least one temporary tablespace is assigned to each user schema.

You need the following information for both creating a new user schema and connecting to an existing one:

➤ **Host name.** The name of the host machine on which Oracle Server is installed.

➤ **Port.** The Oracle listener port. HP Universal CMDB automatically displays the default port, **1521**.

➤ **SID.** The Oracle instance name that uniquely identifies the Oracle database instance being used by HP Universal CMDB.

➤ **Schema name and schema password.** The name and password of the existing user schema, or the name that you are giving the new user schema (for example, UCMDB_FOUNDATION).

If you are creating a new user schema, you need the following additional information:

➤ **Admin user name and admin password** (to connect as an administrator). The name and password of a user with administrative permissions on Oracle Server (for example, a System user).

➤ **Default tablespace.** The name of the default tablespace you created for the user schema. For details on creating an HP Universal CMDB tablespace, see "Manually Creating the Oracle Server Database Schemas" in the *HP Universal CMDB Database Guide* PDF.

➤ **Temporary tablespace.** The name of the temporary tablespace you assigned to the user schema. The default Oracle temporary tablespace is **temp**.

Note: To create a new user schema, you must have user creation privileges.

Tasks

☝ Access the UCMDB Server Configuration Wizard

If you did not set up the database or schema during installation, you can set it up by accessing the UCMDB Server Configuration Wizard from the Windows Start menu by selecting **Start** > **All Programs** > **HP UCMDB** > **Start HP Universal CMDB Server Configuration Wizard**.

☝ Create a Microsoft SQL Server Database
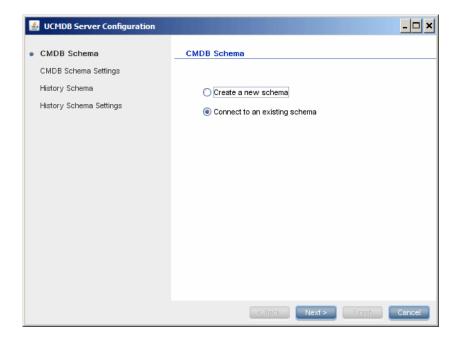
This section explains how to set up the Microsoft SQL Server database. There are two parts to this stage of the installation—setting up the CMDB database and setting up the CMDB History database.

Note: In UCMDB version 9.00 or later, the Foundations and CMDB databases are combined. For upgrade information, see "Upgrading HP Universal CMDB from Version 8.0x to 9.04" on page 175.
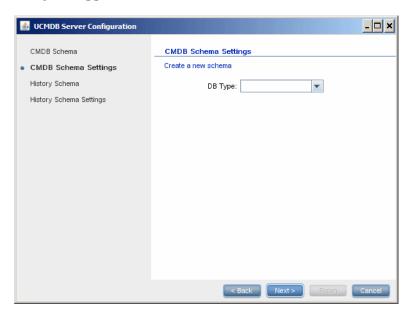
To set up the Microsoft SQL Server database:

1 Following installation, click **Next** to open the CMDB Schema dialog box.
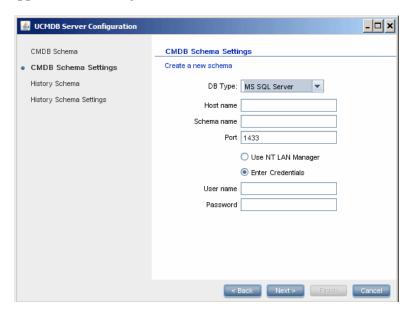
Note: If you have finished installation, you can access the UCMDB Server Configuration wizard from the Windows Start menu. For details, see "Access the UCMDB Server Configuration Wizard" on page 110.

---

2 Select **Create a new schema** and click **Next**. The CMDB Schema Settings dialog box appears.
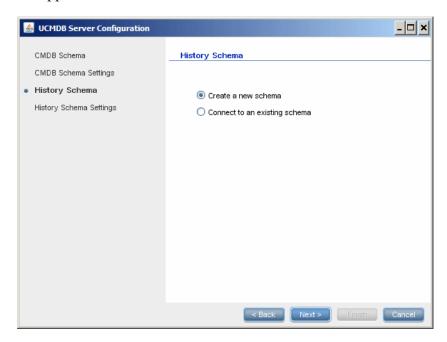
3 In the DB Type list, select **MS SQL Server** and click **Next**. Additional fields appear in the dialog box.
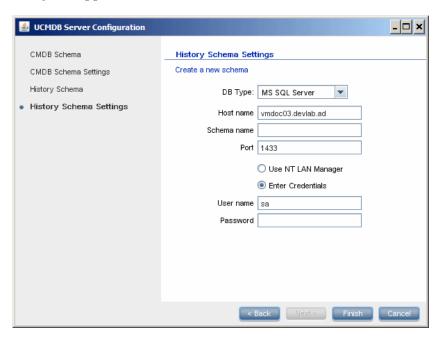
4 Enter the host name and database name, and decide which authentication HP Universal CMDB should use to connect to the database server. For details on Windows authentication, see "Using Windows Authentication to Access Microsoft SQL Server Databases" in the *HP Universal CMDB Database Guide* PDF.

5 Click **Next**. The CMDB database is created. The History Schema dialog box appears.

 6 Select **Create a new schema** and click **Next**. The History Schema Settings
 dialog box appears.
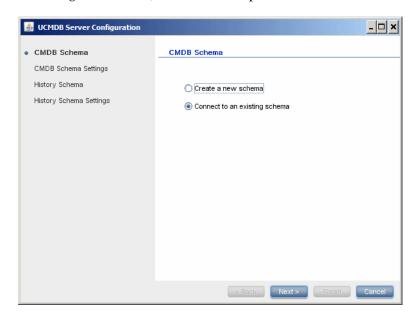
 7 Select **MS SQL Server**. The values you entered for the CMDB settings are
 displayed in the box.

 8 Click **Finish**. The CMDB History database is created.

🖈 Create an Oracle Schema
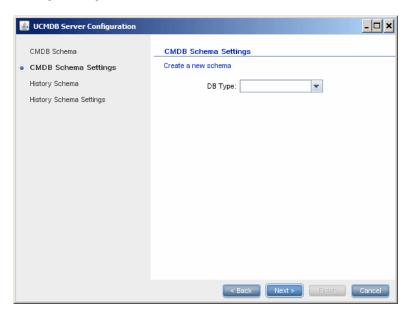
This section explains how to set up the Oracle schema. There are two parts to this stage of the installation—setting up the CMDB schema and setting up the CMDB History schema.

To set up the Oracle schema:
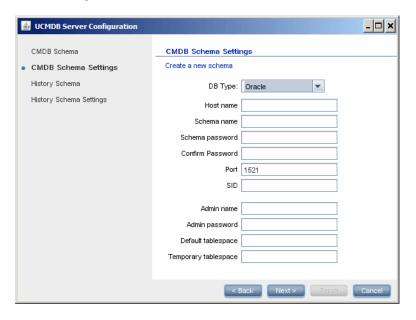
 1 Following installation, click **Next** to open the CMDB Schema dialog box.

2 Select **Create a new schema** and click **Next** to open the CMDB Schema Settings dialog box.
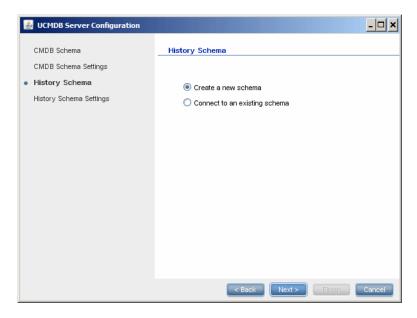
3 In the DB Type list, select **Oracle** and click **Next**. Additional fields appear in the dialog box.
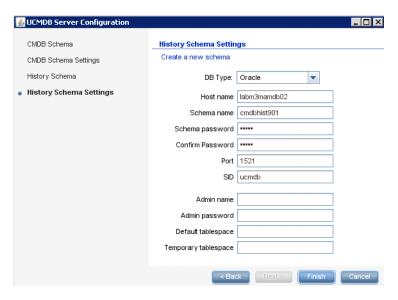
4 Enter the details of the schema:

➤ **Schema name.** The schema name should be unique.

➤ **Default tablespace.** Update this field.

➤ **Temporary tablespace.** If your database administrator created a non-default temporary tablespace, enter that name; otherwise, enter **temp**.

5 Click **Next**. The History Schema dialog box appears.

6 Select **Create a new schema** and click **Next**. The History Schema Settings dialog box appears.

119

    7 Select **Oracle**. The values you entered for the CMDB settings are displayed in the box.

    8 Click **Finish**. The CMDB History database is created.

Connect to an Existing Microsoft SQL Server Database

This section explains how to connect to an existing Microsoft SQL Server database. There are two parts to this stage of the installation—connecting to the CMDB database and connecting to the CMDB History database.

Follow the instructions for creating a Microsoft SQL Server database except for the following steps:

➤ In step 1 on page 111, select **Connect to an existing schema** and click **Next**.

➤ In step 5 on page 114, select **Connect to an existing schema** and click **Next**.

Connect to an Existing Oracle Schema

This section explains how to connect to an existing Oracle Server schema. There are two parts to this stage of the installation—connecting to the CMDB schema and connecting to the CMDB History schema.

Follow the instructions for creating an Oracle Server schema except for the following steps:

➤ In step 1 on page 116, select **Connect to an existing schema** and click **Next**.

➤ In step 5 on page 119, select **Connect to an existing schema** and click **Next**.

ℙ Restart the Server

If you ran the UCMDB Server Configuration Wizard as part of HP Universal CMDB Server installation, you must start HP Universal CMDB on the server only after successfully setting the parameters for all the databases.

If you ran the UCMDB Server Configuration Wizard to modify previously defined database types or connection parameters, restart the HP Universal CMDB Server and the Data Flow Probe after successfully completing the parameter modification process.

9

HP Universal CMDB Services

This chapter includes:

Tasks

➤ View the Status of HP Universal CMDB Server Services on page 124

➤ Start and Stop the HP Universal CMDB Server Service on page 125

Reference

➤ HP Universal CMDB Services on page 126

Troubleshooting and Limitations on page 128

Tasks

🔧 View the Status of HP Universal CMDB Server Services

Select **Start** > **All Programs** > **HP UCMDB** > **HP Universal CMDB Server Status**. The Status and Detailed Status of all services are displayed:

Status

Customer Name	Customer ID	Status
Default Client	1	Up
Test Customer	2	Up
Test 3nd customer	3	Up
New Customer - con	4	Up

Detailed Status

Component	Process	Customer 1	Customer 2	Customer 3	Customer 4
autodiscovery	master	Up	Up	Up	Up
classModel	master	Up	Up	Up	Up
cmdb_mod_not	master	Up	Up	Up	Up
cmdb_sys_tqls	master	Up	Up	Up	Up
cmdb_view	master	Up	Up	Up	Up
configuration	master	Up	Up	Up	Up
content-install	master	Up	Up	Up	Up
correlation	master	Up	Up	Up	Up
data-acquisition	master	Up	Up	Up	Up

The Customer column indicates whether all the HP Universal CMDB services are running (**Up**) or some are down (**Not Started**).

Note: If some services are not running, contact HP Software Support to try and resolve the problem.

🔧 Start and Stop the HP Universal CMDB Server Service

Access the Windows **Services** window and locate the **UCMDB_Server** service. Open the **UCMDB_Server Properties (Local Computer)** dialog box and start the service. If required, change the Startup Type to **Automatic**.

For details on starting and stopping the UCMDB Server, see "Access Commands on the Windows Platform" on page 130 or "Access Commands on the Linux Platform" on page 131.

Reference

🔎 HP Universal CMDB Services

The HP Universal CMDB Server services are described in the following table:

Service Name	Description of Service
autodiscovery	Responsible for Data Flow Management-related services.
classModel	Responsible for maintaining the class model in the CMDB.
cmdb_mod_not	Responsible for notifications of changes that occur in the CMDB.
cmdb_sys_tqls	Responsible for the conditions applied to TQL nodes, and the condition results that are stored in the system TQL.
cmdb_view	Responsible for calculating view definitions over TQL results (the transformation from graph to tree is given the view definition).
configuration	Responsible for snapshots, CI change queries, and TQL/View History queries.
content-install	Responsible for managing the content packs.
data-acquisition	Responsible for managing integrations.
enrichment	Responsible for executing both ad hoc and active enrichments.
fcmdb	Responsible for controlling the adapters, the population and data push flows, data federation, and discovery from one top-level module.
fcmdb-config	A cache mechanism for federated data that allows basic FCMDB services before the FCMDB is fully loaded.
fcmdb-management	Responsible for managing the adapters, federation, and the data push flow.

Service Name	Description of Service
folders	Responsible for managing the folder hierarchy for every type of resource.
framework	Responsible for dispatching operations within the UCMDB server.
grouping	Responsible for holding the different bundles that allow the classification of resources.
historyDB	Responsible for saving changes to CIs and relationships in the CMDB.
impact	Responsible for HP Universal CMDB impact, root cause, and correlation subsystems.
mapping-engine	Used by the integrations. Allows reconciliation during a federated TQL calculation.
model	Responsible for mapping CIs from external data sources to local CMDB CIs.
model_update	Responsible for managing updates to the class model in the CMDB.
packaging	Responsible for packages. Packages are zip files containing resources that are structured in organized, predefined subdirectories.
reconciliation	The CMDB's data population reconciliation service. Responsible for the reconciliation engine of HP Universal CMDB.
report	Responsible for HP Universal CMDB report services, such as adding, editing, and removing System reports, calculation of Asset reports, Node Dependency reports.
scheduler	Responsible for scheduling offline tasks.
security	Responsible for user and authorization management.
state_management	Responsible for managing states.
tql	Responsible for TQL calculations.
tql_res_utils	Responsible for TQL result maintenance (active) and layout retrieval.

Service Name	Description of Service
view	Responsible for part of the business logic of the Modeling Studio, including "watch".
world	A central repository for configuration information that is gathered from the various HP Universal CMDB and third-party applications and tools. This information is used to build HP Universal CMDB views. **Note**: The CMDB service is not necessarily run by the mercury_as process.

🔍 Troubleshooting and Limitations

Problem: UCMDB does not start automatically upon system restart.

Solution:

1 Open the Window **Services** dialog box and select the **UCMDB_Server** service.

2 Open the **UCMDB_Server Properties (Local Computer)** dialog box.

3 In the **General** tab, ensure that:

➤ The **Path to executable** field points to the correct executable location.

➤ The service is configured to automatically start (**Startup type** is **Automatic**).

4 In the **Log On** tab, ensure that:

➤ The service uses the correct user for logon. For details on changing the service user, see "Change the HP Universal CMDB Server Service User" on page 301.

5 In the **Dependencies** tab, ensure that:

➤ The service is configured to have no dependencies (<**No Dependencies**>).

10

Access Commands for the UCMDB Server

This chapter includes:

Tasks

➤ Access Commands on the Windows Platform on page 130

➤ Access Commands on the Linux Platform on page 131

Tasks

℘ Access Commands on the Windows Platform

During the installation of HP Universal CMDB, a start menu is added to the settings of the machine on which you installed UCMDB. You can start and stop the UCMDB Server, access the Database Configuration wizard and view Server service status, and you can uninstall the Server.

Note: For details on starting and stopping the UCMDB Server as a service, see "Start and Stop the HP Universal CMDB Server Service" on page 125.

To access the HP Universal CMDB start menu, select **Start** > **Programs** > **HP UCMDB**. The menu includes the following options:

➤ **Start HP Universal CMDB Server Configuration Wizard.** Enables you to run the wizard to connect to an existing database or schema or to create a new database or schema. For details, see "Choosing the Database or Schema" on page 106.

➤ **Start HP Universal CMDB Server.** Click to start the server service.

➤ **Stop HP Universal CMDB Server.** Click to stop the server service.

➤ **HP Universal CMDB Server Status.** Click to open a Web page with information about the server. For details, see "HP Universal CMDB Services" on page 126. To open a Web page with information about the UCMDB UI Server Status, enter the following URL: **http://<UCMDB Server Host Name or IP>:8080/ucmdb-ui/status.jsp**.

➤ **Uninstall HP Universal CMDB Server.** Click to uninstall the server.

🦴 **Access Commands on the Linux Platform**

Run the following commands to start and stop the UCMDB Server, to access the Database Configuration wizard, Server service status, and to uninstall the Server.

Note:

➤ For details on starting and stopping the UCMDB Server as a service, see "Start and Stop the HP Universal CMDB Server Service" on page 125.

➤ The following commands assume that UCMDB is installed on the default path, that is, **/opt/hp**. If the Server is installed elsewhere, substitute that path for **/opt/hp**.

➤ To start the HP Universal CMDB server:

```
/opt/hp/UCMDB/UCMDBServer/bin/server.sh start
```

➤ To stop the HP Universal CMDB server:

```
/opt/hp/UCMDB/UCMDBServer/bin/server.sh stop
```

➤ To call the HP Universal CMDB Server Configuration wizard:

```
/opt/hp/UCMDB/UCMDBServer/bin/configure.sh
```

➤ To access the UCMDB Server Status Web page, open a browser page and enter the following URL: **http://<UCMDB Server Host Name or IP>:8080/status**. To access the UCMDB UI Server Status Web page, enter the following URL: **http://<UCMDB Server Host Name or IP>:8080/ucmdb-ui/status.jsp.**

Note: You can access the Status pages from any machine and not just from the Linux machine that is hosting the UCMDB Server.

➤ To uninstall the UCMDB Server:

    /opt/hp/UCMDB/UCMDBServer/UninstallerData/Uninstall_UCMDBServer

Part III

Data Flow Probe Installation

11

Data Flow Probe Installation on the Windows Platform

This chapter includes:

Tasks

Reference

Tasks

🔧 Install the Data Flow Probe

The following procedure explains how to install the Data Flow Probe on a Windows platform.

Note: It is highly recommended to thoroughly read "Introduction to HP Universal CMDB" on page 25 before commencing installation. For more information on Data Flow Management, read "Introduction to Data Flow Management" in the *HP Universal CMDB Data Flow Management Guide*.

Note: To deploy a CUP upgrade for a Probe, see "Upgrade the Data Flow Probe from Versions Earlier than 9.03 to 9.04" on page 147.

The Probe can be installed before or after you install the HP Universal CMDB Server. However, during Probe installation, you must provide the Server name, so it is preferable to install the Server before installing the Probe.

Verify that you have enough hard disk space available before beginning installation. For details, see "Data Flow Probe Installation Requirements" on page 153.

For details on licensing, see "Licensing Model for HP Universal CMDB" on page 47.

Important:
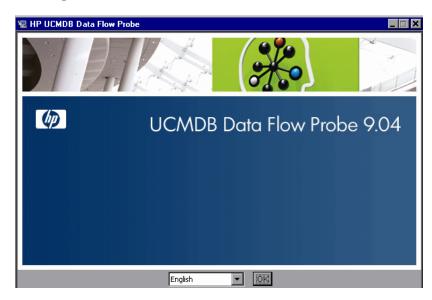
➤ After installing the Probe, we recommend that you disable virus scanning on the main directory that is used to store your MySQL table data. The default directory is **C:\hp\UCMDB\DataFlowProbe\MySQL\data**.

➤ Before installing the Probe on a Windows 2008 machine, a user must have full control permissions on the file system. In addition, after installing the Probe, verify that the user who will run the Probe has full administration permissions on the file system where the Probe is installed.
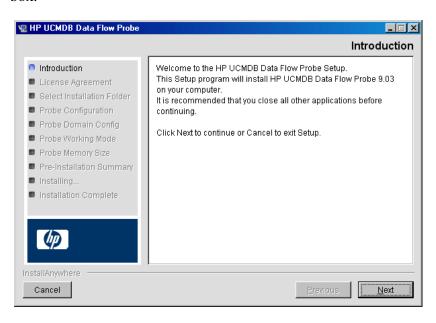
To install the UCMDB Data Flow Probe:

1 Insert the **HP Universal CMDB 9.04 Setup Windows** DVD into the drive from which you are installing the Probe. If you are installing from a network drive, connect to the drive.

2 Double-click the **<DVD root folder>\UCMDB904\ HPUCMDB_DataFlowProbe_904.exe** file.
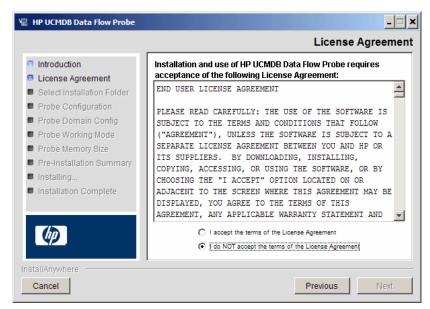
A progress bar is displayed. After the initial process is complete, the splash screen opens.
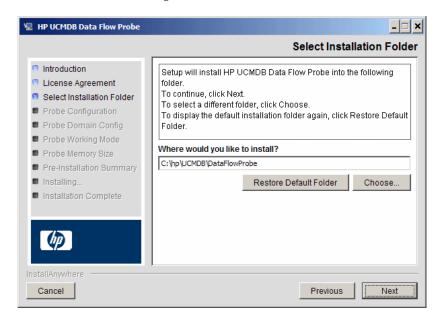
3 Choose the locale language and click **OK** to open the Introduction dialog box.

4 Click **Next** to continue to the License Agreement.
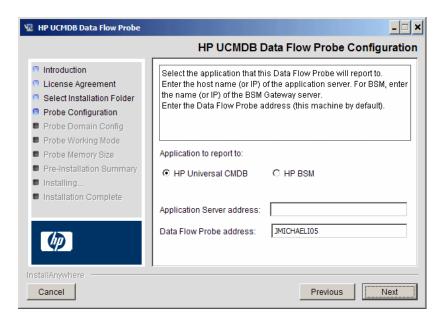
5 Accept the terms of the agreement and click **Next** to open the Select Installation Folder dialog box.

 6 Accept the default entry or click **Choose** to display a standard Browse
   dialog box. To install to a different directory, browse to and select the
   installation folder.

 Note:
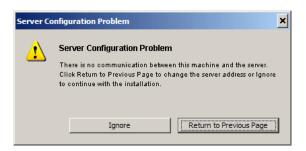
 ➤ The installation folder that you select must be empty.

 ➤ To restore the default installation directory, after selecting a directory
   in the Browse dialog box, click **Restore Default Folder**.

---

 7 Click **Next** to open the HP UCMDB Data Flow Probe Configuration dialog
   box.

➤ **Application to report to.** Choose the application server with which you are working. You can use the Probe with either HP Universal CMDB or Business Service Management.

  ➤ If you select **HP Universal CMDB**, in the **Application Server address** box, enter the name or the IP address of the HP Universal CMDB server to which the Probe is to be connected.

  ➤ If you select HP BSM, in the **Application Server address** box, enter the IP or the DNS name of the Gateway Server.

➤ In the **Data Flow Probe address** box, enter the IP address or the DNS name of the machine on which you are currently installing the Probe, or accept the default.

Note: If the machine has more than one IP address, enter a specific IP address, and not the DNS name.

---

8 If you do not enter the address of the application server, a message is displayed. You can choose to continue to install the Probe without entering the address, or to return to the previous page and add the address.

9 Click **Next** to open the HP UCMDB Data Flow Probe Configuration dialog box.

➤ In the **Data Flow Probe Identifier** box, enter a name for the Probe that is used to identify it in your environment.

Important:
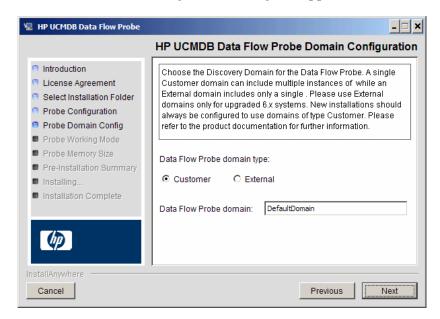
➤ The UCMDB Probe identifier, which is case sensitive, must be unique for each Probe in your deployment.

➤ When installing the Probe in separate mode, that is, the Probe Gateway and Probe Manager are installed on separate machines, you must give the same name (case-sensitive) to the Probe Gateway and all its Managers. This name appears in UCMDB as a single Probe node. Failure to give the same name may prevent jobs from running.

➤ Select **Use Default CMDB Domain** to use the default UCMDB IP address or machine name, as defined in the UCMDB Server installation.

The Default UCMDB Domain is also configurable via Infrastructure Settings, available after installing HP Universal CMDB (**Administration > Infrastructure Settings > Class Model Settings > Default Domain Property Value**).
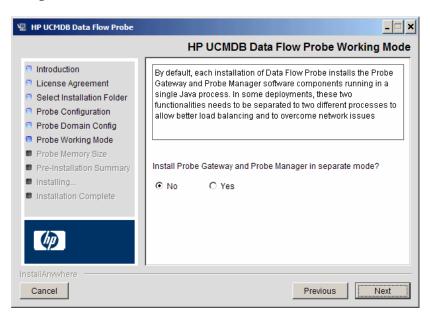
10 Click **Next.** If you cleared the **Use Default CMDB Domain** box in the HP UCMDB Data Flow Probe Configuration dialog box, the HP UCMDB Data Flow Probe Domain Configuration dialog box appears.

➤ **Data Flow Probe domain type**. Choose between **Customer** and **External**, depending on the type of domain on which the Probe is to be running:

  ➤ **Customer.** Select if you are installing one or more Probes in your deployment.

  ➤ **External.** Select if you are upgrading from version 6.x systems.

  Important: For new installations, always select **Customer**.

➤ **Data Flow Probe domain**: If you are not using the default domain defined in UCMDB, enter the name of the domain here.

11 Click **Next** to open the HP UCMDB Data Flow Probe Working Mode dialog box.
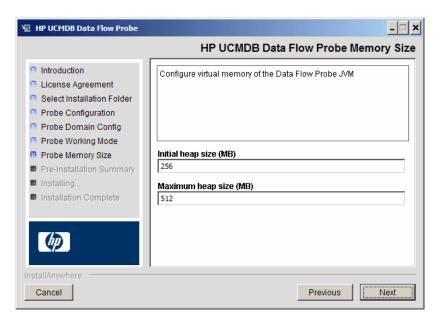
You can run the Probe Gateway and Manager as one Java process or as separate processes. You would probably run them as separate processes in deployments that need better load balancing and to overcome network issues.

Click **No** to run Probe Gateway and Probe Manager as one process.

Click **Yes** to run Probe Gateway and Probe Manager as two processes. For details on the procedure, see "Run Probe Manager and Probe Gateway on Separate Machines" on page 149.

12 Click **Next** to open the HP UCMDB Data Flow Probe Memory Size dialog box.
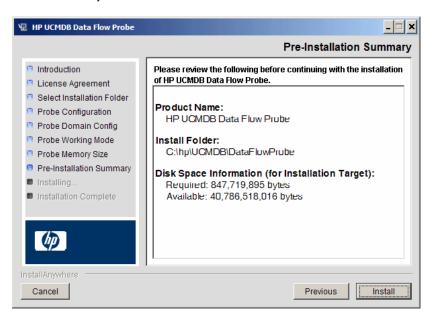
Define the minimum and maximum memory to be allocated to the Probe. The values are measured in megabytes.

Note: To change the maximum heap size value at a later point in time, update the following parameters in the file **WrapperEnv.conf**, located at **C:\hp\UCMDB\DataFlowProbe\bin\WrapperEnv.conf**:

➤ **set.GATEWAY_MAX_MEM**

➤ **set.MANAGER_MAX_MEM**

The maximum heap size allowed in 32-bit JVM is 1536 MB. If the Data Flow probe is installed in separate mode, each parameter will affect the corresponding process.

---

13 Click **Next** to open the Pre-Installation Summary dialog box and review the selections you have made.

14 Click **Install** to complete the installation of the Probe. When the installation is complete the Install Complete page is displayed.

Any errors occurring during installation are written to the following file: **C:\hp\UCMDB\DataFlowProbe\HP_UCMDB_Data_Flow_Probe_Install Log.log**.

15 Click **Done**. The following shortcut is added to the Windows **Start** menu:

All Programs > **HP UCMDB** > **Start Data Flow Probe**

16 Activate the Probe by selecting the shortcut.

You can run the Probe in a console. For details, see "Launch the Probe in a Console" in the *HP Universal CMDB Data Flow Management Guide.*

The Probe is displayed in HP Universal CMDB: access **Data Flow Management** > **Data Flow Probe Setup.** For details see "Data Flow Probe Installation Requirements" on page 153.

Important: HP Software recommends that you disable virus scanning on the main directory that is used to store your MySQL table data. The default directory is **C:\hp\UCMDB\DataFlowProbe\MySQL\data**.

🔧 Upgrade the Data Flow Probe from Versions Earlier than 9.03 to 9.04

This task describes how to upgrade the Data Flow Probe from a version earlier than 9.03 to 9.04.

Note: If you are upgrading from UCMDB 9.03 to 9.04, follow the procedure described in "Upgrade the Probe from Version 9.03 to 9.04" on page 148.

---

1 Uninstall the old Probe

Uninstall all existing Probes. If a Probe is running, stop it before you uninstall it:

Start > **All Programs** > **HP UCMDB** > **Uninstall Data Flow Probe**.

2 Install the new Probe

You should install the new Probe with the same configuration, that is, use the same Probe ID, domain name, and server name as for the previous Probe installation. Remember that the Probe ID is case sensitive.

Note: After performing an upgrade and installing the new Data Flow Probe, all the Discovery jobs that were active before the upgrade are automatically run.

Upgrade the Probe from Version 9.03 to 9.04

Use the following procedure to upgrade the Data Flow Probe when upgrading from UCMDB 9.03 to 9.04:

Note: If an integration is running on the Probe, during the upgrade the integration stops running, and starts over when the Probe is restarted after the upgrade. If an integration is almost finished running, or a significant part has already run, to avoid starting the integration over, we recommend letting it complete its run, and, thereafter, upgrading the Probe.

---

1 Upgrade the UCMDB server to version 9.04. For details, see "Upgrade from UCMDB 9.0x to 9.04" on page 83.

2 Stop the Data Flow Probe.

3 Delete the following folder: **C:\hp\UCMDB\DataFlowProbe\bin\jre**.

4 Create backup versions of the following files:

   ➤ **C:\hp\UCMDB\DataFlowProbe\bin\WrapperGateway.conf**

   ➤ **C:\hp\UCMDB\DataFlowProbe\bin\WrapperManager.conf**

Note: : These files should contain default configurations only and should not be modified. However, if these files were changed as a result of an HP Support request, you need to update the newly created files with the same changes.

---

5 Extract the zip file to the Probe folder: **C:\hp\UCMDB\DataFlowProbe**.

6 Verify that the Probe version is updated to 9.04 in the following file **C:\hp\UCMDB\DataFlowProbe\version.dat**.

7 Start the Probe.

8 In the Data Flow Probe Setup module, verify that the Probe is connected and that the Probe version is updated. For details, see "Details Pane (Probe)" in the *HP Universal CMDB Data Flow Management Guide*.

9 If this process fails, you can uninstall the Probe and reinstall the new one. For details, see "Upgrade the Data Flow Probe from Versions Earlier than 9.03 to 9.04" on page 147.

Probe Version Detection

Beginning in UCMDB 9.04, the Probe reports its version when connecting to the server. The Probe version is displayed in the Details pane of the Data Flow Probe Setup module. If the PROBE version is not compatible with the server version (and there is no supported upgrade) an error is generated and the Probe is forced to shut down.

When you apply a new Cumulative Update Patch (CUP) to the UCMDB 9.04 server, the Probes do not shut down automatically, and are able to report new data to the server. However, this is not recommended. Therefore, when you apply a CUP to the server, you must also apply it to the Probes—either manually or automatically.

🦖 Run Probe Manager and Probe Gateway on Separate Machines

During installation, you can choose to separate the Probe Manager and Probe Gateway processes so that they run on separate machines. You must:

1 Install the Probe on both machines according to the procedure in "Install the Data Flow Probe" on page 136.

2 Choose **Yes** in step 11 on page 144.

3 Perform the configuration in "Configure the Probe Manager and Probe Gateway Components" on page 150.

Note:

➤ At least one Probe Gateway component must be installed. Gateway is connected to the UCMDB Server, receives tasks from the Server, and communicates with the collectors (Probe Manager).

➤ Several Probe Managers can be installed. Managers run jobs and gather information from networks.

➤ The Probe Gateway should contain a list of attached Managers.

➤ The Probe Managers must know to which Gateway they are attached.

🔧 Configure the Probe Manager and Probe Gateway Components

This section explains how to set up the Data Flow Probe when the Probe Manager and Probe Gateway run as separate processes on two machines.

Important: The Probe Manager name in both the probeMgrList.xml and DiscoveryProbe.properties files must be identical. The name is case sensitive.

This section includes the following topics:

➤ "Set Up the Probe Gateway Machine" on page 150
➤ "Set Up the Probe Manager Machine" on page 151
➤ "Start the Services" on page 151

1 Set Up the Probe Gateway Machine

   a Open the following file:

     C:\hp\UCMDB\DataFlowProbe\conf\probeMgrList.xml.

b Locate the line beginning **<probeMgr ip=** and add the Manager machine name or IP address, for example:

```
<probeMgr ip="OLYMPICS08">
```

c Open the following file:

C:\hp\UCMDB\DataFlowProbe\conf\DiscoveryProbe.properties

d Locate the lines beginning **appilog.collectors.local.ip =** and **appilog.collectors.probe.ip =** and enter the Gateway machine name or IP address, for example:

```
appilog.collectors.local.ip = STARS01
appilog.collectors.probe.ip = STARS01
```

2 Set Up the Probe Manager Machine

a In **C:\hp\UCMDB\DataFlowProbe\conf\DiscoveryProbe.properties**, locate the line beginning **appilog.collectors.local.ip =** and enter the Manager machine name or IP address, for example:

```
appilog.collectors.local.ip = OLYMPICS08
```

b Locate the line beginning **appilog.collectors.probe.ip =** and enter the Gateway machine name in uppercase, for example:

```
appilog.collectors.probe.ip = STARS01
```

3 Start the Services

a On the Probe Manager machine, start the Manager service: **Start > All Programs > UCMDB > Start Data Flow Probe Manager**.

b On the Probe Gateway machine, start the Gateway service: **Start > All Programs > HP UCMDB > Start Data Flow Probe Gateway**.

🔨 Connect a Data Flow Probe to a Non-Default Customer

You can connect a Data Flow Probe to a customer that is not the default. The default customer ID is **1**.

1 Open the following file in a text editor:

C:\hp\UCMDB\DataFlowProbe\conf\DiscoveryProbe.properties.

2 Locate the **customerID** entry.

3 Update the value with the customer ID, for example, **customerId = 2**.

4 Restart the Probe so that it is updated with your changes.

Reference

🔍 Data Flow Probe Installation Requirements

This section includes the following topics:

➤ "Hardware Requirements" on page 153

➤ "Software Requirements" on page 153

➤ "Supported Databases" on page 154

➤ "Virtual Environment Requirements" on page 154

Hardware Requirements

Computer/processor	**Windows:** Pentium IV 2.4 GHz or later processor
Memory	**Windows:** Minimum 1 GB RAM (Recommended: 2 GB RAM)
Virtual memory (for Windows deployment)	Minimum 2 GB **Note:** The virtual memory size should always be at least twice the physical memory size.
Free hard disk space	**Windows:** Minimum 4 GB (at least 4 GB for database software and data files) (Recommended: 20 GB hard disk)
Display	**Windows:** Color palette setting of at least 256 colors (32,000 colors recommended)

Software Requirements

Hardware Platform	OS Type	OS Version and Edition	Supported	Recommended
x86	Windows 2008	SP2, Standard/Enterprise editions, 32-bit	Yes	
x86-64	Windows 2008	SP2, Standard/Enterprise editions, 64-bit	Yes	Yes

Hardware Platform	OS Type	OS Version and Edition	Supported	Recommended
x86-64	Windows 2008	R2 and R2 SP1, Standard/Enterprise editions, 64-bit	Yes	
x86	Windows 2003	SP2 and R2 SP2, Standard/Enterprise editions, 32-bit	Yes	
x86-64	Windows 2003	SP2 and R2 SP2, Standard/Enterprise editions, 64-bit	Yes	
	Windows 7	Professional/Enterprise	No	
	Windows 2000		No	

Supported Databases

Database	Version and Edition	Recommended	Comments
MySQL	5.1.46	Yes	This database comes bundled with the Probe installation.

Virtual Environment Requirements

Platform	OS Version and Edition	Supported	Recommended
VMware ESX 3.x	➤ Windows 2003 Standard/Enterprise editions SP2 and R2 SP2, 32/64-bit ➤ Windows 2008 Standard/ Enterprise SP2, 32/64-bit and R2, 64-bit	Yes	
VMware ESX 4.0	➤ Windows 2003 Standard/Enterprise editions SP2 and R2 SP2, 32/64-bit ➤ Windows 2008 Standard/ Enterprise SP2, 32/64-bit and R2, 64-bit	Yes	Yes

Platform	OS Version and Edition	Supported	Recommended
Pre ESX 3.5 (like 3.0.x versions)	➤ May not provide adequate performance ➤ Does not support Windows 2008 or Windows 7	No	
ESXi VMware	All platforms	No	
MS Hyper-V	Server 2008 v1 and R2	No	
Xen Hypervisor 3.x	All platforms	No	

🔍 Troubleshooting and Limitations

Repairing Corrupted Databases

The Data Flow Probe MySQL database may become corrupt without the possibility of recovery, for example, because the machine was shut down but the MySQL service was not stopped.

To repair the corruption:

1 Stop the Probe.

2 Run the **repair_mysql.bat** tool from the following folder: **C:\hp\UCMDB\DataFlowProbe\tools**.

3 Start the Probe.

If this procedure does not fix the corruption, contact HP Software Support.

Probe Downgrade or Rollback

Automatic downgrade or rollback of the probe version is not supported. To perform downgrade or to rollback a version upgrade, uninstall the probe and then install the required version.

Probe Restart

There are several situations where the Probe automatically restarts itself. For example, when deploying a new Content Pack or applying a CUP. In these cases, the Probe waits for 15 minutes to allow the running jobs to finish, and only then shuts down. Jobs that did not finish in that time (for example, long integrations) start running again when the Probe restarts.

12

Data Flow Probe Installation on the Linux Platform

This chapter includes:

Tasks

➤ Install the Data Flow Probe on page 158

➤ Stop the Data Flow Probe on page 167

➤ Upgrade the Probe from UCMDB 9.03 to 9.04 on page 168

➤ Upgrade the Data Flow Probe from Versions Earlier than 9.03 to 9.04 on page 170

➤ Connect a Data Flow Probe to a Non-Default Customer on page 171

Reference

➤ Data Flow Probe Support Requirements on page 172

Troubleshooting and Limitations on page 172

Tasks

🔧 Install the Data Flow Probe

Important:

➤ This Probe is intended for integration use only, and cannot be used for discovery. That is, this Probe does not appear in the Data Flow Setup window.

➤ Only integration with BSM version 9.01 and later is supported on the Probe on Linux.

➤ An instance of Microsoft My SQL database must not be running on the machine on which you are installing the Data Flow Probe. If an instance exists, you must disable it.

➤ To install the Data Flow Probe, you must have root permissions to the Linux machine.

The following procedure explains how to install the Data Flow Probe on a Linux platform.

The Probe can be installed before or after you install the HP Universal CMDB server. However, during Probe installation you must provide the Server name, so it is preferable to install the Server before installing the Probe.

Verify that you have enough hard disk space available before beginning installation. For details, see "Data Flow Probe Support Requirements" on page 172.

For details on licensing, see "Licensing Model for HP Universal CMDB" on page 47.

Important: After installing the Probe, HP Software recommends that you disable virus scanning on the main directory that is used to store your MySQL table data. The default directory is **/opt/hp/UCMDB/DataFlowProbe/MySQL/data**.

To install the UCMDB Data Flow Probe:

1 To run the installation wizard, execute the following command:

sh <path to the installer>/HPUCMDB_DataFlowProbe_904Linux.bin

The following commands are executed:

```
Preparing to install...
Extracting the JRE from the installer archive...
Unpacking the JRE...
Extracting the installation resources from the installer archive...
Configuring the installer for this system's environment...
Launching installer...
```
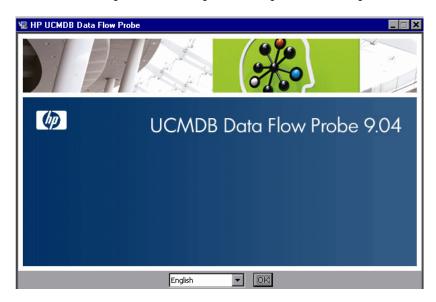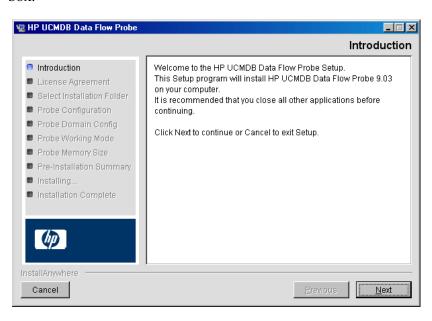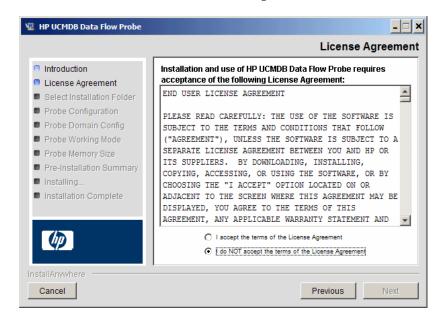
Once the initial process is complete, the splash screen opens.
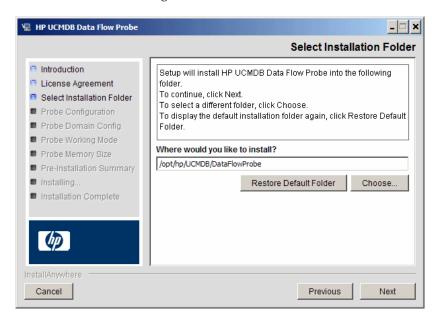
2 Choose the locale language and click **OK** to open the Introduction dialog box.

3 Click **Next** to continue to the License Agreement.

 4 Accept the terms of the agreement and click **Next** to open the Select
Installation Folder dialog box.
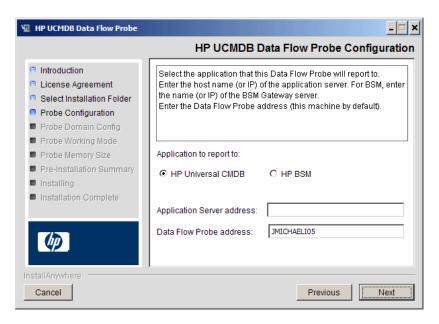
 5 Accept the default entry or click **Choose** to display a standard Browse
dialog box. To install to a different directory, browse to and select the
installation folder.

Note:

➤ You can change the location of the installation, but the directory must
be located under **/opt/**.

➤ To restore the default installation directory, after selecting a directory
in the Browse dialog box, click **Restore Default Folder**.

---

   6 Click **Next** to open the HP UCMDB Data Flow Probe Configuration dialog
   box.

   ➤ **Application to report to.** Choose the application server with which
   you are working. You can use the Probe with either HP Universal
   CMDB or Business Service Management.

      ➤ If you select **HP Universal CMDB**, in the **Application Server address**
      box, enter the name or the IP address of the HP Universal CMDB
      server to which the Probe is to be connected.

      ➤ If you select HP BSM, in the **Application Server address** box, enter
      the IP or the DNS name of the Gateway Server.

   ➤ In the **Data Flow Probe address** box, enter the IP address or the DNS
   name of the machine on which you are currently installing the Probe,
   or accept the default.

   Note: If the machine has more than one IP address, enter a specific IP
   address, and not the DNS name.

 7 If you do not enter the address of the application server, a message is displayed. You can choose to continue to install the Probe without entering the address, or to return to the previous page and add the address.

 8 Click **Next** to open the HP UCMDB Data Flow Probe Configuration dialog box.
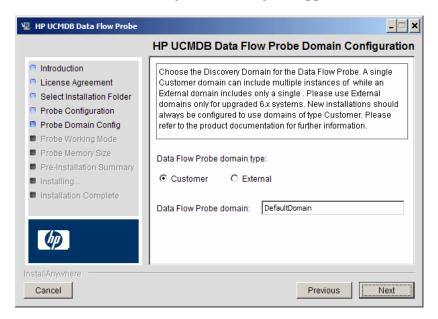
 ➤ In the **Data Flow Probe Identifier** box, enter a name for the Probe that is used to identify it in your environment. This is the name that appears in the Integration Point dialog box. For details, see "New Integration Point/Edit Integration Point Dialog Box" in *HP Universal CMDB Data Flow Management Guide*.

163

Important: The UCMDB Probe identifier, which is case sensitive, must be unique for each Probe in your deployment.

➤ Select **Use Default CMDB Domain** to use the default UCMDB IP address or machine name, as defined in the UCMDB Server installation.

The Default UCMDB Domain is also configurable via Infrastructure Settings, available after installing HP Universal CMDB (**Administration > Infrastructure Settings > Class Model Settings > Default Domain Property Value**).

9 Click **Next.** If you cleared the **Use Default CMDB Domain** box in the HP UCMDB Data Flow Probe Configuration dialog box, the HP UCMDB Data Flow Probe Domain Configuration dialog box appears.

➤ **Data Flow Probe domain type**. Choose between **Customer** and **External**, depending on the type of domain on which the Probe is to be running:

➤ **Customer.** Select if you are installing one or more Probes in your deployment.

➤ **External.** Select if you are upgrading from version 6.x systems.

Important: For new installations, always select **Customer**.

➤ **Data Flow Probe domain**: If you are not using the default domain defined in UCMDB, enter the name of the domain here.

Note: The installation procedure skips the HP UCMDB Data Flow Probe Working Mode dialog box. This is because the Probe Gateway and Probe Manager must be run as one Java process.

---

10 Click **Next** to open the HP UCMDB Data Flow Probe Memory Size dialog box.

Define the minimum and maximum memory to be allocated to the Probe. The values are measured in megabytes.

Note: To change the maximum heap size value at a later point in time, update the following parameters in the file **WrapperEnv.conf**, located at: **/opt/hp/UCMDB/DataFlowProbe/bin/WrapperEnv.conf**:

➤ **set.GATEWAY_MAX_MEM**

➤ **set.MANAGER_MAX_MEM**

The maximum heap size allowed in 32-bit JVM is 1536 MB. If the Data Flow probe is installed in separate mode, each parameter will affect the corresponding process.

11 Click **Next** to open the Pre-Installation Summary dialog box and review the selections you have made.

12 Click **Install** to complete the installation of the Probe. When installation is complete the Install Complete page is displayed.

Any errors occurring during installation are written to the following file: **/opt/hp/UCMDB/DataFlowProbe/HP_UCMDB_Data_Flow_Probe_ InstallLog.log**. If you installed the Probe to another directory under **/opt/**, the log file is located there.

13 Click **Done**.

14 Activate the Probe by executing the following command: **/opt/hp/UCMDB/DataFlowProbe/bin/ProbeGateway.sh start**

To activate the Probe in a console, execute the following command: **/opt/hp/UCMDB/DataFlowProbe/bin/ProbeGateway.sh console**

The installed Probe is displayed in the New Integration Point dialog box, in the list of Probes. For details, see "New Integration Point/Edit Integration Point Dialog Box" in *HP Universal CMDB Data Flow Management Guide*.

Note: The user running the Probe service must be a member of the Administrators group.

🪶 Stop the Data Flow Probe

To stop the Probe server, execute the following command:

/opt/hp/UCMDB/DataFlowProbe/bin/ProbeGateway.sh stop

Upgrade the Probe from UCMDB 9.03 to 9.04

Use the following procedure to updgrade the Data Flow probe when upgrading from UCMDB 9.03 to 9.04:

Note: If an integration is running on the Probe, during the upgrade the integration stops running, and starts over when the Probe is restarted after the upgrade. If an integration is almost finished running, or a significant part has already run, to avoid starting the integration over, we recommend letting it complete its run, and, thereafter, upgrading the Probe.

---

1 Upgrade the UCMDB server to version 9.04. For details, see "Upgrade from UCMDB 9.0x to 9.04" on page 83.

2 Stop the Data Flow probe.

3 Delete the following folder: **/opt/hp/UCMDB/DataFlowProbe/bin/jre**.

4 Create backup versions of the following files:

  ➤ **/opt/hp/UCMDB/DataFlowProbe/bin/WrapperGateway.conf**

  ➤ **/opt/hp/UCMDB/DataFlowProbe/bin/WrapperManager.conf**

Note: : These files should contain default configurations only and should not be modified. However, if these files were changed as a result of an HP Support request, you need to update the newly created files with the same changes.

---

5 Extract the zip file to the probe folder: **/opt/hp/UCMDB/DataFlowProbe**.

6 Verify that the probe version is updated to 9.04 in the following file: **/opt/hp/UCMDB/DataFlowProbe/version.dat**.

7 Start the probe.

8 If this process fails, you can uninstall the probe and reinstall the new one. For details, see "Upgrade the Data Flow Probe from Versions Earlier than 9.03 to 9.04" on page 170.

⚒ Upgrade the Data Flow Probe from Versions Earlier than 9.03 to 9.04

This task describes how to upgrade the Data Flow Probe from a version earlier than 9.03 to 9.04.

Note: If you are upgrading from UCMDB 9.03 to 9.04, follow the procedure described in "Upgrade the Probe from UCMDB 9.03 to 9.04" on page 168.

---

1 Uninstall the old Probe

Uninstall all existing Probes. If a Probe is running, stop it before you uninstall it. For details, see "Stop the Data Flow Probe" on page 167.

Either:

➤ In shell, execute:

    sh /opt/hp/UCMDB/DataFlowProbe/UninstallerData/Uninstall_Discovery_Probe

Or:

➤ Double-click on the Uninstall_Discovery_Probe file in the file system.

2 Install the new Probe

You should install the new Probe with the same configuration, that is, use the same Probe ID, domain name, and server name as for the previous Probe installation. Remember that the Probe ID is case sensitive.

Note: After performing an upgrade and installing the new Data Flow probe, all the Discovery jobs that were active before the upgrade are automatically run.

🔧 Connect a Data Flow Probe to a Non-Default Customer

You can connect a Data Flow Probe to a customer that is not the default. The default customer ID is **1**.

1 Open the following file in a text editor:

../DataFlowProbe/conf/DiscoveryProbe.properties.

2 Locate the **customerID** entry.

3 Update the value with the customer ID, for example, **customerId = 2**.

4 Restart the Probe so that it is updated with your changes.

Reference

🔖 Data Flow Probe Support Requirements

For details on minimum requirements, see "HP Universal CMDB Support Matrix" on page 35.

🔍 Troubleshooting and Limitations

The Data Flow Probe MySQL database may become corrupt without the possibility of recovery, for example, because the machine was shut down but the MySQL service was not stopped.

To repair the corruption:

1 Stop the Probe.

2 Run the **repair_mysql.sh** tool from the following folder: **/opt/hp/UCMDB/DataFlowProbe/tools**.

3 Start the Probe.

If this procedure does not fix the corruption, contact HP Software Support.

Probe Downgrade or Rollback

Automatic downgrade or rollback of the probe version is not supported. To perform downgrade or to rollback a version upgrade, uninstall the probe and then install the required version.

Probe Restart

There are several situations where the Probe automatically restarts itself. For example, when deploying a new Content Pack or applying a CUP. In these cases, the Probe waits for 15 minutes to allow the running jobs to finish, and only then shuts down. Jobs that did not finish in that time (for example, long integrations) start running again when the Probe restarts.

Part IV

Upgrading HP Universal CMDB from Version 8.0x to 9.0x

13

Upgrading HP Universal CMDB from Version 8.0x to 9.04

Important:

➤ If you are installing a service pack version (such as 9.04), see the release notes for the most updated instructions.

➤ It is highly recommended that you read this chapter thoroughly before commencing the upgrade procedure.

This chapter includes:

Concepts

➤ Upgrade Overview on page 176

Tasks

➤ Upgrade HP Universal CMDB Summary on page 177

➤ Upgrade to UCMDB 9.04 on page 184

➤ Terminate the Upgrade Procedure on page 191

Reference

Troubleshooting and Limitations on page 192

Concepts

⬥ Upgrade Overview

This chapter explains how to upgrade HP Universal CMDB (UCMDB) from version 8.0x to version 9.04.

The upgrade process runs offline, during which time all resources and data are transformed from the 8.0x class model to the BDM (BTO Data Model). For details on the data model, see "UCMDB Data Model Introduction" in the *HP Universal CMDB Modeling Guide*.

You can upgrade resources only or perform a full upgrade:

➤ **Resources Only upgrade**. Settings, resources, and the class model are upgraded. All CIs are deleted, as are history events, so the data must be rediscovered.

➤ **Full upgrade**. Upgrades the data and history as well as all resources.

Tasks

🛠 Upgrade HP Universal CMDB Summary

This section lists the steps necessary for the upgrade process.

Note: If you plan to run the UCMDB server on a hardened platform (including using the HTTPS protocol), review the hardening procedures described in Part VI, "Hardening HP Universal CMDB."

This task includes the following steps:

➤ "Prerequisites" on page 178

➤ "Check the Hardware and Operating System Requirements" on page 178

➤ "Prepare the Databases" on page 178

➤ "Save Modified Integration (Federation) Adapters" on page 179

➤ "Save the Encryption Key" on page 179

➤ "Uninstall Previous UCMDB Versions" on page 180

➤ "Uninstall Previous Probes" on page 180

➤ "Install UCMDB Version 9.04" on page 181

➤ "Copy the Encryption Key" on page 181

➤ "Run the Upgrade Tool" on page 181

➤ "Perform Post Upgrade Procedures" on page 182

➤ "Install the Version 9.04 Data Flow Probe" on page 183

1 Prerequisites

➤ If you have any version of HP Universal CMDB 8.0x, you must upgrade to Discovery and Integration Content Pack 8.00 before upgrading to version 9.04.

➤ If you have any version of HP Universal CMDB earlier than 8.04, upgrade to version 8.04 or later. If you are upgrading, HP Software recommends upgrading to the latest 8.0x version.

➤ If you have Discovery and Integration Content Pack 7.00 or earlier, you must install Content Pack 8.00. This step must be performed after upgrading to version 8.04 or later.

➤ When working with Microsoft SQL Server, the CMDB collation and the SQL Server collation must be the same for the upgrade to run properly.

Note: When upgrading from UCMDB 8.0x to 9.04, the highest Content Pack version you can run is version 8.00. You cannot install Content Pack 9.01 with the upgrade. However, after upgrading UCMDB, you can upgrade the Content Pack version separately.

2 Check the Hardware and Operating System Requirements

For details, see "HP Universal CMDB Support Matrix" on page 35.

3 Prepare the Databases

➤ The upgrade requires approximately 250% of the space normally required for the CMDB schema. Make sure you allocate this space.

➤ Back up the version 8.0x CMDB, History, and Foundation schemas. In UCMDB 9.04, the Foundation and CMDB schemas are combined. Backup all three schemas individually to ensure the correct binding during the version 9.04 upgrade.

Important: As an added precaution, run your current UCMDB version against the backup schemas to verify that they are not corrupt.

For details on working with the CMDB, see the *HP Universal CMDB Database Guide* PDF.

4 Save Modified Integration (Federation) Adapters

For all out-of-the-box adapters: If you modified an adapter configuration in version 8.0x, it is highly recommended that you save all adapter files from that version, and redo the modifications on the adapter files of version 9.04.

For all non out-of-the-box adapters: You must redeploy the adapters in version 9.04. For details, see "Package Manager" in the *HP Universal CMDB Administration Guide*.

Important: All adapters must be compatible with the new BDM model. If you made changes to existing out-of-the-box adapters, you must make the same changes to the adapter files in the 9.00 version. That is, do not copy files from version 8.0x and overwrite the files in version 9.00.

5 Save the Encryption Key

Copy the encryption key from the UCMDB 8.0x server located at following path:
C:\hp\UCMDB\UCMDBServer\root\lib\server\discovery\key.bin

UCMDB uses the encryption key to encrypt credentials information and to send sensitive credentials information to probes. This encryption key is not stored in the database, but on the file system due to security reasons.

6 Uninstall Previous UCMDB Versions

Perform the following procedure **only if you intend to install your UCMDB version 9.04 Server on the same machine where you previously ran version 8.0x**. If you are using two or more servers, you do not need to uninstall 8.0x before upgrading to 9.04 and you can skip to the next step ("Uninstall Previous Probes" on page 180); however, you must stop the 8.0x instance before installing version 9.04.

Note: If version 7.x is installed, upgrade from that version to the latest 8.0x version, then continue with the procedures in this chapter. For details on upgrading to 8.0x, refer to the version 8.0x documentation.

To remove the UCMDB 8.0x Server:

a Stop the UCMDB Server: **Start** > **All Programs** > **HP UCMDB** > **Stop HP Universal CMDB Server.**

b Uninstall the Server: **Start** > **All Programs** > **HP UCMDB** > **Uninstall HP Universal CMDB Server**. For details, see "Uninstall HP Universal CMDB" on page 85.

c Remove the entire **C:\hp\UCMDB** folder from the UCMDB Server machine.

d Restart the UCMDB Server machine.

7 Uninstall Previous Probes

The minimum requirement for the upgrade to UCMDB 9.04 is UCMDB version 8.04 or later on which Discovery and Integration Content Pack 8.00 is installed.

Stop and uninstall the DFM (or Data Flow) Probes. For details, see "Upgrade the Data Flow Probe from Versions Earlier than 9.03 to 9.04" on page 147 (Windows) or "Upgrade the Data Flow Probe from Versions Earlier than 9.03 to 9.04" on page 170 (Linux).

8 Install UCMDB Version 9.04

Note: If you are upgrading a high availability environment, ensure that you perform the steps described in "Note:" on page 278.

For details, refer to "HP Universal CMDB Installation on a Windows Platform" on page 71 or "HP Universal CMDB Installation on a Linux Platform" on page 87.

Important: Do **not** set up the database or schema. Following completion of the installation, do not continue with the UCMDB Server Configuration Wizard (to set up the database or schema). Click **No** at step 12 on page 82. Instead, continue to the next step in this procedure.

9 Copy the Encryption Key

Replace the **C:\hp\UCMDB\UCMDBServer\conf\discovery\key.bin** file with the file you copied in step 5 on page 179.

10 Run the Upgrade Tool

You can perform a full upgrade or you can upgrade resources only. For details, see "Upgrade Overview" on page 176.

For details on running the upgrade, see "Upgrade to UCMDB 9.04" on page 184.

For details on failure implications and log messages, see "Upgrade Process: Technical Descriptions" on page 195.

11 **Perform Post Upgrade Procedures**

The following steps may be necessary after the upgrade.

➤ **Reverse Proxy**. Unless the upgraded system is going to run the same environment as the version 8.0x system, reconfigure the reverse proxy after the upgrade. For configuration details, see "Using a Reverse Proxy" on page 317.

➤ **SSL**. Reinstall SSL configurations. For details, see "Enabling Secure Sockets Layer (SSL) Communication" on page 303.

➤ **LW-SSO**. Reinstall LW-SSO. For details, see "Lightweight Single Sign-On Authentication (LW-SSO) – General Reference" on page 379 and "Enable Login to HP Universal CMDB with LW-SSO" on page 395.

➤ **LDAP**. Reinstall the LDAP configuration and mapping between LDAP users and groups. For details, see "Synchronize HP Universal CMDB User Roles With LDAP Groups" in the *HP Universal CMDB Administration Guide*.

➤ **JMX Console**. The default administrator's user and password are **sysadmin**. For details on hardening the JMX Console, see "Change System User Name or Password for the JMX Console" on page 300.

➤ **Delete Foundation Schema**. The Foundation schema is no longer used after the upgrade and can be deleted.

➤ **Redo modifications on integration (federation) adapters**. All adapters must be compatible with the new BDM model. If you made changes to existing out-of-the-box adapters, you must make the same changes to the adapter files in the 9.04 version. That is, do not copy files from version 8.0x and overwrite the files in version 9.04. For all non-out-of-the-box adapters, you must redeploy the adapters. For details, see "Package Manager" in the *HP Universal CMDB Administration Guide*.

➤ **Enable Aging**. After the upgrade, aging is disabled. This is to prevent CIs being deleted because of the time during which the Probe is not collecting data (between the running of the upgrade process and until discovery starts reporting all CIs).

Therefore, it is recommended to wait until the system has stabilized before re-enabling aging. To verify this, run discovery and monitor all CIs that are marked for deletion.

For details on aging, see "CI Lifecycle and the Aging Mechanism" in the *HP Universal CMDB Administration Guide*.

For details on running discovery, see "Discovery Control Panel – Advanced Mode Workflow" in the *HP Universal CMDB Data Flow Management Guide*.

12 Install the Version 9.04 Data Flow Probe

Install Data Flow Probe version 9.04. For the location of the **HPUCMDB_DataFlowProbe_904.exe** file, see "Data Flow Probe Installation on the Windows Platform" on page 135 or "Data Flow Probe Installation on the Linux Platform" on page 157.

The probe must be updated with the new encryption key, as described in "Update an Encryption Key on a Probe" on page 351.

Important: You must give the probe the same name as the old, uninstalled, probe. Remember that the name is case sensitive.

Note: After performing an upgrade and installing the new Data Flow probe, all the Discovery jobs that were active before the upgrade are automatically run.
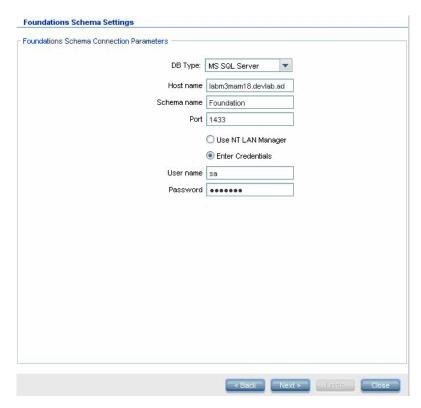
�upgrade **Upgrade to UCMDB 9.04**

This section explains how to upgrade data from UCMDB version 8.04 or later to version 9.04.
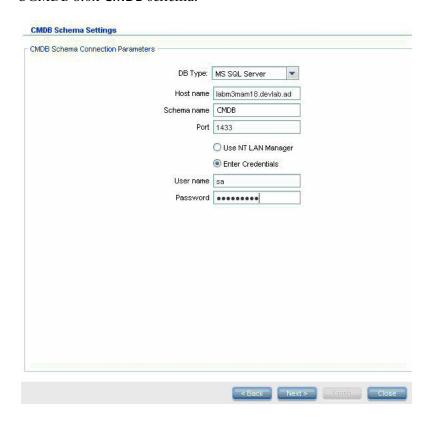
Important: You must perform this upgrade procedure only if you have UCMDB version 8.04 or later installed with Discovery and Integration Content Pack 8.00 deployed.

---

1 Locate, then launch the **upgrade** file:
   C:\hp\UCMDB\UCMDBServer\tools\upgrade.bat (Windows) or
   upgrade.sh (Linux).

2 The **Preparing to Upgrade** wizard opens. Click **Next** to open the UCMDB Server Upgrade window.

3 Select an **Oracle** or **MS SQL Server** database and set the **Foundations Schema** connection parameters.
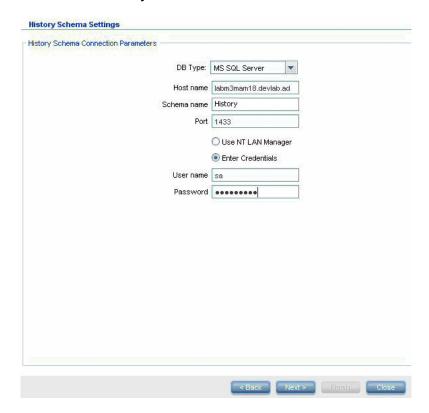
The **Schema name** should match the name of your previously replicated UCMDB 8.0x **Foundations** schema. For more details about the connection parameters see "Required Information for Setting Database Parameters" on page 107.
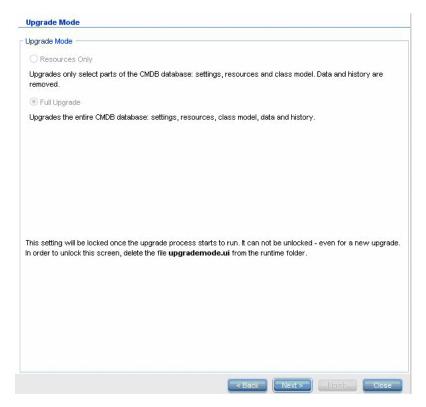
 4 Click **Next** and set the **CMDB Schema** connection parameters. The
   Schema name should match the name of your previously replicated
   UCMDB 8.0x **CMDB** schema.

5 Click **Next** and set the **History Schema** connection parameters. The **Schema name** should match the name of your previously replicated UCMDB 8.0x **History** schema.

History Schema Settings

History Schema Connection Parameters

DB Type:	MS SQL Server ▼
Host name	labm3mam18.devlab.ad
Schema name	History
Port	1433
	○ Use NT LAN Manager
	● Enter Credentials
User name	sa
Password	••••••••

< Back   Next >   Finish   Close
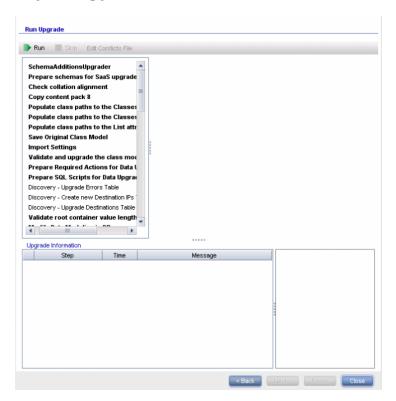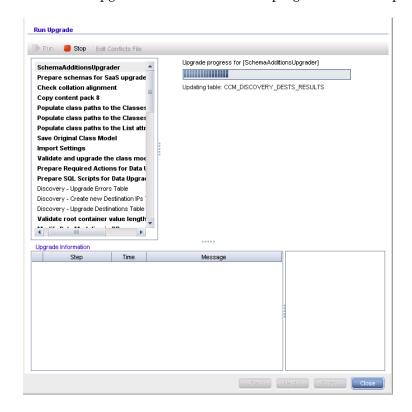
6 Click **Next** and select the Upgrade Mode:

Upgrade Mode

Upgrade Mode

○ Resources Only

Upgrades only select parts of the CMDB database: settings, resources and class model. Data and history are removed.

◉ Full Upgrade

Upgrades the entire CMDB database: settings, resources, class model, data and history.

This setting will be locked once the upgrade process starts to run. It can not be unlocked - even for a new upgrade. In order to unlock this screen, delete the file **upgrademode.ui** from the runtime folder.

[< Back] [Next >] [Finish] [Close]

➤ **Resources Only.** Upgrades only selected parts of the CMDB, not including data and history.

➤ **Full Upgrade.** Upgrades the entire CMDB, including data and history.

7 Click **Next**. The Run Upgrade screen lists the upgrade steps. Click **Run** to begin the upgrade.

 8 The Run Upgrade screen indicates the progress of each step.

 For details on failure implications and log messages for each step, see
 "Upgrade Steps" on page 197.

 For details about validating data model conflicts, see "Validate Data Model
 Conflict" on page 192.

 9 To re-run a specific step, right-click the step in the **Steps** pane and select
 Run Selected.
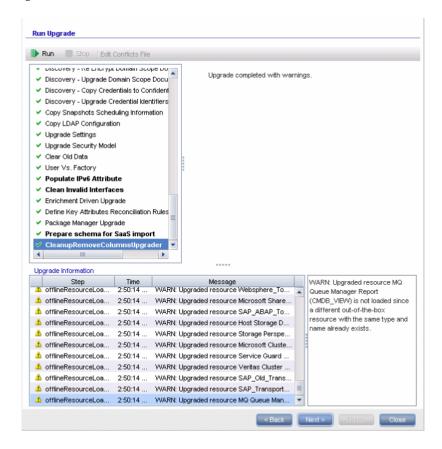
 Important: Rerunning a successful upgrade step should be done only for
 troubleshooting purposes.

⚓ Terminate the Upgrade Procedure

Upgrade may take a long time to complete. To terminate the upgrade at any point, click the red **Stop** button:

Steps that either complete with a warning or fail to run are logged in the **Upgrade Information** pane. To view this information, highlight the row where the upgrade step appears. Relevant information appears to the right.

191

Reference

🔍 Troubleshooting and Limitations

This section describes troubleshooting and limitations for upgrading from UCMDB 8.04 or later to UCMDB 9.04.

Validate Data Model Conflict

The Validate Data Model step in the upgrade uses the previous class model, the predefined transformations, and the out-of-the-box data model as input, then generates a modified data model (after the addition of missing data model entities) to disk under **C:\hp\UCMDB\UCMDBServer\runtime\old-class-model.xml**.

If a conflict is detected, for example, when a new class or attribute name defined by the user is allocated to a new out-of-the-box class or attribute, a new additional transformation file is generated and saved to disk under **C:\hp\UCMDB\UCMDBServer\runtime\added-class-model-changes.xml** and the upgrade process fails.

The new transformation file defines an additional transformation aimed to solve the conflicts by renaming classes and attributes. By running the upgrade again, you include these new transformations and enable the upgrade to proceed.

Important: If an additional transformation file is generated, you must close the upgrade wizard and restart it.

Resources Are Not Loaded to the Upgraded UCMDB

Resources using classes that are removed during upgrade are not upgraded and are not loaded to the upgraded UCMDB. Similarly, queries using attributes as a property condition are also removed during the upgrade. Apart from the data model transformations applied over these resources, the following changes are made:

➤ Views are redefined to match the new view definition.

➤ Topology reports are redefined as Views. In UCMDB 9.04, reports and views are regarded as different visualizations of the same data.

➤ Queries are saved in a user-friendly XML format.

14

Upgrade Process: Technical Descriptions

This chapter includes:

Reference

Reference

🔖 Input Parameters for the Upgrade Process

Depending on the type of upgrade you run (**Full** or **Resource Only**), the upgrade process uses the following components:

➤ Your database schema.

➤ Files describing the class model transformation being performed during the upgrade. These are files ending with **_changes.xml** located under the **C:\hp\UCMDB\UCMDBServer\conf\upgrade** directory.

➤ The out-of-the-box class model of version 8.04 and DDM Content Pack 8.00. This version enables the upgrade process to add missing class model entities before the upgrade.

➤ The out-of-the-box data model of version 9.00 and DDM Content Pack 8.00. This version enables the upgrade process to add missing class model entities after the upgrade procedure, and makes sure that the upgraded class model is compliant with HP Universal CMDB and Business Service Management.

🔖 Log Files for the Upgrade Process

During the upgrade, the following log files are used:

➤ **upgrade.detailed.log**. This is the main log file for the upgrade procedure. All upgrade actions are written to this log (unless otherwise stated in a specific upgrade step). Typically this file is between 30 MB to 70 MB in size.

➤ **upgrade.short.log**. A summary of the detailed log. All lines in this file appear in **upgrade.detailed.log** as well. This file should be used as a table of contents for the more detailed file, or as a general overview. Typically this file is less than 5 MB.

➤ **upgrade.detailed.attribute_cleanup.log**. This log file shows the progress of a complete cleanup of the data model so that an attribute is defined only once in a class hierarchy. All other definitions should be **attribute override** and all invalid attribute overrides are removed. This process occurs several times during the complete upgrade, during class model manipulation (validation with the previous class model, class model upgrade, and validation with the target class model). Typically, the combined size of these log files (**.log** file and all roll-over files) can be hundreds of MBs.

➤ **error.log**. This file is not specific to the upgrade and contains all errors and warnings sent by any other log (unless specifically blocked). It can be used as a map and as a general overview of upgrade success.

➤ **mam.packaging.log**. This log is relevant only for the Redeploy Basic Packages step and includes all of that step's information. For details, see "Redeploy Basic Packages" on page 249.

Upgrade Steps

This section describes the steps that comprise the complete upgrade process. For each step in the upgrade procedure, the following is described:

➤ A description of the step.

➤ Whether the step is critical. A step is considered critical in the following cases:

  ➤ Skipping it would prevent the UCMDB server from starting after upgrade.

  ➤ Skipping it would induce critical configuration or data loss that cannot be restored after upgrade.

  ➤ Skipping it would prevent a critical component from operating properly after the upgrade.

➤ If the step can be re-run. In case of failure during the upgrade, whether or not this step can be re-run over the same schemas.

➤ Implications of failure. If this upgrade step fails, what is the effect on the UCMDB? If the step can be re-run, what can be done to resolve the issues?

➤ Log Files. Important messages from the log file that are typical to this upgrade step, and the meaning of each message. Unless otherwise specified, all messages appear in the following log files:

➤ **C:\hp\UCMDB\UCMDBServer\runtime\log\upgrade.detailed.log**

➤ **C:\hp\UCMDB\UCMDBServer\runtime\log\upgrade.short.log** (Log messages in this file may be a duplicate of messages in the **upgrade.detailed.log** file.)

For details on logs, see "Log Files for the Upgrade Process" on page 196.

Important: Steps that are relevant for a **Resources Only** upgrade are marked as such.

This section includes the following steps:

➤ "Clear Old Data" on page 260

➤ "User vs. Factory" on page 261

➤ "Populate IPv6 Attribute" on page 263

➤ "Enrichment Driven Upgrade" on page 263

➤ "Define Key Attributes Reconciliation Rules" on page 264

➤ "Package Manager Upgrade" on page 264

SchemaAdditionsUpgrader

Adds the new required tables and columns to the CMDB.

Is Critical (Y/N)	Can Be Rerun (Y/N)
Y	Y

Implications of Failure

➤ Permissions issues (not enough permissions)

➤ Database connectivity issues (database cannot be connected)

➤ Locking (tables cannot be modified)

Log Files

➤ Updating table: … When updating a specific table in the database.

➤ Initializing default customer registration. When updating the global customer information.

Save Original Class Model

Note: Resources only upgrade.

Saves the complete class model, prior to the upgrade, to disk under
C:\hp\UCMDB\UCMDBServer\runtime\original-class-model.xml.

Is Critical (Y/N)	Can Be Rerun (Y/N)
Y	Y

Implications of Failure

➤ The existing user class model could not be read from the CMDB. Likely
cause: a corrupt class model definition. Solution: manually edit the class
model definition in the database before trying to re-run the step.

➤ The CMDB has no permissions to write to the
C:\hp\UCMDB\UCMDBServer\runtime folder. **Read/Write/Create** folder
permissions are needed for the entire installation folder (although most
Write commands are executed only on the **C:\hp\UCMDB\UCMDBServer
\runtime** folder).

Log Files

Failures in the **cmdb.classmodel.log** or **error.log** files may indicate which
entity in the class model failed to load.

Import Settings

Note: Resources only upgrade.

Copies relevant settings from the Foundation database to the management
table in the CMDB.

Is Critical (Y/N)	Can Be Rerun (Y/N)
Y	Y

Implications of Failure

Settings have not been correctly migrated and CMDB factory default values are being used instead. If the aging mechanism is enabled, large portions of the CMDB data model may be removed when the CMDB first starts up.

Incorrectly configured (or non-existent) Foundations database. Solution: Configure the Foundations database using the upgrade wizard. If the database has been damaged or a new database is desired, create an empty Foundations database using the UCMDB 8.0x database wizard.

Log Files

➤ Fetch old settings. When retrieving the settings from the 8.0x Foundations database.

➤ Set new settings. When writing the settings to the new Management database.

➤ Aging mechanism has been disabled. For details on aging, see "CI Lifecycle and the Aging Mechanism" in the *HP Universal CMDB Administration Guide*.

Validate and Upgrade Class Model

The Validate Class Model and Upgrade Class Model steps have been combined into one procedure, running one after the other. If the second part (upgrade) fails, then both steps will be run again in sequence. This step contains the following parts:

➤ "Validate Class Model" on page 203
➤ "Upgrade Class Model on Disk" on page 207

Validate Class Model

Note: Resources only upgrade.

Ensures your old class model, read from **C:\hp\UCMDB\UCMDBServer\ runtime\original-class-model.xml**, is aligned with the expected out-of the box class model. This is needed so that the old class model can be accessible for the class model transformations that are part of the upgrade process. This step uses the previous class model, the predefined transformations, and the out-of-the-box class models as input, and generates a modified class model after adding the missing class model entities to the **C:\hp\UCMDB\UCMDBServer\runtime\original-fixed-class-model.xml** file.

Important:

Class model changes files must not be modified after the completion of this step. This refers to the out-of-the-box files, the automatic conflict resolution file, and any file manually placed under **C:\hp\UCMDB\UCMDBServer\conf\upgrade**.

If the class model changes files are changed, the upgrade wizard and the automatic conflict resolution file must be completely closed and re-opened for the changes to take effect correctly.

Is Critical (Y/N)	Can Be Rerun (Y/N)
Y	Y

Note: If at the beginning of this step the **original-class-model.xml** file does not exist, it is re-read from the database.

Implications of Failure

If this step fails, check one of the following:

➤ **Attribute mismatch**. The **attribute** type is different from the out-of-the-box class model attribute types. Type conversion is not supported.

➤ **Class or attribute conflict**. The new class or attribute name defined by the user is allocated to a new out-of-the-box class or attribute. If this occurs, a new transformation file is automatically generated and saved to disk under **C:\hp\UCMDB\UCMDBServer\runtime\added-class-model-changes.xml** and the upgrade process fails. The new transformation file defines an additional transformation aimed at solving the conflicts by renaming your classes and attributes. Run the upgrade again to include these new transformations and allow the upgrade to proceed. Before re-running the upgrade, you can also manually modify these actions, for example, by choosing new names.

Note: If a conflict resolution file has been created or if you edit it via the UI, you must close the upgrade wizard completely and re-open it to correctly reload these changes.

Log Files

➤ A missing entity or unsupported additional entity in the user class model writes a warning to the log file. The warning includes the type of entity, its name, the location in the class model hierarchy, and the action taken to handle the entity (if any).

   ➤ Attribute type change is not allowed. Attribute <name> in Class <name> change type from <old-type> to <new-type>. In case of attribute type change, the error includes the name of the attribute and its class.

   ➤ Class hierarchy change may cause upgrade problems in Class <name>. The class name has changed its location in the class model hierarchy. The upgrade can handle specific kinds of hierarchy change, but at this point in the upgrade there is not yet enough information to decide on the change.

➤ Class removal is not allowed in Class <name>. Class was added. A factory class is missing from the user class model, so the class is forced back into the model. This can happen as a result of a user removing a class or as a result of failure in Content Pack 8.00 deployment.

➤ Class Qualifier addition of type <name> is not allowed. The qualifier was removed in Class <name>. Certain types of class qualifiers must not be added by the user. If a user added one of these qualifiers, this message is displayed and the class qualifier is removed from the class.

➤ Class Qualifier removal of type <name> is not allowed in Class <name>. The qualifier was added. If a qualifier is missing from a factory class, it is added to the class.

➤ Attribute removal <name> is not allowed. Attribute <name> in Class <name>. The Attribute was added. A factory attribute is missing from the user class model in a factory class, so the attribute is added to the class. This can happen as a result of a user removing an attribute or as a result of failure in Content Pack 8.00 deployment.

➤ Attribute Qualifier addition of type <name> in new attribute <name> is not allowed. The qualifier was removed in Class <name>. New attributes are attributes added by a user to a factory class. However, specific types of attribute qualifiers must not be added to new attributes, so the attribute qualifier is removed from the attribute in the user class model.

➤ Attribute Qualifier addition of type <name> in existing attribute <name> is not allowed. The qualifier was removed in Class <name>. Users must not add specific types of attribute qualifiers to factory attributes. The attribute qualifier, therefore, is removed from the attribute in the user class model.

➤ Attribute Qualifier addition of type <name> in new attribute <name> is not allowed. The qualifier was removed from the attribute override in Class <name>. New attributes are attributes created by a user for a factory class. The user also added an override on the new attribute in a sub-class. However, specific types of attribute qualifiers must not be added to new attributes or their overrides. Therefore, the attribute qualifier is removed from the attribute override in the user class model.

➤ Attribute Qualifier addition of type <name> in existing attribute <name> is not allowed. The qualifier was removed from the attribute override in Class <name>. Specific types of attribute qualifiers must not be added to factory attributes or its overrides. Therefore, the attribute qualifier is removed from the attribute override in the user class model.

➤ Attribute Qualifier removal <name> is not allowed. Attribute <name> in Class <name>. A user removed an attribute qualifier that came with the out-of-the-box class model. Specific types of attribute qualifiers must not be removed from factory attributes.

➤ Attribute Qualifier removal <name> in override is not allowed. Attribute <name> in Class <name>. A user removed an attribute qualifier in an attribute override that was included in the out-of-the-box class model. Specific types of attribute qualifiers must not be removed from factory attribute overrides.

➤ Valid Link <name> removal is not allowed. A valid link was removed by a user or failed to deploy from Content Pack 8.00. The valid link is restored to the user class model.

➤ Calculated Link <name> removal is not allowed. Class <name>. A calculated link was removed by the user or failed to deploy from Content Pack 8.00. The calculated link is returned to the user class model.

➤ TypeDef <name> removal is not allowed. If a factory type definition (Factory TypeDef – Enum or List) is missing from the user class model, it is returned to the model. The definition could be missing as a result of removal by the user or as a result of failure in a Content Pack 8.00 deployment.

➤ Enum entry removal is not allowed. Enum <name> with Enum entry key <key> and Enum entry value <value>. If an **Enum** entry is missing in a **Enum** type definition, the entry is returned to the **Enum** definition. The Enum entry could be missing as a result of removal by the user or as a result of failure in a Content Pack 8.00 deployment.

➤ List entry removal is not allowed. List <name> with List entry value <value>. If a List entry is missing in a List definition type, the entry is returned to the List. The List entry could be missing as a result of removal by the user or as a result of failure in a Content Pack 8.00 deployment.

➤ Enum entry addition can cause conflicts. Enum <name> with Enum entry key <key> and Enum entry value <value>. A user added an entry to a **Enum** type definition. At this point in the upgrade, there is not enough information to determine if the added entry causes the upgrade to fail.

➤ List entry addition can cause conflicts. List <name> with List entry value <value>. A user added an entry to a List type definition. At this point in the upgrade, there is not enough information to determine if the added entry causes the upgrade to fail.

➤ In case of attribute type changes, an error is produced with the name of the attribute and its class.

➤ Hierarchy changes produce a warning, with the name of the class that changed the parent class.

➤ Problems with the user class model produce the following error message: User class model is not valid for upgrade.

➤ Problems with class model transformations produce the following error message: Upgrade configuration files are not valid.

Upgrade Class Model on Disk

Note: Resources only upgrade.

Uses the class model generated in the Validate Class Model step:
C:\hp\UCMDB\UCMDBServer\runtime\original-fixed-class-model.xml
together with the predefined transformation files to generate the upgraded class model. This upgraded model is saved to disk under
C:\hp\UCMDB\UCMDBServer\runtime\upgraded-class-model.xml. For details, see "Validate Class Model" on page 203.

Is Critical (Y/N)	Can Be Rerun (Y/N)
Y	Y

Implications of Failure

The class model cannot currently be upgraded correctly.

➤ **Solution 1**: Edit the problematic classes in the 8.0x UCMDB instance and re-run the upgrade.

➤ **Solution 2**: Edit the class model changes files. For details, see "Validate Class Model" on page 203. If you edit these files, you must re-run the Validate Class Model step before continuing with the upgrade.

Log Files

➤ **General messages (all top level class model entities)**:

  ➤ Adding non-modified <entity type> <entity name>. The entity has not been modified between the user and the target class model. This message can also appear as Adding un-upgraded…

  ➤ Adding <entity type> <name>. An upgraded entity is added to the target class model.

  ➤ Skipping <entity type> <name> - Dropped in upgrade. The entity is to be explicitly removed in the upgrade. This message can also appear as Not adding…

  ➤ Skipping <entity type> <name> - exists in new basic CM. The entity exists in the basic class model and its definition there is used.

  ➤ Adding new <entity type> <name>. A new entity, marked to be added during the upgrade, is added to the target class model.

  ➤ Skipping adding new <entity type> <name> - exists in new basic CM. A new entity, marked to be added during the upgrade, is not added to the target class model since it is already specified by the basic class model.

➤ **Calculated links related messages**:

  ➤ Skipping calculated link <name> - exists in new basic CM, adding only triplets. The calculated link exists in the basic class model, but triplets from the user class model are added to it to preserve query (TQL) results.

➤ **Class related messages**:

  ➤ About to upgrade class <name>. This message is written before a class is to be upgraded. If a failure occurs, this message can be used to track which class caused the failure.

  ➤ Skipping class <name> - already added as a calculated link. The class has already been added as part of a calculated link. Refer to the previous log messages to discover what actually occurred with that class.

  ➤ skipping adding new class <name> extends <parent name> which does not exist. The class is not added to the class model because its parent cannot be found in the target class model.

➤ **Valid link related messages**:

  ➤ Skipping adding new valid link <name> - <end> class <class name> does not exist. The valid link cannot be added since a class (**end1**, **end2**, or **link**) cannot be found in the target class model.

  ➤ Duplicate CITs found: <names>. Due to an error, CITs have been added twice to the target class model. This error is unrecoverable without editing the upgrade class model changes files and re-running the Validate Class Model and Upgrade Class Model steps again. For details, see "Validate Class Model" on page 203 and "Upgrade Class Model on Disk" on page 207.

  ➤ Adding <old name> > <new name> to rename map. The rename map is used to identify old class names and map them to new class names.

  ➤ Mismatch between incremental rename map and changes util! Using incremental rename map. Incremental: <old name> > <new name>. Util: <old name2> > <new name2>. The actual rename map and the upgrade definition do not agree. This should be noted for verification since it may indicate a problem in the class model upgrade. This message does not itself stop the upgrade process.

➤ **Valid links validation**:

- ➤ Start removing invalid links. Valid links are to be checked and invalid ones (that is, no **end1**, **end2**, or **link** class) are removed.

- ➤ Link <entity> <name> does not exist in target class model - Removing valid link <name>. The valid link entity (**end1**, **end2**, or **link** class) does not exist in the target class model and so the valid link must be removed for the entire class model to be valid. Later, this may cause resources (for example, TQLs and Views) to fail the upgrade.

- ➤ Done removing invalid links. This message is displayed when this sub-step is complete.

➤ For a user class with key attributes different from its parent, the complete set of key attributes is restored. Each key attribute removed from its out-of-the-box ancestors and added to the new user class produces the following log information message: Added ID qualifier to attribute <attribute name> in class <class name>.

Prepare Required Actions for Data Upgrade

Note: Resources only upgrade.

Uses the **C:\hp\UCMDB\UCMDBServer\runtime\original-class-model.xml** file, the **C:\hp\UCMDB\UCMDBServer\runtime\upgraded-class-model.xml** file, and the class model transformations to deduce the actions required to perform the data transformation.

Saves the analysis result to disk in the following file: **C:\hp\UCMDB\ UCMDBServer\runtime\data-upgrade-actions.xml**. This step skips CITs that cause the data upgrade to omit data that cannot be upgraded. The CITs are listed in **C:\hp\UCMDB\UCMDBServer\upgrade\ DataModelUpgradeConfig.xml** (**app-infra.jar**).

Is Critical (Y/N)	Can Be Rerun (Y/N)
Y	Y

Implications of Failure

The upgrade cannot deduce the actions needed to transform the data model from the previous version class model to the target class model. Configuration and data upgrade cannot continue without this step being completed.

Log Files – Initial Analysis

Note: In this section, **DI** means data items: CIs or Links.

General Information

➤ This step regards the data upgrade configuration as a series of copy rules with possible transformations and conditions.

➤ A source for an attribute can be either:

  ➤ A property on the source DI.

  ➤ A constant value for all DIs of a specific concrete class.

➤ The logs for this step are nested (using indentations). An indented log message is usually preceded by a header that determines the context of the analysis.

➤ Class rule types:

  ➤ Modified, Moved, Merged. DIs that belong to rules marked as one of these should be copied to the new data model (with possible transformations).

  ➤ Added, Deprecated. These CITs are new. As such, they cannot have any DIs.

  ➤ Removed. These CITs are explicitly removed during the upgrade. Their DIs are not copied to the target class model (unless otherwise noted by another rule).

➤ Attribute rule types:

  ➤ Added. The rule defines an attribute that is either new or keeps its name.

  ➤ Deprecated, Modified. The rule defines a transformation for an existing attribute that is being renamed.

  ➤ Removed. The rule defines that this attribute should not exist in the target DI.

➤ Default rule or default action. Defined on a specific CIT. That is, the target CIT name is the same as the source CIT name. Attributes of DIs defined in the target CIT level are copied from attributes with the same name at the source CIT level name. Attributes in the parent CIT use the parent CIT rules.

General Class or Rule Analysis

➤ Rule type for class <name> is <type>. Analysis for the specified class is about to start.

➤ Class <name> added to added CITs. The CIT is new, therefore no DIs exist for it. It is added to an added CITs reference list in the XML file.

➤ Class <name> added to removed CITs. The CIT is marked to be removed together with all its DIs.

➤ Change has empty class name. A warning that the requested transformation is invalid and no action is to be taken. Cause: invalid transformation definition.

➤ Target CIT name is <name>, Source CIT name is <name> (from <origin>). DIs of the source CIT are to be copied to the target CIT.

➤ Target CIT <name> does not exist in target class model, skipping rule! A warning that the target CIT was not properly created. The entire rule is to be skipped since it cannot be completed. Cause: invalid transformation definition or incorrect class model upgrade.

➤ Source CIT <name> does not exist in source class model, skipping rule! A warning that the source CIT cannot be found in the user class model. The entire rule is to be skipped since it cannot be completed. Cause: invalid transformation definition, incorrect class model upgrade, or the user class model (after fixes) does not conform to the 8.0x class model.

➤ Source CIT <name> does not exist in source class model, skipping rule, adding to added CITs! A warning that the rules do not match the actual class model. The source CIT cannot be found, so the target CIT is to be handled as if it is a new CIT (that is, there is no data upgrade). Cause: invalid transformation definition, incorrect class model upgrade, or the user class model (after fixes) does not conform to the 8.0x class model.

➤ Source CIT is empty, Target CIT is empty. A warning that the transformation rule is invalid. The rule is skipped. Cause: invalid transformation definition.

Copy Condition Analysis

➤ Could not create copy condition for source CIT <name> - CIT does not exist in old class model. The class has a condition from which DIs should be copied, but that source CIT does not exist in the user class model. A warning that the condition is to be ignored. Cause: invalid transformation definition or the user class model (after fixes) does not conform to the 8.0x class model.

➤ Could not create copy condition for source CIT <name> and attribute <attribute name> - CIT exists but does not have the attribute. The class has a condition from which DIs should be copied, but that attribute in the source CIT does not exist in the user class model. A warning that the copy instruction is to be ignored. Cause: invalid transformation definition or the user class model (after fixes) does not conform to the 8.0x class model.

➤ Copy condition attribute: <name>, Type: <type>, Operator: <operator>, Copy condition value: <value>. For a DI to be copied (and not discarded), the value of the attribute must maintain the indicated condition (for example, **ipport not-equal to 3**).

➤ Attribute condition.attribute name is empty. The attribute name is empty. A warning that the copy condition is invalid and is not to be used (all DIs are to be copied). Cause: invalid transformation definition.

➤ Copy condition value is empty. The copy condition value is empty. A warning that the copy condition is invalid and is not to be used (all DIs are to be copied). Cause: invalid transformation definition.

General Attribute Analysis

➤ Entering copy attribute analysis. The attribute analysis is about to start.

➤ Rule type for attribute <old name> > <new name> is <rule type>. The analysis for this rule is about to start. Note: MERGED and MOVED types are not applicable for attribute rules.

➤ Rule type changed from <original type> to ADDED - no old name or oldName == Name. Although the rule is defined as modified, the actual data action should treat this attribute as added, since there is either no change in the attribute name or there is no such old attribute (the difference between the user class model and the expected 8.0x class model).

➤ No target class <name> in new class model. A warning that the target class cannot be found in the target class model and this attribute rule is to be skipped. Cause: incorrect class model upgrade.

➤ No target attribute <name> in target class <class name> in new class model. A warning that the target attribute in the target class cannot be found in the target class model and this attribute rule is to be skipped. Cause: incorrect class model upgrade.

➤ Attribute <name> in class <class name> in new class model is declared STATIC_ATTRIBUTE. Skipping rule. Static attributes are connected to the CIT and not to the actual DI. As such, they should not be copied during the data upgrade.

➤ Attribute <name> in class <class name> in new class model is of simple list type. Skipping rule. Value lists (multiple values) are handled in a different upgrade step and are skipped here.

➤ Attribute <name> is a root class attribute that is not duplicated to concrete classes. Skipping rule. The specific rule is skipped because the attribute should not be copied to the concrete class tables in the database.

Copy Attribute from Class Analysis

➤ Copy attribute from class. This attribute value is determined by the concrete class of the DI.

➤ Attribute constant value: <value>. For this concrete class, the attribute value is the value specified in the message.

Copy Attribute from Attribute Analysis

➤ Copy attribute from attribute. This attribute value is determined by another attribute.

➤ Old attribute name: <name>. Applicable for an added attribute: the source attribute is the name specified in the message.

➤ Source attribute name (from enum): <name>, Source attribute name (from OldName): <name>. Applicable for a modified attribute: the source for this rule either is constant (from enum) or is another attribute (from OldName).

➤ **Mapped transformation inside copy attribute**:

  ➤ Entering map transformation analysis. The source should be transformed using source to target mapping (dictionary).

  ➤ Adding transformation: <old value> > <new value>. The old value is to be replaced with the new value.

  ➤ From value is empty. To value is empty. The from/to value is empty, and this transformation does not occur. Cause: invalid transformation definition.

Added Attribute (New or not Renamed) Analysis

➤ Copy attribute from default value: <name>. The attribute has no attribute source, so its value is determined by the new default value.

  ➤ Attribute name is empty, Attribute default value is empty. This attribute rule is invalid and is not used. Cause: invalid transformation definition.

Modified Attribute (Renamed) Analysis

➤ Copy attribute from source value: <name>. The attribute value is determined by another attribute in the source DI.

  ➤ Attribute name is empty, Attribute default value is empty. This attribute rule is invalid and is not used. Cause: invalid transformation definition.

Common Attribute Analysis

➤ Completing and adding. A message that the upgrade is beginning the common analysis stage for this attribute rule.

➤ Attribute was not properly completed. The common analysis stage failed, and the attribute rule is not used. This is preceded by one of the following messages:

  ➤ Target CIT empty. The target CIT is empty. Cause: invalid rule.

  ➤ Target CIT does not exist in new class model. The target CIT is empty. Cause: invalid rule or incorrect class model upgrade.

  ➤ Target attribute name is empty. The target attribute name is empty. Cause: invalid rule.

  ➤ Target attribute <name> does not exist in target CIT in new class model! The attribute was not found in the target class model. Cause: invalid rule or incorrect class model upgrade.

  ➤ Cannot determine target type <name>. The target attribute type is invalid. Cause: incorrect class model upgrade.

  ➤ Source CIT name is empty. The source CIT is empty. Cause: invalid rule, incorrect class model upgrade, or previous error in data action analysis.

  ➤ Source attribute name is empty, Source attribute is null. The source CIT is empty. Cause: invalid rule, incorrect class model upgrade, or previous error in data action analysis.

➤ Types:

  ➤ Setting new type <type>, Setting old type <type>. The attribute was determined to be of the specified type. This is later used to create the correct SQL type-cast.

  ➤ Target attribute is <name>, Source attribute is <name>. The attribute name is the name specified in the message.

  ➤ Constant value requires new type declaration. New type and old type are <type>. The attribute should be filled from a constant value with the specified type.

➤ Default values:

  ➤ Target default value is <value>. The target attribute has a default value. This value is used if the original DI property is empty.

  ➤ Source default value is <value>. If the DI original property is equal to the old default value, it is transformed into the new default value.

➤ Size limits:

  ➤ New size set <size> set from default, Constant value new size is <size>. The target attribute is of type string. As such, it must have a size limit. None was specified so the default size limit is used (50 characters).

  ➤ Old size is <size>, setting truncate flag. The target size limit is less than the source size limit. Values may be truncated.

  ➤ New size is <size>. A new size limit is specified.

➤ Attribute did not pass validation. The final validation failed, so the attribute rule is not used. The actual causes must be looked for in messages from the actual action building. This must be preceded by one of the following:

  ➤ No target attribute. For some reason, the target attribute name remains empty.

  ➤ Target attribute does not exist in target class model. The target attribute does not exist in the target class model.

  ➤ No source. The attribute source (source attribute or constant value) remains undetermined.

  ➤ Source attribute does not exist in source class model

  ➤ Source attribute size limit > Target attribute size limit but truncate needed flag is false.

  ➤ Target attribute target type is missing.

  ➤ Target attribute source type is missing.

  ➤ Target attribute source and target types are not the same, but attribute source is of type CONSTANT_VALUE.

  ➤ Instruction for target attribute already exists. Values for the target attribute in this specific CIT are already generated by another rule.

➤ Value transformation source is empty, Value transformation target is empty. The value map transformation is invalid.

Log Files – Post Analysis

Rules Flattening. The rules defined in the class model changes have been converted to actions. This stage now copies rules from parent classes to child classes, to create a complete non-trivial rule-set disconnected from the class hierarchy.

➤ Flatten rules stage. The stage begins.

➤ Building class to direct children map. Starting to build a complete class to child dictionary.

  ➤ Class <child name> is a child of <parent name>.

  ➤ Class appeared twice. Warns that a class was found twice. Most likely, the class model is not valid.

➤ Building by target and by source rules map. Starting to build two class-to-rules dictionaries: one is source class to rule, the other is a target class to rule.

  ➤ Found rule from <source> to <target>.

  ➤ Adding this rule will corrupt the by target map, By source map already contains this CIT. A warning that the rule cannot be added to the map because another instance of it already exists under a different target or source class. The rule is ignored for child classes.

➤ Entering DFS over target class model. Starting the flattening stage by going over the class model, from top to bottom.

  ➤ Visiting <class> (added <children> children). Starting to handle the specified class. Found that this class has the specified children and handles them later.

  ➤ No rule for <name>, it exists in old class model and it was not explicitly added or removed - adding default rule. A default rule is used to copy the DIs of this CIT.

➤ Visiting rule from <source class name>. Starting to look at attribute rules from the specified source CIT. During this stage, the source tree is checked from the bottom (the specified CIT) up (root), to collect the correct set of rules. The bottom-most rule that generates a value for a target attribute is the one used.

   ➤ Visiting source class <name>. The specified source class to be checked.

   ➤ Found rule from source class <source> to <target>. Starting to check the specified attribute copy rule.

   ➤ Rule matches for flattening. The can be applied over the target class (the rule target class is the **current** target class or a parent of that class).

   ➤ Going over source rules with targets: <targets>. Starting investigating the rule with the given target attributes.

   Rule to <target> is not mapped - attribute exists in concrete source class and concrete target class. The rule is not used since the attribute exists in the source concrete class and the target concrete class (it should be copied as-is).

   Rule to <target> is not mapped. The specified target attribute still does not have any value generator rule.

   Rule is not in ignore list - adding to target attribute rules. The specified rule is used to generate values for the target attribute.

   Attribute did not pass validation. The attribute rule did not pass validation. See the previous section about possible validation messages and causes.

   Rule is in ignore list - not added. The attribute cannot be copied (it is marked as such), so it cannot be used.

   ➤ Going over ignore list: <attributes>. If an attribute was removed, it appears in this list. Attributes from this list should not be copied to the target attribute. Since the investigation is done bottom-up, this list is created and added to at each CIT level.

   Adding ignored attribute <name>. Found an attribute in the do not copy list. Adding it to the current ignore list so that this attribute would not be copied if seen in the parent CIT.

➤ Going over copy conditions. Copies the copy conditions (whether the DI should be copied at all). This is also copied from the parent class (bottom-most rule wins).

Copy condition is for attribute name <name>. Found a copy condition that depends on the specified attribute.

Adding copy condition for attribute name <name> with values <values>. The attribute was not yet constrained by any other copy condition. Now it is constrained by the 'current' copy condition.

Abstract classes elimination stage. Abstract CITs do not have DIs (or tables under the new data model). Rules that have been created for these CITs (flattening process, errors, and a mismatch between the user 8.0x class model and the expected class model result) are now deleted.

➤ Remove abstract classes stage. This stage is starting.

➤ Removing rule from <source name> to <target name> - <source/target> is abstract in new class model. This copy rule is removed because either the source CIT or target CIT is marked as abstract.

Trivial rules stage. If an attribute with the same name exists in the source CIT and the attribute name is not part of attributes not-to-copy collection, a default rule is added for it.

➤ Found rule from <source class> to <target class>. Processing the specified rule.

➤ Adding CMDB_ID rule. All CITs should have a rule to copy the CMDB_ID column.

➤ Target class <class name> is a link. Adding <end1> and <end2> rules. All link classes should have two rules to copy the end1 column and end2 column.

➤ Checking attribute <name>. Processing the specified attribute.

➤ Attribute <name> has qualifier STATIC_ATTRIBUTE, skipping. The attribute is static, so it should not be copied.

➤ Attribute <name> is CmdbSimpleList, skipping. Multi values attributes are handled in a different upgrade step, so no rule is needed.

➤ Attribute <name> appears in root, skipping. Attribute appears in root class and it is not duplicated in the leaves tables, so no rule is needed.

➤ Attribute is not mapped, nor in 'do not copy' list. Attribute should be copied using a default rule.

➤ Found source attribute with the same name - creating default copy rule. An attribute with the same name was found in the source class model, so it is going to be the source for the default rule.

➤ No source attribute, checking default value, Found non empty default value - creating default constant copy rule. Default value: <value>. There is no source attribute with the same name, so the default value (if one exists) is used as a source for the default rule. If the second message does not appear, then no rule is used and the attribute value remains empty.

➤ completing and adding. Attribute was not properly completed. Attribute did not pass validation. These messages have the same meaning as in the initial stage.

Prepare SQL Scripts for Data Upgrade

Note: Resources only upgrade.

Analyzes the **C:\hp\UCMDB\UCMDBServer\runtime\data-upgrade-actions.xml**, generates the actual SQL statements that should be executed in the database to upgrade the data and saves it to disk under **C:\hp\UCMDB\UCMDBServer\runtime\data-upgrade-script.sql**.

Is Critical (Y/N)	Can Be Rerun (Y/N)
Y	Y

Implications of Failure

Failure in this step means that the upgrade could not convert the actions (from the XML) to the SQL statements needed to transform the data model from the previous version class model to the target class model. Configuration and data upgrade cannot continue without this step being completed.

Possible fixes for errors: Remove the offending action (entire class or just the attribute) from the data upgrade actions XML. This would result in a possible data loss (that class / attribute would not be copied) but would enable the upgrade to continue.

Log Files

➤ Could not create cast for <source class> > <target class>, on <source> > <target attribute>. The SQL generator did not find the correct way to transform the type of the source (attribute or constant) to the type of the target attribute. Possible causes are unsupported type casts (not all possible type conversions are supported) or a bad analysis (error / bad definitions / unexpected user class model changes). The effect is that these attribute values would not be cast. During the actual SQL invocation, this might fail the statement. This error should not stop the upgrade process.

➤ Could not create copy condition for <source class> > <target class>. The SQL generator could not understand conditional copy clause. Possible causes are unsupported conditions (not all possible conditions are supported) or a bad analysis (error / bad definitions / unexpected user class model changes). The effect is that this copy condition does not occur and all CIs of the source CIT type are copied. This error should not stop the upgrade process.

➤ Default value exceeding 4000 characters is ignored. Table: <table>. Column: <column>. The default value set for this column is too large to fit into the SQL statement. Possible cause is a too big default value in the user class model. The effect is as if no default value exists for this column. This error should not stop the upgrade process.

Discovery – Upgrade Errors Table

Upgrades discovery errors data (stored in the **CCM_DISCOVERY_ERRORS** table in the CMDB). This table replaces error messages by error codes with parameters (discovery runtime information).

Is Critical (Y/N)	Can Be Rerun (Y/N)
N	Y

Implications of Failure

Information regarding discovery errors is lost. Skipping this step requires you to truncate the **CCM_DISCOVERY_ ERRORS** table in the CMDB and re-activate all discovery jobs after the server is backed up.

Log Files

➤ Starting upgrade 'CCM_DISCOVERY_ERRORS' table

➤ Upgrade 'CCM_DISCOVERY_ERRORS' table was successfully finished!

➤ Failed to upgrade 'CCM_DISCOVERY_ERRORS' table

Discovery – Create New Destination IPs Table

Creates a new table in the CMDB named **CCM_DISCOVERY_DEST_IPS**. The new table holds the IPs of each one of the destinations. The information is extracted from the **CCM_DISCOVERY_DESTS** table (discovery runtime information).

Is Critical (Y/N)	Can Be Rerun (Y/N)
N	Y

Implications of Failure

Information regarding discovery destinations is lost. Skipping this step requires you to truncate the **CCM_DISCOVERY_DEST_IPS** table in the CMDB and re-activate all discovery jobs after the server is back up.

Log Files

➤ Starting upgrade 'CCM_DISCOVERY_DEST_IPS' table

➤ Upgrade 'CCM_DISCOVERY_DEST_IPS' table was successfully finished!

➤ Failed to upgrade 'CCM_DISCOVERY_DEST_IPS' table

Discovery – Upgrade Destinations Table

Renames CI types in **CCM_DISCOVERY_DESTS** table in the CMDB (discovery runtime information).

Is Critical (Y/N)	Can Be Rerun (Y/N)
N	Y

Implications of Failure

Information regarding discovery destinations is lost. Skipping this step would require the user to truncate the **CCM_DISCOVERY_DESTS** table in the CMDB and re-activating all discovery jobs after the Server is up.

Log Files

➤ Starting upgrade 'CCM_DISCOVERY_DESTS' table

➤ Upgrade 'CCM_DISCOVERY_DESTS' table was successfully finished!

➤ Failed to upgrade 'CCM_DISCOVERY_DESTS' table

➤ Ci type [old CI type] has been upgraded to [new CI type]. Indicates that the class [old CI type] was renamed to [new CI type].

➤ failed to update [old CI type], skipped. Indicates that a CI type could not be changed according to new schema, possibly due to data inconsistency in CMDB or wrong CI type defined by the user. Does not affect the discovery functionality, but can affect the display of destination in UI.

Modify Data Modeling in DB

Note: Resources only upgrade.

Modify CMDB structure to the new 9.00 structure.

Is Critical (Y/N)	Can Be Rerun (Y/N)
Y	N

Implications of Failure

Failure means that the database schemas are not in a correct format for the new UCMDB. The upgrade process cannot continue without this step. To try and run this step again, restore the CMDB schemas from the backup, delete the **C:\hp\UCMDB\UCMDBServer\runtime** folder, and run the upgrade tool from the beginning.

Log Files

None

Copy E-mail Recipient Information

Note: Resources only upgrade.

Copies e-mail recipient information from the **EmailRecipient** data table to the **EN_UI_RECIPIENTS** management table in the CMDB. (In UCMDB 8.x the recipient data was modeled as a CI). **EmailRecipient** is later removed as part of the data upgrade.

Is Critical (Y/N)	Can Be Rerun (Y/N)
N	Y, if the class model upgrade has not yet run

Implications of Failure

Scheduled reports are not sent. Users must add recipients through the Recipients Manager or through the upgraded scheduled jobs themselves.

Log Files

➤ Number of EmailRecipients in the CMDB is x. The existing number of recipients.

➤ Failed to handle Recipient. If the upgrade fails.

➤ RecipientUpgrader is complete. If the upgrade succeeds.

Copy Report's Scheduling Information

Note: Resources only upgrade.

Copies scheduled reports configuration from Foundation database to new management table in the CMDB.

Is Critical (Y/N)	Can Be Rerun (Y/N)
N	Y

Implications of Failure

Your scheduled reports are not upgraded, so you should reschedule them.

Log Files

➤ Upgrade of scheduled report finished successfully.

➤ failed to upgrade scheduled reports. For an overall failure.

➤ failed to upgrade scheduled report of job name <job name>. For failure on a specific job.

Copy Resources to Disk

Note: Resources only upgrade.

Extracts queries, views, reports, enrichments, and correlations from the database and stores them to disk. The resources are stored under a **C:\hp\UCMDB\UCMDBServer\runtime\1\<resource type>\<sub folder name>** subfolder. Resource types can be one of the following:

➤ **bacviews**. Old resource type, does not exist in 9.0.

➤ **bundles**. Used to define a resource group. Allows many to many relationship.

➤ **cmdbview**. New view definition, undergo class model upgrade only.

➤ **Correlations**. Correlation rules, undergo class model upgrade only.

➤ **Enrichments**. Enrichment rules, undergo class model upgrade only.

➤ **goldmaster**. Goldmaster report definition, undergo class model upgrade only.

➤ **Patterns**. Queries (TQLs), undergo both structure and class model upgrade.

➤ **reports**. Topology reports, undergo structure upgrade to become cmdbview and, after that, class model upgrade.

➤ **singlepatternref**. Perspective based query, undergo class model upgrade only.

➤ **viewrefs**. Perspective based view, undergo class model upgrade only.

➤ **views**. Old view definitions, undergo structure upgrade to become cmdbview.

Subfolders can be one of the following:

➤ **db**. Original resources.

➤ **structure**. Resources after structure upgrade.

➤ **classmodel**. Resources after class model upgrade.

Resources are upgraded in two phases:

➤ **Structure upgrade**. Upgrades the resources from old to new format. This step is performed for patterns, views, and topology reports. Upgraded resources are put under the **structure** folder, with the exception of views and reports, which are both upgraded to the **cmdbview\structure** folder. Resources without a structure upgrade are copied from the **db** to the **structure** subfolder.

➤ **Class model upgrade.** Upgrades the resources according to class model transformations. This affects all resources. Upgraded resources are saved to the **classmodel** folder.

In addition to the resources, some additional data is copied: **bundles** (resource grouping) and **bacviews** (handles to views). These are maintained as unchanged during the upgrade.

Is Critical (Y/N)	Can Be Rerun (Y/N)
Y	Y

Implications of Failure

Resources cannot be upgraded, since none exist on the disk for upgrade. Do not try to continue without completing this step.

Log Files

➤ Retrieve resources from database messages:

   ➤ got <number> < resource-type> from database. Specify how many resources were retrieved from the database for each type of resource. This message is followed by the list of resource names.

   ➤ did not succeed to read <resource-type> from database . Consult the exception that comes with the message for problem description.

   ➤ did not success to write <resource-type> to disk! Check the accompanying exception for reason. Verify write permissions exist and enough disk space.

   ➤ Could not write resource <name>. Check the accompanying exception for reason. Verify write permissions exist and enough disk space.

   ➤ did not success to write resource bundles to disk! Check the accompanying exception for reason. Verify write permissions exist and enough disk space.

➤ Remove resources from database messages:

   ➤ did not success to remove all <resource-type> from database. Consult the exception that comes with the message for problem description.

   ➤ did not success to remove from database all <resource-type> additional data for <resource-type>. Consult the exception that comes with the message for problem description.

Truncate Data Tables

Note: Resources only upgrade.

Removes all non-relevant data from the CMDB and History schemas. All non-configuration data that is not needed for the Resource Only upgrade is deleted in this step.

Is Critical (Y/N)	Can Be Rerun (Y/N)
Y	Y

Implications of Failure

Non-upgraded data remains in the CMDB and History schemas. Since part of the data is not upgraded in the next steps, the system behavior after the upgrade finishes is unpredictable .

Log Files

➤ Truncating table <name>. Removing all data from the specified table.

➤ Table <name> will not be truncated (data is needed for resources upgrade). The table contains configuration data, and we do not delete this data.

➤ Query to delete irrelevant data from root table: <SQL-statement>. The statement that removes all irrelevant data from the root table.

Rename Original Data Tables

Note: Resources only upgrade.

Rename your old data tables, adding the **TEMP_** prefix to the names of all CDM tables.

Is Critical (Y/N)	Can Be Rerun (Y/N)
Y	N

Implications of Failure

The upgrade process should be run again from the beginning after fixing the problem. Restore the database schemas, delete the **C:\hp\UCMDB\UCMDBServer\runtime** folder, and start the upgrade from the beginning.

Log Files

None

Upgrade Class Model in DB

Note: Resources only upgrade.

Truncate class model tables in the CMDB, removing old class model definitions, uses the **C:\hp\UCMDB\UCMDBServer\runtime\upgraded-class-model.xml** to populate the class model tables with the upgraded class model data and creates the new data tables (CDM tables) in their upgraded structure.

Is Critical (Y/N)	Can Be Rerun (Y/N)
Y	Y

Implications of Failure

Failure implies that the new class model was not loaded into the database. The upgrade cannot continue without the new class model.

Log Files

None

Upgrade Resources on Disk

Note: Resources only upgrade.

Reads original queries, views, reports, enrichments and correlations from disk, upgrade and store them upgraded on disk. It is important to know that resources using classes which are being removed during the upgrade are not being upgraded and will not be loaded to the upgraded UCMDB. Similarly, queries using attributes that are removed during the upgrade, as a property condition, are also removed. Apart from the class model transformations applied over these resources, the following changes are made:

➤ Views are redefined to match the new view definition.

➤ Topology reports are redefined as views. UCMDB 9.0 introduces the new concept which considers reports and views as different visualization of the same data.

➤ Queries are being saved in a new, more human readable, XML format.

Is Critical (Y/N)	Can Be Rerun (Y/N)
Y	Y

Implications of Failure

Failure in the entire step results in failure of the entire upgrade. In this case, after performing the necessary fixes, it is possible to re-run the upgrade from this step.

Failure to upgrade individual resource can be handled by running this step again or after the upgrade has finished. The failed resources should be updated manually in order to fix the problem that caused them to fail in upgrade.

Log Files

➤ General log messages:

➤ Removing all the following resources: [<list-of-resources-names>] of type <name> due to filter_resources.xml configuration file. The configuration file **filter_resources.xml** contains all the names and types of old resources from UCMDB 8.0x that do not exist in UCMDB 9.0x. All these resources are removed in the upgrade process. This log message specifies all those resources.

➤ Pattern upgrade:

➤ About to upgrade pattern structure for the following patterns (<number-of-patterns>) <list-of-pattern-names>. List the pattern names that are about to be upgraded.

➤ About to check if pattern <name> should be removed. Notifies before checking if needs to upgrade this pattern or not. If the pattern is removed, the next message informs you of such an action.

➤ Pattern <name> should be removed - has template instance group id. All patterns within the group template instance are removed in the upgrade.

➤ About to remove unneeded pattern <name>. Pattern that are not upgraded, like pattern <name>, can be located under the path **C:\hp\UCMDB\UCMDBServer\runtime\upgrade\<customer-id>\patterns\unupgradeable\<pattern-name>.xml**. The pattern is not upgraded and therefore would not exist in the post-upgrade resources.

➤ About to check if pattern <name> should be upgraded. Notifies before checking if this pattern is to be upgraded. The messages to follow specify the reasons for upgrading a pattern.

➤ Pattern <name> _should_ be upgraded, about to upgrade. Going to upgrade the pattern. The following messages specifies the parts of the pattern that are upgraded.

➤ About to write patterns to disk after structure upgrade (<number-of-patterns>):{<list-of-pattern-names>}. These patterns can be found under **C:\hp\UCMDB\UCMDBServer\runtime\upgrade\<customer-id>\patterns\structure**.

➤ About to upgrade pattern <name>. Starting the class model upgrade in the pattern.

➤ Pattern <name> was upgraded. The pattern was upgraded and is located under **C:\hp\UCMDB\UCMDBServer\runtime\upgrade\<customer-id>\patterns\classmodel**.

➤ Pattern <name> did not need upgrade. All the class model entities in the pattern are already compatible with 9.0. The pattern can be found under **C:\hp\UCMDB\UCMDBServer\runtime\upgrade\<customer-id>\patterns\classmodel**.

➤ Pattern <name> is not valid after upgrade. The pattern was removed and was not upgraded. It is probably because at least one class model entity does not exist in the class model anymore.

➤ Could not upgrade pattern <name>. Check the following exception for problem description.

➤ Single pattern reference:

➤ About to upgrade single pattern reference <name>. The result resources can be located under **C:\hp\UCMDB\UCMDBServer\runtime\upgrade\<customer-id>\singlepatternref\classmodel**.

➤ Enrichment upgrade:

➤ About to upgrade enrichment <name>. Enrichment does not need structure upgrade, so we start directly with the class model upgrade.

➤ Couldn't obtain pattern <name> for enrichment definition<name>. Pattern does not exist for the current enrichment.

➤ Enrichment <name> was upgraded. The enrichment is upgraded and is located under **C:\hp\UCMDB\UCMDBServer\runtime\upgrade\<customer-id>\enrichments\classmodel**.

➤ Enrichment <name> did not need upgrade. All the class model entities in the enrichment are already compatible with 9.0. The enrichment can be found under **C:\hp\UCMDB\UCMDBServer\runtime\upgrade\<customer-id>\ enrichments \classmodel**.

➤ Enrichment <name> is not valid after upgrade. The enrichment was removed and was not upgraded. It is probably because at least one class model entity does not exist in the class model anymore.

➤ Correlation upgrade:

➤ About to upgrade correlation <name>. Correlation does not need structure upgrade, so we start directly with the class model upgrade.

➤ Correlation <name> was upgraded. The correlation was upgraded and can be found under **C:\hp\UCMDB\UCMDBServer\runtime\upgrade\<customer-id>\correlations\classmodel**.

➤ Gold Master report upgrade:

➤ About to upgrade gold master definitions for class model changes. Gold master does not need structure upgrade, so we start directly with the class model upgrade.

➤ Got <number> gold master definitions. Number of gold masters in the system.

➤ Gold master report <name> was upgraded for class model changes. The report was upgraded and is located under **C:\hp\UCMDB\UCMDBServer\runtime\upgrade\<customer-id>\goldmaster\classmodel**.

➤ Gold master report <name> was not changed. All the class model entities in the report are already compatible with 9.0. The report can be found under **C:\hp\UCMDB\UCMDBServer\runtime\upgrade\<customer-id>\ goldmaster\classmodel**.

➤ View upgrade:

  ➤ About to upgrade view <name> structure.

  ➤ Could not upgrade template view [bac view name: [<name>], mam name: [<name>]] - <reason>. A common reason is Pattern by name [<name>] not found. This can happen after the pattern is removed in the pattern upgrade stage. The list of removed patterns is in the log message Removing all the following resources: [<list-of-resources-names>] of type <name> due to filter_resources.xml configuration file.

  ➤ View <name> structure was upgraded by a previous depending view. View was previously upgraded. No need to upgrade again.

  ➤ View <name> structure was upgraded. The view can be found under **C:\hp\UCMDB\UCMDBServer\runtime\upgrade\<customer-id>\cmdbview\classmodel** or **C:\hp\UCMDB\UCMDBServer\runtime\upgrade\<customer-id>\bacviews\classmodel**, according to the view type.

  ➤ Could not upgrade view <name>. The accompanying exception can elaborate on the reason for the failure. The view is not upgraded and is located in one of the following folders: **C:\hp\UCMDB\UCMDBServer\runtime\upgrade\<customer-id>\cmdbview\unupgradeable** or **C:\hp\UCMDB\UCMDBServer\runtime\upgrade\<customer-id>\bacviews\unupgradeable**, according to the view type.

  ➤ About to upgrade view <name>. Start to upgrade the class model entities in the view.

  ➤ Class model transformation for view <name> finished. The view can be found under **C:\hp\UCMDB\UCMDBServer\runtime\upgrade\<customer-id>\cmdbview\classmodel**.

  ➤ Could not upgrade view <name>. The views can be found under **C:\hp\UCMDB\UCMDBServer\runtime\upgrade\<customer-id>\cmdbview\unupgradeable**.

  ➤ About to copy unchanged BacViews. The views can be found under **C:\hp\UCMDB\UCMDBServer\runtime\upgrade\<customer-id>\bacviews\classmodel**.

➤ Report upgrade:

   ➤ About to upgrade report <name> structure.

   ➤ Upgrading report <name> with tql name <name>.

   ➤ Report pattern <name> for report <name> was not found. Upgraded pattern is not found on the disk for the current report. If the pattern is not moved to version 9.0x (after the upgrade or as it is) it is located under **C:\hp\UCMDB\UCMDBServer\runtime\upgrade\ <customer-id>\patterns\unupgradeable**, and this message is produced. The report can be found under **C:\hp\UCMDB\ UCMDBServer\runtime\upgrade\<customer-id>\reports\structure**.

   ➤ Report <name> was upgraded to view <name>. Finished upgrading report. The report can be found under **C:\hp\UCMDB\UCMDBServer\runtime\upgrade\<customer-id>\cmdbview\structure**. The class model upgrade is done by the view upgrade.

   ➤ Could not upgrade report structure <name>. Search the reason for the failure in the exception. The report can be found under **C:\hp\UCMDB\UCMDBServer\runtime\upgrade\<customer-id>\reports\unupgradeable**.

Upgrade Data

Note: Resources only upgrade.

Executes SQL statements from **C:\hp\UCMDB\UCMDBServer\runtime\data-upgrade-script.sql**, reads data from the old data tables and the **TEMP** tables, performs the required transformation, and populates the new data tables (CDM tables) with the upgraded data.

Note: This step doubles the space consumed by the CMDB. After upgrade finishes, this space is released.

Is Critical (Y/N)	Can Be Rerun (Y/N)
Y	N

Implications of Failure

Data in database is not upgraded.

Log Files

None.

Create Temporary Removed CIs Table

Creates new temporary table in the CDMB database named **UPGRADE_REMOVED_ELEMENTS** to hold the IDs and types of all objects removed during the upgrade (were not copied from old to new data tables) to be used by subsequent steps.

Is Critical (Y/N)	Can Be Rerun (Y/N)
Y	Y

Implications of Failure

Failure means that the Upgrade List Attribute Table and Handle non-Consistent Data steps cannot be executed.

Log Files

None.

Populate Root Table

Note: Resources only upgrade.

Copies upgraded relevant attribute values from leaf data tables to the root table (CDM ROOT).

Is Critical (Y/N)	Can Be Rerun (Y/N)
Y	N

Implications of Failure

The root table would not be populated and all CIs would not exist in the UCMDB. Failure is equivalent for deleting all the data from the UCMBD. To recover, start the upgrade procedure from the beginning.

Log Files

None.

Upgrade List Attribute Table

Note: Resources only upgrade.

Upgrade attributes of type list which are stored in a separate table.

Is Critical (Y/N)	Can Be Rerun (Y/N)
Y	N

Implications of Failure

All attributes of type **list** have wrong values.

Log Files

None.

Delete Legacy Configuration Tables

Note: Resources only upgrade.

Removes tables no longer needed in CMDB.

Is Critical (Y/N)	Can Be Rerun (Y/N)
N	Y

Implications of Failure

The tables that are meant to be deleted remain in the CMDB schema, but do not disrupt the normal behavior of the UCMDB. It is possible to manually remove these tables.

Log Files

None.

Upgrade History DB

Upgrade History database. History database may hold huge amounts of data. During this step we keep reference to the last upgraded data so in case of failure the upgrade continues from the point that it stops.

Is Critical (Y/N)	Can Be Rerun (Y/N)
Y	Y

Implications of Failure

This step can be re-run multiple times and can recover from failure using designated recovery files, located below the **C:\hp\UCMDB\UCMDBServer\runtime\upgrade** folder. Each file contains the status of a sub-step; together they hold the status of the entire history upgrade. File names are:

➤ **recovery_for_history_cleanup.txt**

➤ **recovery_for_history_class_remove_upgrader.txt**

➤ **recovery_for_history_attribute_remove_upgrader.txt**

➤ **recovery_for_history_attribute_rename_upgrader.txt**

➤ **recovery_for_history_class_rename_upgrader.txt**

➤ **recovery_for_history_snapshot_upgrader.txt**

Skipping this step results in a loss of historical data and requires creating a new history schema via the Configuration wizard.

Log Files

➤ General log messages:

  ➤ History DB upgrader failed, but is not failing upgrade process… On failure.

  ➤ INFO - <step name> is upgrading chunk <current chunk number> out of <total number of chunks>. Progress report message.

  ➤ No upgrade is needed. Upgrade was finished in the previous upgrade. This is not the first time the History database was run. In the previous time, the upgrade finished successfully.

  ➤ <step-name> is upgrading chunk <number> out of <number>. Specify the progress for each step of the upgrade.

  ➤ Executing SQL statement on attributes between event id <number> and <number>. Statement: <SQL-statement>. Perform update or remove attributes of specific type (specified in the SQL-statement).

  ➤ old Class <name> has history attributes of types <list-of-names>. For each class that needs to be removed /updated, list all the attribute types that needs handling.

➤ Create auxiliary tables for History DB upgrade. This is a pre-upgrade step for collecting relevant data:

  ➤ The history DB has <number> events. Information message with number of history events currently held in the History database.

  ➤ The Chunk between rows <number> and <number>, translate to events IDs between <number> and <number>. Each chunk works on a range of rows in the History database, which is translated to a SQL statement for a range of history events IDs.

➤ Collect non-history data from the history DB. We perform cleaning operations on the History database to clean it from non-existing or non-history class model elements. This step collects the relevant data, to be handled later on.

  ➤ Recover cleanup data from file <name>. The upgrade was run before. Relevant data for cleaning the schema was collected before and available in the file.

  ➤ Collect data from table for type <name>. Cleaning data is collected separately for each attribute type.

  ➤ Class <name>, attribute <name> is monitored in history DB. List all the attributes for each class in the class model that has entry in the History database.

  ➤ Summary of all collect data from History DB. The following log messages contain the collected data grouped by class name.

  ➤ Class <name>, attributes [<list-of-names>] are monitored in history DB. Lists again all attributes for all classes that has entries in the History database, grouped by class name.

  ➤ Cleanup problems found in the history DB. The following log messages specify all the data that needs to be removed from the History database, because it is inconsistent with the class model.

    ➤ Class <name> exists in history DB but not in class model. The class will be removed from the history DB.

    ➤ Link Class <name> is not marked as monitored for change. The class will be removed from the history DB. (Link classes must have the qualifier TRACK_LINK_CHANGES to be monitored)

➤ Attribute <name> in Class <name> exists in history DB but not in class model. The attribute will be removed from the history DB.

➤ Attribute <name> in Class <name> exists in history DB but not marked as monitored for change. The attribute will be removed from the history DB.

➤ Class <name> has no attributes marked as monitored for change. The class will be removed from the history DB.

➤ Get colliding rules. In case of attribute merge that needs to be done as part of the changes in the class model, we need to identify those attributes, and handle them.

➤ Skipped - Attribute name: <name> Class name: <name> was not found in old ClassModel. Non-meaningful log message.

➤ Classes <list-of-names> have history qualifiers. These classes have attributes that can potentially be merged. The next stage verifies this.

➤ Classes <list-of-names> has renamed attributes with CopyAttributeFromAttribute. Those classes has attributes that were the data source for the data of the merged attributes.

➤ Add remove data to configuration for merge rules:

Attribute <name> in Class <name> has colliding renaming rules. This attribute has at least two attribute in the old class model that are mapped to it.

Attribute <name> in Class <name> will receive its value from <old-attribute-name>. Determine the data source of the attribute.

Attribute <name> in Class <name> has more than one rename (including alias) without copyAttributeFromAttribute rule. All merged attributes are not defined as the data source for the new attribute. Select one old attribute arbitrarily as the data source.

In class <name> the following attributes will be removed because of merging: <list-of-old-attribute-names>. Summary of all attribute per class to be removed as a result of the merging.

➤ Removes history events that contain removed class model classes. This step finds all classes that need to be removed from the History database.

   ➤ Class remove rule: oldClassName (object) = <name>

   ➤ Class remove rule: oldClassName (link) = <name>

   ➤ Class remove rule: oldClassName (cleanup) = <name>. The rule was created in the cleaning stage.

   ➤ Executing SQL statement for remove class between event id <number> and <number>. Statement: < SQL-statement>. Perform remove classes in the current chunk

➤ Removes history events that contain removed class model attributes. This step finds all attributes that need to be removed from the History database.

   ➤ Attribute remove rule: oldClassName = <name>, oldAttributeName <name>, attribute type = <name>

   ➤ Attribute remove rule (cleanup): oldClassName = <name>, oldAttributeName <name>, attribute type = <name>. The rule was created in the cleaning stage.

➤ Upgrades records that contain renamed class model attributes. This step finds all attributes that need to be renamed in the History database.

   ➤ Attribute rename rule: oldClassName = <name>, oldAttributeName <name>, new attribute name = <name>, attribute type = <name>

➤ Upgrades records that contain renamed class model classes. This step finds all classes that need to be renamed in the History database.

   ➤ Class rename rule: oldClassName (object) = <name> new class name = <name>

   ➤ Class rename rule: oldClassName (object) = <name> new class name = <name>

   ➤ Executing SQL statement for rename class between event id <number> and <number>. Statement: <SQL-statement>

➤ Upgrades records that contain snapshot result. This step finds all snapshots that need to be upgraded in the History database.

　➤ Executing SQL statement on snapshots between event id <number>

　➤ ExecuteBatch for snapshot is done in seconds

Handle Non-Consistent Data

Note: An OutOfMemoryError exception might occur if there are around 20 million CIs, and at least one of the CI types contains approximately 5 million instances.

In this case, we recommend increasing the amount of memory allocated to the JVM heap space using the parameter **-Xmx** in the **upgrade.bat** file in the **\UCMDBServer\tools** directory.

The default value is 4GB, and you can increase it according to your system's capabilities. However, if you change this parameter, it is also recommended that you change the parameter **-XX:MaxNewSize**. The ratio between these two parameters should be 4:1.

This recommendation can be also applied in other steps or other cases, in which the OutOfMemoryError exception occurs. However, since increasing the amount of memory allocated to the JVM heap space might cause other problems, the general recommendation in such a case is to call HP software support to supply the **dump file java_pidnnn.hprof**, which should appear in the **\UCMDBServer\tools** directory.

Handle non-consistent data performs the following:

➤ Removes links where one of their end objects is removed during the upgrade.

➤ Performs recursive delete if necessary.

➤ Recalculates the value for attributes defined as calculated-attributes for all objects and links.

Is Critical (Y/N)	Can Be Rerun (Y/N)
N	Y

Implications of Failure

The data is inconsistent, which can affect values of attributes that are calculated. Running the Database Consistency Tool after the upgrade is finished removes links only if one of their end objects is missing.

Log Files

The following log messages appear in the upgrade short log:

➤ Found x objects/links that were removed during upgrade. The number of objects and links removed during the upgrade.

➤ Found x dangling links. The number of dangling links being removed.

➤ Found x recursive-delete objects. The number of objects being removed due to recursive-delete.

➤ Updating calculated attributes for type CLASS_NAME (x instances, y bulks). Row for each type of object/link for attribute-recalculation is being performed.

Recalculate Non-Random Generated IDs

Note: Resources only upgrade.

Recalculates IDs for all objects for which the IDs are not random but rather being calculated as a function of their type and key properties.

Is Critical (Y/N)	Can Be Rerun (Y/N)
Y	Y

Log Files

None

Populate Global ID

Note: Resources only upgrade.

Standalone UCMDB functions as a CMS and requires for each CI to have a global ID. This step populates the global ID column in root data table.

Is Critical (Y/N)	Can Be Rerun (Y/N)
N	Y

Implications of Failure

Might cause the CIs not to have a global id. This can be a significant problem when using integrations or complex deployments of UCMDB.

Workaround. The Multiple CMDB Instances Services can be used after the upgrade to fix this issue:

➤ If a global id generator server is needed, you will need to make it a non global id and then make it a global id generator.

➤ If a non global id generator server is needed, you will need to make it a global id generator and then make it a non global id generator.

Log Files

None.

Discovery – Upgrade Configuration

Note: Resources only upgrade.

Recalculates IDs for DFM configuration CIs.

Is Critical (Y/N)	Can Be Rerun (Y/N)
Y	N

Implications of Failure

Discovery may not function at all. If you skip this step, you must perform the following:

1 Disable the Three Upgraders

2 Export user packages from the previous CMDB.

3 Upgrade all packages manually through the Packages Migration tool. For details, see "Upgrading Packages from Version 8.0x (8.04 and Higher) to 9.04" on page 267.

4 Before the upgrade process, remove the following instances of discovery configuration CIs from the CMDB:

> ➤ domain

> ➤ discoveryjob

> ➤ discoverymodule

> ➤ cmdbclass

> ➤ discoverypattern

> ➤ discoverywizard

> ➤ discoveryprobegateway

> ➤ discoveryprobemanager

> ➤ discoveryresource

> ➤ discoverytql

> ➤ triggers

> ➤ management

5 After the upgrade process, import the upgraded packages.

Log Files

➤ Starting upgrade Discovery Configuration CIs.

➤ Upgrade Discovery Configuration CIs was successfully finished!

➤ Failed to upgrade some Discovery Configuration CIs.

➤ About to get discovery configuration CIs and links from server.

➤ Finish getting discovery configuration CIs and links from server. Load instances of discovery configuration CIs from CMDB.

➤ About to remove old Discovery Configuration CIs.

➤ Finish removing old Discovery Configuration CIs. Remove old CIs from CMDB. CIs now exist in the cache only. Failure in this step might cause data loss.

➤ About to update discovery configuration CIs.

➤ Finish updating [amount of CIs] discovery configuration CIs. Update the CIs and save in CMDB.

➤ Failed to add CI [new CI id, CI type], (old CI [old CI id]) skipped. A specific CI failed to be updated in schema. For more details, check error log.

➤ About to update links related to discovery configuration CIs.

➤ Finish updating links related to discovery configuration CIs. Recreating links between CIs. Failure in this step might cause data to be inconsistent.

Federation – Remove old Configuration

Removes old Federation configuration data (new configuration is being deployed).

Is Critical (Y/N)	Can Be Rerun (Y/N)
Y	Y

Implications of Failure

May cause Federation or replication not to work.

Workaround. Use the JMX **deleteByClassType** operation (in Model Services) to remove all instances of the **fcmdb_configuration** CIT. For details on working with the JMX Console, see .

Log Files

For log messages, see the **cmdb.model.audit.short.log** and **cmdb.model.audit.detailed.appender** log files.

Redeploy Basic Packages

Note: Resources only upgrade.

Deploys the CMDB factory packages. Class model updates in this step are restricted to additions only so the factory packages do not remove user-added attributes.

Is Critical (Y/N)	Can Be Rerun (Y/N)
N	Y

Implications of Failure

In case of failure, it is possible to redeploy these packages from the UCMDB itself. However, any addition made by the user to these classes could possibly be lost in the redeploy.

Log Files

For log messages, see the **mam.packaging.log** log file.

Validate Upgraded Class Model

Note: Resources only upgrade.

Validates that upgraded class model is BDM- and CMS-compliant by comparing it with an out-of-the-box 9.04 class model. Missing class model entities are being added.

The class model existing in the database before this step (upgraded + packages) is written to **C:\hp\UCMDB\UCMDBServer\runtime\upgraded-after-packages-class-model.xml**. The updated class model is written to **C:\hp\UCMDB\UCMDBServer\runtime\upgraded-fixed-after-packages-class-model.xml**.

If the class model is changed during this step, it is updated back to the database.

Is Critical (Y/N)	Can Be Rerun (Y/N)
N	Y

Implications of Failure

Failure in this stage does not fail the entire upgrade process. However, it should be taken seriously, since the failure means that the user class model is incomplete and not CMS and Business Service Management compliant.

Log Files

For details, see "Validate Class Model" on page 203.

Discovery – Upgrade Statistics

Renames CI types in the **CCM_DISCOVERY_STATS** table in the CMDB (discovery history information).

Is Critical (Y/N)	Can Be Rerun (Y/N)
N	Y

Implications of Failure

Statistic information of previous discovery executions is lost. Skipping this step would require the user to truncate **CCM_DISCOVERY_STATS** table in the CMDB.

Log Files

➤ Starting upgrade CCM_DISCOVERY_STATS table.

➤ Upgrade 'CCM_DISCOVERY_STATS' table was successfully finished!

➤ Failed to upgrade 'CCM_DISCOVERY_STATS' table.

➤ Ci type [old CI type] has been upgraded to [new CI type]. Indicates that and old CI type has been renamed to new CI type.

➤ failed to update [Old CI type], skipped. Indicates that a CI type could not be changed according to new schema. It might be caused due to data inconsistency in the CMDB or that the wrong CI type was defined by the user. Does not affect the discovery, however the row in the statistics panel relating to this CI appears in red.

Discovery – Upgrade Resources

Note: Resources only upgrade.

Upgrades discovery resources: patterns, jobs, and modules (discovery configuration data).

Is Critical (Y/N)	Can Be Rerun (Y/N)
Y	Y

Implications of Failure

Same as the step for "Discovery – Upgrade Configuration" on page 246.

Log Files

➤ Starting upgrade discovery resources.

➤ Upgrade discovery resources have been successfully finished!

➤ Upgrade discovery resources have been finished. Failed to upgrade the following resources: [resource name1], [resource name2], …

➤ File containing resources to filter, upgrade/filtered_resources.xml, not found. Cannot find file which holds the list of resources to remove during the upgrade, no resources would be removed.

➤ Resource [resource name] of type [subsystem] was successfully updated. Indicates that the resource was successfully upgraded.

➤ Failed to upgrade res [resource name] of type [subsystem]/ The resource might be already compatible with new schema. Please check resource manually. Resource was not upgraded. Please check resource manually after CMDB starts. In most cases, such errors follow after another log message with more details.

Load Upgraded Resources

Note: Resources only upgrade.

Loads the upgraded resources created in the previous step "Discovery – Upgrade Resources" on page 251 from the disk to the database.

Note: Upgraded resources from the factory packages take precedence over user resources. This means that if the same resource (name and type) exists in both the factory packages and the upgraded resources folder, the final version is the one from the factory packages.

Is Critical (Y/N)	Can Be Rerun (Y/N)
Y	Y

Implications of Failure

The upgraded resources are not loaded onto the database. The factory resources are already in the database, as a result of the step "Redeploy Basic Packages" on page 249. Only the user resources are missing from the database.

Log Files

➤ got <count> <type> from disk. Specifies the number of resources for each type retrieved from the disk. The message is followed by list of those resources.

➤ Could not get resources map - all resources will be deployed from disk. The factory packages that have been deployed to the database cannot be retrieved. The factory resources cannot take precedence over the user resources, so all the user resources are loaded into the database, and overwrite the factory resources with the same name and type.

➤ did not success to add business view enrichment <name>. Look for the problem description in the attached exception.

➤ did not success to add gold master definition <name>. Look for the problem description in the attached exception.

➤ Resource <name> does not exist in CMDB and should be added. The resource is a user resource and is loaded into the database.

➤ Resource <name> could not be loaded because of missing dependencies: <list-of-names>. The resource cannot be loaded into the database since other resources that it needs do not exist in the database. After the upgrade is finished, it is possible to re-run this step to load these resources.

➤ Upgraded resource <name> and out-of-the-box resource are the same, not loading upgraded resource. The factory resource was not changed by the user.

➤ Upgraded resource <name> is not loaded since a different out-of-the-box resource with the same type and name already exists. The user changed the factory resource, and is going to lose the changes he/she made.

➤ Failed to add <type> <name>. The resource of the specific type was not loaded.

Upgrade Snapshots

Upgrade snapshot data is stored in the CMDB.

Is Critical (Y/N)	Can Be Rerun (Y/N)
N	Y

Log Files

None.

Discovery – Re-Encrypt Domain Scope Document

Note: Resources only upgrade.

Re-encrypts the **domainScopeDocument** file from DES encryption (used in 8.0x) to AES encryption.

Is Critical (Y/N)	Can Be Rerun (Y/N)
N	Y

Implications of Failure

Discovery might not function at all. Skipping this step requires that you do the following:

1 Export the **domainScopeDocument** file from the old CMDB.

2 After the upgrade process, import the **domainScopeDocument** file. For details, see "Export and Import Credential and Range Information in Encrypted Format" on page 344.

Log Files

➤ Upgrade process of DomainScopeDocument re-encryption to AES had been started.

➤ Upgrade process of DomainScopeDocument re-encryption to AES had been finished successfully.

➤ Upgrade process of DomainScopeDocument re-encryption to AES had been failed.

➤ DSD is empty - doing nothing... Indicates that the **domainScopeDocument** file is empty and therefore this step is redundant and will not do anything.

➤ The DSD already encrypted by AES - doing nothing… Indicates that the **domainScopeDocument** file is already encrypted by AES; the step is redundant and will not do anything.

➤ The DSD is encrypted by 3DES... Indicates that the **domainScopeDocument** file is encrypted by 3DES, therefore it is re-encrypted by AES.

➤ Failed to decrypt DSD by 3DES. Indicates that the encryption process of the **domainScopeDocument** file failed (this step failed to re-encrypt the **domainScopeDocument** file by AES); you need to import the **domainScopeDocument** file to the UCMDB system after the upgrade process.

➤ Failed to encrypt DSD by AES. The step failed. You need to import the **domainScopeDocument** file to the UCMDB system after the upgrade process.

➤ Got empty DSD after AES encryption. The step failed. You need to import the **domainScopeDocument** file to UCMDB system after the upgrade process.

➤ Got empty DSD after 3DES decryption. The step failed. You need to import the **domainScopeDocument** file to UCMDB system after the upgrade process.

➤ Failed to decrypt the DSD by AES and 3DES. The step failed. You need to import the **domainScopeDocument** file to UCMDB system after the upgrade process.

Discovery – Upgrade Domain Scope Document

Note: Resources only upgrade.

Renames CI types and attributes in the **domainScopeDocument** file.

Is Critical (Y/N)	Can Be Rerun (Y/N)
N	Y

Implications of Failure

See "Discovery – Re-Encrypt Domain Scope Document" on page 254.

Log Files

➤ Upgrade process of DomainScopeDocument data has been started

➤ DomainScopeDocument data has been successfully upgraded

➤ Failed to upgrade DomainScopeDocument data

Discovery – Copy Credentials to Confidential Manager

Note: Resources only upgrade.

Extracts credentials information from the **domainScopeDocument** file to the Confidential Manager. Credentials information in the **domainScopeDocument** file are replaced by Confidential Manager identifiers. For details, see "Confidential Manager" on page 397.

Is Critical (Y/N)	Can Be Rerun (Y/N)
N	Y

Implications of Failure

Same as for the step "Discovery – Re-Encrypt Domain Scope Document" on page 254.

Log Files

➤ Upgrade process of DomainScopeDocument insertion to Confidential Manager had been started

➤ Upgrade process of DomainScopeDocument insertion to Confidential Manager had been finished successfully

➤ Upgrade process of DomainScopeDocument insertion to Confidential Manager had been failed

Discovery – Upgrade Credential Identifiers

Note: Resources only upgrade.

Upgrade **credential_id** attribute over the CIs in the CMDB to match the confidential manager identifiers.

Is Critical (Y/N)	Can Be Rerun (Y/N)
N	Y

Implications of Failure

Credential attribute of existing CIs contains wrong data. Skipping this step would require you to run massive discovery to reconstruct the data.

Log Files

➤ Upgrade process of credentials_id's update had been started.

➤ Upgrade process of credentials_id's update had been finished successfully.

➤ Upgrade process of credentials_id's update had been failed.

➤ Failed to get layout (and update credentials id) for object of type <type>. Indicates that the upgrade process for type <type> failed, meaning that the CIs of type <type> might contain obsolete credentials ids. After the upgrade process is done, need to re-run massive discovery on the system.

Copy Report Configuration

Note: Resources only upgrade.

Copies reports configuration from Foundation database to new Management database.

Is Critical (Y/N)	Can Be Rerun (Y/N)
N	Y

Implications of Failure

Favorite filters from 8.0x are not upgraded and their scheduling is not available.

Log Files

➤ failed to upgrade report: <report name>.

Copy Snapshots Scheduling Information

Note: Resources only upgrade.

Copies snapshots scheduling data from Foundation database to new Management tables in the CMDB. Also, removes scheduled jobs of types which are no longer relevant (run TQL, rebuild views and package deploy).

Is Critical (Y/N)	Can Be Rerun (Y/N)
N	Y

Implications of Failure

Scheduled snapshots are not upgraded and you must redefine them.

Log Files

➤ Failed to handle schedulerJob [<schedulerJob.toString()>] .

Upgrade Settings

Note: Resources only upgrade.

Rename CI types in selected settings.

Is Critical (Y/N)	Can Be Rerun (Y/N)
N	Y

Implications of Failure

If class names existed in the settings manager and their name was changed by class model upgrader, you may encounter odd application behavior depending on the setting.

Example: Root CIT and its relationship is defined. Additional setting is frontend URL. If a load balancer is defined, you may need to redefine the frontend URL. Reverse proxy settings are not affected.

Log Files

➤ SettingsClassModelUpgrader failed or a specific one with the prefix failed to upgrade.

Upgrade Security Model

Note: Resources only upgrade.

Upgrades permissions according to the new ACL Model.

Is Critical (Y/N)	Can Be Rerun (Y/N)
N	Y

Implications of Failure

Some permissions are aligned with new ACL model but some are not. Administrators must access Security Manager and verify that all permissions are as required and, if not, set accordingly.

Log Files

➤ Role [<role name>] failed to get permissions due to the following error:…

Clear Old Data

Note: Resources only upgrade.

Removes old data tables (TEMP tables).

Is Critical (Y/N)	Can Be Rerun (Y/N)
N	Y

Implications of Failure

The UCMDB works correctly, but could be slower due to garbage left in those tables. It is possible to manually remove all the tables with the prefix **TEMP**.

Log Files

None.

User vs. Factory

Note: Resources only upgrade.

Comparing upgraded class model to an out-of-the-box class model to decide for each class model entity whether it is a user's entity or a factory's entity.

Is Critical (Y/N)	Can Be Rerun (Y/N)
N	Y

Implications of Failure

All class model entities are marked as factory entities. Certain operations on the class model are closed for user over factory entities.

Log Files

The following messages alert to problems in the data model. The entity specified in the message is a factory entity that is missing in the user class model. This may suggest a previous problem in the deployment of Content Pack 8.00 or in the upgrade process.

The affected steps may be one or more of the following:

➤ "Validate Class Model" on page 203.

➤ "Upgrade Class Model on Disk" on page 207.

➤ "Upgrade Class Model in DB" on page 230.

➤ "Redeploy Basic Packages" on page 249.

➤ "Validate Upgraded Class Model" on page 249.

➤ !!! Class <name> doesn't exist in the upgraded class model.

➤ !!! Class <name> is missing qualifiers in the upgraded class model. The qualifiers are: <list-of-names>.

➤ !!! Attribute <name> in Class <name> is missing from the upgraded class model.

➤ !!! Attribute <name> in Class <name> is missing qualifiers in the upgraded class model. The qualifiers are: <list-of-names>.

➤ !!! Attribute Override <name> was removed in Class <name> and is missing qualifiers in the upgraded class model. The qualifiers are: <list-of-names>.

➤ !!! Attribute Override <name> in Class <name> is missing qualifiers in the upgraded class model. The qualifiers are: <list-of-names>.

➤ !!! Class <name> is missing method <name> in the upgraded class model.

➤ !!! Method <name> in Class <name> is missing qualifiers in the upgraded class model. The qualifiers are: <list-of-names>.

➤ !!! Valid Link <name> is missing in the upgraded class model.

➤ !!! Valid Link <name> is missing qualifiers in the upgraded class model. The qualifiers are <list-of-names>.

➤ !!! Calculated Link <name> with Class <name> is missing in the upgraded class model.

➤ !!! Calculated Link <name> with Class <name> is missing triplet in the upgraded class model. The triplet is <triplet>.

➤ !!! Enum <name> doesn't exist in the upgraded class model.

➤ !!! List <name> doesn't exist in the upgraded class model.

➤ !!! Enum entry with key <number> and value <value> in Enum <name> doesn't exist in the upgraded class model.

➤ !!! List entry <value> in List <name> doesn't exist in the upgraded class model.

Populate IPv6 Attribute

Copies the IP value from the name attribute to the new IpAddressValue attribute in the IpAddress class in IPv6 normalized form.

Is Critical (Y/N)	Can Be Rerun (Y/N)
Y	Y

Implications of Failure

Discovery might not work.

Workaround. An update should be done on IPs and IP subnet in the CMDB. The update can be done manually from the UI (one at a time).

Log Files

For log messages, see the **cmdb.reconciliation.log** log file.

Enrichment Driven Upgrade

Invokes predefined enrichments to update data as part of the upgrade process.

1. Update name attribute at J2EE Domain to remove suffix (all characters after '@').

2. Update name attribute at Cluster Resource Group, fill it with the suffix from the value of its host key attribute (all characters after ':').

3. Removes old report archive CIs which are not being upgraded.

Is Critical (Y/N)	Can Be Rerun (Y/N)
N	Y

Define Key Attributes Reconciliation Rules

Note: Resources only upgrade.

Adds a reconciliation rule of type 'key-attributes' to any user's CI type with key attributes.

Is Critical (Y/N)	Can Be Rerun (Y/N)
N	Y

Implications of Failure

A user defined CIT that was identified by key attributes in 8.00 uses its parent reconciliation rule.

The key attribute identification rule can be added later on from a package/reconciliation JMX.

Log Files

None.

Package Manager Upgrade

Note: Resources only upgrade.

Updates packaging information stored in the UCMDB server model.

The configuration file of the Package Manager Upgrade is stored in **C:\hp\UCMDB\UCMDBServer\runtime\upgrade\PackageManagerUpgrader\config.xml** (**cmdb.jar**). The configuration lists obsolete subsystems and the subsystem rename rules.

The Package Manager Upgrade tool performs the following steps:

1 Removes resources of obsolete subsystems from packages

2 Renames old subsystem names to the new ones

3 Updates the names of the class model resources used by Package Manager

   a Changes class names in class definitions

   b Changes class names in the definitions of valid links

   c Changes class names in the triplets of the calculate link definitions

4 Removes non-existing resources from packages

Is Critical (Y/N)	Can Be Rerun (Y/N)
N	Y

Implications of Failure

Incorrect packaging information may cause creation of incorrect package files during package export and may cause failures when trying to undeploy a package.

Log Files

None.

15

Upgrading Packages from Version 8.0x (8.04 and Higher) to 9.04

This chapter includes:

Concepts

➤ Package Migration Utility – Overview on page 268

Tasks

➤ Migrate a Custom Package on page 269

Reference

Troubleshooting and Limitations on page 271

Concepts

⚙ Package Migration Utility – Overview

This chapter explains how to use the package migration utility to migrate custom packages in HP Universal CMDB (UCMDB) from version 8.0x (8.04 or higher) to version 9.04.

Custom packages created before upgrading the system to version 9.04 may contain resources that are not supported in the new version. To reduce the risk of problems in such custom packages, it is recommended that you migrate these packages offline using the provided Package Migration Utility before deploying the packages in the UCMDB version 9.04 system.

Using the Package Migration Utility to migrate custom packages offline provides the following benefits:

➤ No downtime is required.

➤ Migration of custom packages can be completed before they are deployed in the system, thereby reducing risk.

➤ You can migrate your packages, then immediately deploy them and rediscover the data.

➤ HP content packages can be migrated in a single process, reducing the risk of corrupted content.

The Package Migration Utility enables you to perform the migration on custom packages offline, without the need for a running server.

Tasks

🔧 Migrate a Custom Package

The following procedure explains how to migrate custom packages to HP Universal CMDB version 9.04.

To migrate custom packages:

1 Place the custom packages to be migrated in a separate directory together with the packages on which the upgraded resources depend. For example:

   ➤ If a custom package contains a view or enrichment rule which relies on a TQL definition that resides in another package, place the package containing the TQL definition in the directory with the custom package.

   ➤ If a custom package has a reference to a custom class definition which is not supplied by any of the factory packages, place the package with the custom class definition in the directory with the custom package.

2 Ensure that you have the old class model definition XML files, that is, the class model of the UCMDB version (such as 7.0 or 7.5) with which your package was created.

   To create the class model, access the JMX console, navigate to **CMDB Class Model Services** and run the **exportClassModelToXML** method.

3 Run the script:

   ➤ Windows: **C:\hp\UCMDB\UCMDBServer\tools\packupgrade.bat**

   ➤ Linux: **opt/hp/UCMDB/UCMDBServer/tools/packupgrade.sh**

   The syntax for running the script is shown below. (This information can also be displayed by running the script without arguments.)

```
packupgrade -cm {CLASS_MODEL_DEF_FILE} [-u {UPGRADE_CONFIG_FILE}] [-
exclude <package(s)>] -out {OUTPUT_DIR} {INPUT_DIR}
```

   -i. Login to the JMX console.

-cm {CLASS_MODEL_DEF_FILE}. File name of the old class model definition; this file can be created via JMX: navigate to the **Class Model Services** in the JMX console and invoke the **exportClassModelToXml** method.

-u {UPGRADE_CONFIG_FILE}. The upgrade configuration file.

-exclude {package(s)}. The package to exclude or the list of package names to be excluded, separated with commas.

-filterResources {file path of filtered resources list}. Exclude resources listed in the given XML file (the XML file should conform to the **schema\filtered_resources.xsd** file).

-fullCM. Changes the class model upgrade to **full mode**. In full mode, new packages are created and the class model is treated as a whole, enabling more validations and corrections. In full mode, the packages cover the entire out-of-the-box class model (at least). By default, upgrade is done in **partial mode** which does not assume completeness.

-analyzeDataActions {DATA_ACTIONS_FILE}. Analyzes the changes and generates the data actions analysis file with the given file name. Implies -fullCM.

-outputFullCM {OUTPUT_FULL_CM_FILE}. Outputs the new full class model to a file. Implies -**fullCM**.

-out {OUTPUT_DIR}. Directory path for upgraded packages.

-doNotCreateNewPackages. If this option is given, the upgrader does not create any new package file.

{INPUT_DIR}. The directory path of the packages to be upgraded.

Environment variables. **ucmdb.home**. Must point to the product directory (usually **C:\hp\UCMDB\UCMDBServer** for standalone UCMDB).

4 Locate the migrated packages in the output directory you provided. Deploy your migrated packages in the UCMDB version 9.04 system.

Reference

🔍 Troubleshooting and Limitations

➤ The Package Migration Utility has been verified only for packages compatible with UCMDB 8.0x (8.04 or higher).

➤ Enrichment definition packages that refer to deleted or updated CI types cannot be updated using the Package Migration Utility.

➤ Partial migration is not supported. The Package Migration Utility does not create a new package if one or more of the resources cannot be migrated successfully.

Part V

High Availability and Capacity Planning

16

High Availability Mode Installation

This chapter includes:

Concepts

➤ Best Practices for the HP Universal CMDB High Availability Solution on page 276

➤ Tasks on page 278

➤ Transitions Between the Active and Passive Servers on page 277

Tasks

➤ Install HP Universal CMDB in High Availability Mode on page 278

➤ Configure Network High Availability on page 283

➤ Configure Full Site on page 284

Concepts

♣ Best Practices for the HP Universal CMDB High Availability Solution

This section outlines best practices for field implementation of the HP Universal CMDB High Availability solution.

Solution diagram:

➤ All external access to the HP Universal CMDB application is made via the load balancer.

➤ Two or more Servers are configured.

➤ HP Universal CMDB services run on all the Servers in the cluster, but the customer components are active on the active Server only.

➤ Load balancer with:

> ➤ Keep alive to **http://<UCMDB-Server:port>/ping?clusterId=<clusterId>.**

> ➤ Round robin policy for the Servers.

> ➤ Session stickiness is maintained.

> ➤ Virtual IP is configured per cluster.

➤ Each Server is connected to two separate networks:

> ➤ Front-end (for load balancer access)

> ➤ Back-end (for database and High Availability Controller communication)

Transitions Between the Active and Passive Servers

To improve start up times for the passive machines during a transition from the active machine, HP Universal CMDB starts the passive machines in partial mode.

In this case, the Model Topology component on the passive machines is started in read-only mode. Then it is synchronized with the changes occurring on the active Server, by the UCMDB database, every few seconds.

When the passive machine takes over, it starts up quickly because most of the model is already loaded to memory.

Tasks

🔧 Install HP Universal CMDB in High Availability Mode

This section describes the installation, startup, and configuration procedures when HP Universal CMDB is run in high availability mode.

Note:

➤ When upgrading to a new service pack version and working in high availability mode, perform the following steps:
- Stop all the servers in the cluster.
- Upgrade all the servers to the new service pack version.
- First start one server until it gets an Up status.
- Then start the rest of the servers.

➤ High Availability mode is not supported in a multiple-customer environment.

This section includes the following topics:

➤ "Install the Servers" on page 279

➤ "Complete the Server Startup" on page 279

➤ "Configure the Server" on page 281

➤ "Configure the Load Balancer" on page 281

➤ "Configure the Probe" on page 282

1 Install the Servers

a Install the UCMDB Server on two or more machines without running the configuration wizard (select **No** at the wizard prompt). The typical configuration is an **active** Server and a **passive** Server.

For details, see "HP Universal CMDB Installation on a Windows Platform" on page 71 or "HP Universal CMDB Installation on a Linux Platform" on page 87.

Note: The machines used for the active and passive UCMDB Servers should have similar hardware (especially the same amount of memory) and should be running the same operating system.

---

b Run the configuration wizard on the Server that is to be the active Server. Select **Create a new schema**. For details, see "UCMDB Server Configuration" on page 105.

c Run the configuration wizard on the passive Server. Select **Connect to an existing schema** and provide the details of the schema you created for the active Server.

➤ To run the wizard from a Windows platform, select **Start** > **All Programs** > **HP UCMDB** > **Start HP Universal CMDB Server Configuration Wizard**.

➤ To run the wizard from a Linux platform:

```
/opt/hp/UCMDB/UCMDBServer/bin/configure.sh
```

2 Complete the Server Startup

a Start the active Server. Wait until the startup process is complete.

b **For Windows**: Access **server_management.bat** (the Server Management Tool) located in the following folder: **C:\hp\UCMDB\UCMDBServer\tools**.

For Linux: Run **server_management.sh** located in the following folder: **/opt/hp/UCMDB/UCMDBServer/tools/**.

➤ On the login page, enter the Server name and credentials.

If the default SSL port is being used (port **8443**), enter the Server name only (for example, **localhost**).

If the SSL port has been changed, enter the Server name and the new port (for example, **localhost:443**).

Note: When running in High Availability mode, you must log on to the Server Management Tool using the address of the active server.

➤ Enter the user name and password of the system user (the default is **sysadmin** and **sysadmin**).

Note: The connection from the tool to the HP Universal CMDB Server is made through HTTPS. If there is a problem with the connection, make sure that **SSL** mode is configured (**Enable HTTPS connections** should be set to **true**).

---

c In the Server Management Tool, select **Clusters** in the left menu. Click the **New Cluster** button to create a new cluster.

d In the **Add Server** box, enter the machine name of one of the Servers you installed. Click **Add**. Repeat for the other Servers.

Note: High Availability servers should be configured with short server names (not with IP addresses).

---

e In the Server Name list, select the Server that is to be the active Server. Click **Set Active**.

f Click **OK**.

g Answer **Yes** to the question about switching all existing customers to the active Server.

Note: To change user or server, click the **Logout** link to log out of the Server Management tool.

---

h Start the passive Server and run the **server_management.bat** file on that Server.

Note: Database inconsistency can occur when using the Server Management tool to convert a UCMDB Server from active to passive. To prevent this occurring, on the active machine, stop the UCMDB Server. After a short period (about one minute), the passive Server becomes the active Server.

All Servers in a cluster must work on the same port for HTTP, HTTPS, and so on. You cannot configure the two Servers to work on different ports.

---

3 Configure the Server

a Select **Administration** > **Infrastructure Settings** > **General Settings** category.

b Locate and change the following settings:

➤ **Is Frontend URL from settings enabled?** should be set to **True**.

➤ **Frontend URL** should be set to the load balancer's URL. The required format is **URI://<Server name>:<port>**.

4 Configure the Load Balancer

Define the virtual IP for the two HP Universal CMDB Servers with the following configuration:

➤ Select the port defined in Infrastructure Settings.

➤ Verify that the virtual IP is configured per cluster.

➤ The keep alive address for the session is:
   http://<UCMDB-Server:port>/ping?clusterId=<clusterId>. An active
   Server in the cluster returns HTTP response 200 (OK). A passive Server
   returns HTTP response 503 (service unavailable).

➤ Active and Passive are printed to the HTML page when browsing to the
   keepalive page of the active or passive server, respectively.

5 Configure the Probe

a Run the Probe installation on the Probe machine with the load
   balancer virtual IP address as the HP Universal CMDB Server name.

b Start the Probe.

ᴪ Configure Network High Availability

To deploy network high availability, connect load balancers and databases via switches to Servers using spanning tree Intel NIC mode (for Windows).

Full Network Redundancy configuration solution diagram:

⚜ Configure Full Site

➤ The back-end network should be defined on the prime interface (the interface bound to the Server name). If it is not defined this way, edit the etc/hosts file to define the back-end interface as bound to the Server name.

➤ During the Server installation, the back-end hostname/IP should be defined as the HP Universal CMDB Server/IP.

17

HP Universal CMDB Large Capacity Planning

This chapter includes:

Concepts

Tasks

Reference

Concepts

🔷 Large Capacity Planning Overview

Using the default configuration, HP Universal CMDB can work with a deployment of more than 25 million objects and links. To work with a larger deployment, you must implement the following configuration:

➤ Increase the CMDB heap to 8 GB. For details, see "UCMDB Server Configuration" on page 288.

➤ If working with an Oracle database, set up the Oracle Database SGA as follows: 4 GB supported, 8 GB recommended. For details, see "Oracle Database Configuration" on page 289.

The following table displays the maximum supported number of CIs and links for a UCMDB deployment:

Database/Operating System	Windows	Linux
MS SQL Server	40 million CIs and links	12.5 million CIs and links
Oracle	40 million CIs and links (Configuration required as described in this section)	40 million CIs and links (Configuration required as described in this section)

For more details on:

➤ The changes you must make to the system configuration to support this capacity, see "UCMDB Server Configuration" on page 288.

➤ How you can improve performance, see "Oracle Database Configuration" on page 289.

➤ The setup used for capacity testing, see "System Test Setup" on page 290.

➤ Performance results of the system test run on UCMDB 9.04, see "System Test Results" on page 291.

Managed Nodes and Node-Related CIs

When planning capacity, among other issues, you should consider the ratio of managed nodes in your CMDB to node-related CIs. Node-related CIs include all CIs of types which are subclasses of Application Resource, Node Element, or Running Software.

The following table lists the number of node-related CIs you can discover for each managed node in your environment. This number depends on the size of your deployment and the number of managed nodes—the more managed nodes you maintain in the CMDB, the fewer node-related CIs you can discover for each managed node.

For example, in an Enterprise deployment if you are running 89,600 managed nodes, you can discover 160 host-related CIs for each managed host. If you are running only 28,000 managed hosts, you can discover 500 resource CIs for each managed host.

Deployment	Number of Managed Hosts/Host-Related CIs
Enterprise	89600/160 - 28800/500
Standard	9000/160 – 3000/500
Small	4500/160 – 1000/500

Note: The numbers in the table include only CIs and not links.

Tasks

🔧 UCMDB Server Configuration

For the system to support 40 million CIs and links, you should update the following parameters on the UCMDB Server:

Windows:

➤ **C:\hp\UCMDB\UCMDBServer\bin\wrapper-platform.conf**

wrapper.java.initmemory=2048

wrapper.java.maxmemory=8192

➤ **C:\hp\UCMDB\UCMDBServer\conf\settings.override.properties**

dal.object.condition.max.result.size=50000000

dal.use.memory.instead.temp.table.high.threshold.oracle=6000000

dal.joinf.max.result.size=4000000

Linux:

➤ **opt/hp/UCMDB/UCMDBServer/bin/wrapper-platform.conf**

wrapper.java.initmemory=2048

wrapper.java.maxmemory=8192

➤ **opt/hp/UCMDB/UCMDBServer/bin/settings.override.properties**

dal.object.condition.max.result.size=50000000

dal.use.memory.instead.temp.table.high.threshold.oracle=6000000

dal.joinf.max.result.size=4000000

🪝 Oracle Database Configuration

When working on a system containing 40 million objects and links, you can improve performance by increasing the Oracle SGA size from 6 to 8 GB (the recommended configuration). This improves the performance of both the TQL calculation for several types of TQLs, as well as for data-in operations performed on the system.

Reference

🔍 System Test Setup

The system capacity for the system test was 40 million CIs and links.

The following hardware was used for the test:

Role	Machine Type	CPU	Memory	VM/ SWAP	OS + 3rd Party SW
CMDB	HP Proliant BL460c G6	2 x Intel Xeon Processor 2.533 GHz Quad core	16 GB	Windows: 24 GB Linux: 16 GB	Win2008R2 64-bit Red Hat Enterprise Linux Server release 5.5
Data Flow Probe	HP ProLiant DL 140 G2	2 * 3.0 GHz CPU	2 MB	3 MB	Windows 2003 Server EE
Database	HP Proliant BL460c G6	2 x Intel Xeon Processor 2.933 GHz Quad core	32 GB	51 GB	Win2008R2 64-bit REHL 5.4

The following software version was used for the test:

➤ Oracle Database 11g, Release 11.2.0.1.0

The following business flows were tested as part of the system test:

➤ **TQL Calculation**

 TQLs were divided into sub groups according to the result size (<100, <1000, and <10000), according to the data set that the TQL retrieves, and according to the TQL configuration:

➤ Like Condition

➤ Like, Ignore case

➤ Different number of hierarchies in the TQL results (1-5)

➤ Compound

➤ Sub-graph

➤ **Data-in**

The data-in scenario in the system test included insertion, updates, and deletion.

➤ **Enrichments**

Enrichment scenarios included insert, update, and delete.

System Test Results

Following a 24-hour load test, with a scenario that includes query execution, data-in, and enrichment execution, the following results have been achieved:

➤ The system was stable throughout the run. No restarts, memory leaks, or any other degradation over time was observed.

➤ System performance is acceptable.

Part VI

Hardening HP Universal CMDB

18

Introduction to Hardening

This chapter includes:

Concepts

➤ Hardening Overview on page 296

➤ Hardening Preparations on page 297

Tasks

➤ Deploy HP Universal CMDB in a Secure Architecture on page 299

➤ Change System User Name or Password for the JMX Console on page 300

➤ Change the HP Universal CMDB Server Service User on page 301

Concepts

🔗 Hardening Overview

This section introduces the concept of a secure HP Universal CMDB application and discusses the planning and architecture required to implement security. It is highly recommended that you read this section before proceeding to the hardening discussion in the following sections.

HP Universal CMDB is designed so that it can be part of a secure architecture, and can therefore meet the challenge of dealing with the security threats to which it might be exposed.

The hardening guidelines deal with the configuration required to implement a more secure (hardened) HP Universal CMDB.

The hardening information provided is intended primarily for HP Universal CMDB administrators who should familiarize themselves with the hardening settings and recommendations prior to beginning the hardening procedures.

It is highly recommended that you use a reverse proxy with HP Universal CMDB to achieve a secure architecture. For details on configuring a reverse proxy for use with HP Universal CMDB, see "Using a Reverse Proxy" on page 317.

If you must use another type of secure architecture with HP Universal CMDB other than described in this document, contact HP Software Support to determine which architecture is the best one for you to use.

For details on hardening the Data Flow Probe, see "Data Flow Probe Hardening" on page 357.

Important:

➤ The hardening procedures are based on the assumption that you are implementing only the instructions provided in these chapters, and that you are not performing other hardening steps documented elsewhere.

➤ Where the hardening procedures focus on a particular distributed architecture, this does not imply that this is the best architecture to fit your organization's needs.

➤ It is assumed that the procedures included in the following chapters are to be performed on machines dedicated to HP Universal CMDB. Using the machines for other purposes in addition to HP Universal CMDB may yield problematic results.

➤ The hardening information provided in this section is not intended as a guide to making a security risk assessment for your computerized systems.

Hardening Preparations

➤ Evaluate the security risk/security state for your general network, and use the conclusions when deciding how to best integrate HP Universal CMDB into your network.

➤ Develop a good understanding of the HP Universal CMDB technical framework and HP Universal CMDB security capabilities.

➤ Review all the hardening guidelines.

➤ Verify that HP Universal CMDB is fully functioning before starting the hardening procedures.

➤ Follow the hardening procedure steps chronologically in each chapter. For example, if you decide to configure the HP Universal CMDB server to support SSL, read "Enabling Secure Sockets Layer (SSL) Communication" on page 303 and then follow all the instructions chronologically.

➤ HP Universal CMDB does not support basic authentication with blank passwords. Do not use a blank password when setting basic authentication connection parameters.

Tip: Print out the hardening procedures and check them off as you implement them.

Tasks

🔧 Deploy HP Universal CMDB in a Secure Architecture

Several measures are recommended to securely deploy your HP Universal CMDB servers:

➤ **DMZ architecture using a firewall**

The secure architecture referred to in this document is a typical DMZ architecture using a device as a firewall. The basic concept of such an architecture is to create a complete separation, and to avoid direct access between the HP Universal CMDB clients and the HP Universal CMDB server.

➤ **Secure browser**

Internet Explorer and FireFox in a Windows environment must be configured to securely handle Java scripts, applets, and cookies.

➤ **SSL communication protocol**

Secure Sockets Layer protocol secures the connection between the client and the server. URLs that require an SSL connection use a secure version (HTTPS) of the Hypertext Transfer Protocol. For details, see "Enabling Secure Sockets Layer (SSL) Communication" on page 303.

➤ **Reverse proxy architecture**

One of the more secure and recommended solutions suggests deploying HP Universal CMDB using a reverse proxy. HP Universal CMDB fully supports secure reverse proxy architecture. For details, see "Using a Reverse Proxy" on page 317.

Note: When the UCMDB Server is configured to connect with reverse proxy, mutual authentication using SSL between the reverse proxy server and the Data Flow Probe is not supported. For details, see "Enable SSL Between UCMDB Server and Data Flow Probe with Mutual Authentication" on page 362.

⚓ Change System User Name or Password for the JMX Console

The JMX console uses system users, that is, cross-customer users in a multi-customer environment. You can log in to the JMX console with any system user name. The default name and password is **sysadmin**/**sysadmin**.

You change the password either through the JMX console or through the Server Management tool.

To change the default system user name or password through the JMX console:

1 Launch a Web browser and enter the following address: http://localhost.<domain_name>:8080/jmx-console.

2 Enter the JMX console authentication credentials, which by default are:

➤ Login name = **sysadmin**

➤ Password = **sysadmin**

3 Locate **UCMDB:service=Security Services** and click the link to open the Operations page.

4 Locate the **changeSystemUserPassword** operation.

➤ In the **userName** field, enter **sysadmin**.

➤ In the **password** field, enter a new password.

5 Click **Invoke** to save the change.

To change the default system user name or password through the Server Management tool:

1 For **Windows**, run the following file:
   C:\hp\UCMDB\UCMDBServer\tools\server_management.bat.

   For Linux: Run **server_management.sh** located in the following folder:
   /opt/hp/UCMDB/UCMDBServer/tools/.

2 Log in to the tool with the authentication credentials:
   sysadmin/sysadmin.

3 Click the **Users** link.

4 Select the system user and click **Change password for logged-on user**.

5 Enter the old and new passwords and click **OK**.

🔧 Change the HP Universal CMDB Server Service User

On a Windows platform, the HP Universal CMDB service, which runs all HP Universal CMDB services and processes, is installed when you run the Server and Database Configuration utility. By default, this service runs under the local system user. However, you may need to assign a different user to run the service (for example, if you are using NTLM authentication).

The user you assign to run the service must have the following permissions:

➤ sufficient database permissions (as defined by the database administrator)

➤ sufficient network permissions

➤ administrator permissions on the local server

To change the service user:

1 Disable HP Universal CMDB through the Start menu (**Start > All Programs > HP UCMDB > Stop HP Universal CMDB Server**) or by stopping the HP Universal CMDB Server service. For details, see "Start and Stop the HP Universal CMDB Server Service" on page 125.

2 In the Windows **Services** window, double-click **UCMDB_Server**. The **UCMDB_Server Properties (Local Computer)** dialog box opens.

3 Click the **Log On** tab.

4 Select **This account** and browse to choose another user from the list of valid users on the machine.

5 Enter the selected user's Windows password and confirm this password.

6 Click **Apply** to save your settings and **OK** to close the dialog box.

7 Enable HP Universal CMDB through the Start menu (**Start > All Programs > HP UCMDB > Start HP Universal CMDB Server**) or by starting the HP Universal CMDB Server service. For details, see "Start and Stop the HP Universal CMDB Server Service" on page 125.

19

Enabling Secure Sockets Layer (SSL) Communication

This chapter includes:

Tasks

Tasks

🖎 Enable SSL on the Server Machine With a Self-Signed Certificate

These sections explain how to configure HP Universal CMDB to support communication using the Secure Sockets Layer (SSL) channel.

HP Universal CMDB uses Jetty 6.1 as the default Web server.

1 Prerequisites

a Before starting the following procedure, remove the old **server.keystore** located in **C:\hp\UCMDB\UCMDBServer\conf\security\server.keystore**.

b Place the HP Universal CMDB keystore (JKS type) in the **C:\hp\UCMDB\UCMDBServer\conf\security** folder.

2 Generate a Server Keystore

a Create a keystore (JKS type) with a self-signed certificate and matching private key:

➤ From **C:\hp\UCMDB\UCMDBServer\bin\jre\bin**, run the following command:

```
keytool -genkey -alias hpcert -keystore
C:\hp\UCMDB\UCMDBServer\conf\security\server.keystore
```

The console dialog box opens.

➤ Enter the keystore password. If the password has changed, run the **changeKeystorePassword** JMX operation, in **UCMDB:service=Security Services**. If the password has not changed, use the default **hppass** password.

➤ Answer the question, **What is your first and last name?** Enter the HP Universal CMDB Web server name. Enter the other parameters according to your organization.

➤ Enter a key password. The key password MUST be the same as the keystore password.

A JKS keystore is created named **server.keystore** with a server certificate named **hpcert**.

b Export the self-signed certificate to a file:

➤ From **C:\hp\UCMDB\UCMDBServer\bin\jre\bin**, run the following command:

```
keytool -export -alias hpcert -keystore
C:\hp\UCMDB\UCMDBServer\conf\security\server.keystore -storepass <your
password> -file hpcert
```

3 Place the Certificate in the Client's Trusted Store

After generating **server.keystore** and exporting the server certificate, for every client that needs to communicate with HP Universal CMDB over SSL using this self-signed certificate, place this certificate in the client's trusted stores.

Limitation: There can be one server certificate only in **server.keystore**.

---

4 Disable HTTP Port 8080

For details, see "Enable or Disable HTTP/HTTPS Ports" on page 313.

Note: Check that HTTPS communication works before closing the HTTP port.

---

5 Restart the Server

6 Display HP Universal CMDB

To verify that the UCMDB Server is secure, enter the following URL in the Web browser: **https://<UCMDB Server name or IP address>:8443/ ucmdb-ui**.

🖐 Enable SSL on the Server Machine With a Certificate from a Certification Authority

To use a certificate issued by a Certification Authority (CA), the keystore must be in Java format. The following example explains how to format the keystore for a Windows machine.

1 Prerequisites

Before starting the following procedure, remove the old **server.keystore** located in **C:\hp\UCMDB\UCMDBServer\conf\security\server.keystore**.

2 Generate a Server Keystore

a Generate a CA signed certificate and install it on Windows.

b Export the certificate into a ***.pfx** file (including private keys) using Microsoft Management Console (**mmc.exe**).

Enter any string as the password for the **pfx** file. (You are asked for this password when converting the keystore type to a JAVA keystore.) The **.pfx** file now contains a public certificate and a private key and is password protected.

c Copy the **.pfx** file you created to the following folder: **C:\hp\UCMDB\UCMDBServer\conf\security**.

d Open the command prompt and change the directory to **C:\hp\UCMDB\UCMDBServer\bin\jre\bin**.

➤ Change the keystore type from **PKCS12** to a **JAVA** keystore by running the following command:

```
keytool -importkeystore -srckeystore
c:\hp\UCMDB\UCMDBServer\conf\security\<pfx file name> -srcstoretype
PKCS12 -destkeystore server.keystore
```

You are asked for the source (**.pfx**) keystore password. This is the password you supplied when creating the pfx file in step b.)

e Enter the destination keystore password. This password must be the same as defined previously in the **changeKeystorePassword** JMX method, in Security Services. If the password was not changed, use the default **hppass** password.

f After generating the certificate, disable HTTP port 8080. For details, see "Enable or Disable HTTP/HTTPS Ports" on page 313.

g If you used a password other than **hppass** or the password used for the .pfx file, run the **changeKeystorePassword** JMX method and make sure that the key has the same password.

Note: Check that HTTPS communication works before closing the HTTP port.

---

3 Restart the Server

4 Verify the Server Security

To verify that the UCMDB Server is secure, enter the following URL in the Web browser: **https://<UCMDB Server name or IP address>:8443/ ucmdb-ui**.

Limitation: There can be one server certificate only in **server.keystore**.

✎ Enable SSL on the Client Machines

If the certificate used by the HP Universal CMDB Web server is issued by a well-known Certificate Authority (CA), it is most likely that your Web browser can validate the certificate without any further action.

If the CA is not trusted by the Web browser, you should either import the entire certificate trust path or import the certificate used by HP Universal CMDB explicitly into the browser's truststore.

The following example demonstrates how to import the self-signed **hpcert** certificate into the Windows truststore to be used by Internet Explorer.

To import a certificate into the Windows truststore:

1 Locate and rename the **hpcert** certificate to **hpcert.cer**.

In Windows Explorer, the icon shows that the file is a security certificate.

2 Double-click **hpcert.cer** to open the Internet Explorer Certificate dialog box.

3 Follow the instructions for enabling trust by installing the certificate with the Certificate Import Wizard.

Note: Another method of importing the certificate issued by the UCMDB Server to the Web browser is by logging in to UCMDB, and installing the certificate when the untrusted certificate warning is displayed.

⚜ Enable SSL on the Client SDK

You can utilize HTTPS transportation between the client SDK and the server SDK:

1 On the client machine, in the product that embeds the client SDK, locate the transportation setting and make sure it is configured to HTTPS, and not HTTP.

2 Download the CA certificate/self-signed public certificate to the client machine, and import it into the **cacerts** truststore on the JRE that is going to connect to the server.

Use the following command:

```
Keytool -import -alias <CA name> -trustcacerts -file <server public certificate path> -
keystore <path to client jre trusted cacerts store (e.g. x:\program
files\java\jre\lib\security\cacerts)>
```

⚜ Enable Mutual Certificate Authentication for SDK

This mode uses SSL and enables both server authentication by the UCMDB and client authentication by the UCMDB-API client. Both the server and the UCMDB-API client send their certificates to the other entity for authentication.

Important: The following method of enabling SSL on the SDK with mutual authentication is the most secure of the methods and is therefore the recommended communication mode.

---

1 Harden the UCMDB-API client connector in UCMDB:

a Access the UCMDB JMX console: Launch a Web browser and enter the following address: **http://<UCMDB machine name or IP address>:8080/jmx-console**. You may have to log in with a user name and password (default is sysadmin/sysadmin).

309

   b Locate **UCMDB:service=Ports Management Services** and click the link to open the Operations page.

   c Locate the **PortsDetails** operation and click **Invoke**. Make a note of the HTTPS with client authentication port number. The default is 8444 and it should be enabled.

   d Return to the Operations page.

   e To map the ucmdb-api connector to the mutual authentication mode, invoke the **mapComponentToConnectors** method with the following parameters:

   ➤ **componentName**: ucmdb-api

   ➤ **isHTTPSWithClientAuth**: true

   ➤ All other flags: false

   The following message is displayed:

   > Operation succeeded. Component ucmdb-api is now mapped to:
   > HTTPS_CLIENT_AUTH ports.

   f Return to the Operations page.

2 Make sure the JRE that runs the UCMDB-api client has a keystore containing a client certificate.

3 Export the UCMDB-api client certificate from its keystore.

4 Import the exported UCMDB-api client certificate to the UCMDB Server Truststore.

   a On the UCMDB machine, copy the created UCMDB-api client certificate file to the following directory on UCMDB: **C:\HP\UCMDB\UCMDBServer\conf\security**

   b Run the following command:

   > C:\HP\UCMDB\UCMDBServer\bin\jre\bin\keytool.exe -import -v -keystore
   > C:\HP\UCMDB\UCMDBServer\conf\security\server.truststore -file <exported
   > UCMDB-api client certificate> - alias ucmdb-api

   c Enter the UCMDB Server Truststore password (default **hppass**).

  d When asked, **Trust this certificate?**, press **y** and then ENTER.

  e Make sure the output is Certificate was added to keystore.

5 Export the UCMDB server certificate from the server keystore.

  a On the UCMDB machine, run the following command:

```
C:\HP\UCMDB\UCMDBServer\bin\jre\bin\keytool.exe -export -alias hpcert -
keystore
C:\HP\UCMDB\UCMDBServer\conf\security\server.keystore -file
C:\HP\UCMDB\conf\security\server.certi
```

  b Enter the UCMDB Server Truststore password (default **hppass**).

  c Verify that the certificate is created in the following directory:
  C:\HP\UCMDB\UCMDBServer\conf\security\server.cert

6 Import the exported UCMDB certificate to the JRE of the UCMDB-API
client truststore.

7 Restart the UCMDB Server and the UCMDB-API client.

8 To connect from the UCMDB-API client to UCMDB-API server, use the
following code:

```
UcmdbServiceProvider provider =
UcmdbServiceFactory.getServiceProvider("https",
<SOME_HOST_NAME>,
<HTTPS_WITH_CLIENT_AUTH_PORT_NUMBER (default:8444>));
UcmdbService ucmdbService =
provider.connect(provider.createCertificateCredentials(<TheClientKeyst
ore. e.g: "c:\\client.keystore">, <KeystorePassword>),
provider.createClientContext(<ClientIdentification>));
```

🔧 Change the Server Keystore Passwords

After installing the Server, the HTTPS port is open and the store is secured with a weak password (the default **hppass**). If you intend to work with SSL only, you must change the password.

The following procedure explains how to change the **server.keystore** password only. However, you should perform the same procedure for changing the **server.truststore** password.

Note: You must perform every step in this procedure.

---

1 Start the UCMDB Server.

2 Execute the password change in the JMX console.

   a Launch the Web browser and enter the Server address, as follows: **http://<UCMDB Server Host Name or IP>:8080/jmx-console**.

     You may have to log in with a user name and password.

   b Under UCMDB, click **UCMDB:service=Security Services** to open the Operations page.

   c Locate and execute the **changeKeystorePassword** operation.

     This field must not be empty and must be at least six characters long. The password is changed in the database only.

3 Stop the UCMDB Server.

4 Run commands.

From **C:\hp\UCMDB\UCMBServer\bin\jre\bin**, run the following commands:

   a Change the store password:

```
keytool -storepasswd -new <new_keystore_pass> -keystore
C:\hp\UCMDB\UCMDBServer\conf\security\server.keystore -storepass
<current_keystore_pass>
```

b The following command displays the inner key of the keystore. The first parameter is the alias. Save this parameter for the next command:

```
keytool -list -keystore
C:\hp\UCMDB\UCMDBServer\conf\security\server.keystore
```

c Change the key password (if the store is not empty):

```
keytool -keypasswd -alias <alias> -keypass <currentPass> -new <newPass> -
keystore C:\hp\UCMDB\UCMDBServer\conf\security\server.keystore
```

d Enter the new password.

5 Start the UCMDB Server.

6 Repeat the procedure for the Server truststore.

🦴 Enable or Disable HTTP/HTTPS Ports

You can enable or disable the HTTP and HTTPS ports from within the user interface or from the JMX console.

To enable or disable the HTTP/HTTPS ports from within the user interface:

1 Log on to HP Universal CMDB.

2 Select **Administration** > **Infrastructure Settings**.

3 Enter either **http** or **https** in the **Filter** (by Name) box to display the HTTP settings.

➤ **Enable HTTP(S) connections**. **True**: the port is enabled. **False**: the port is disabled.

4 Restart the server to apply the change.

Limitation: The HTTPS port is open by default; closing this port prevents **Server_Management.bat** from functioning.

To enable or disable the HTTP/HTTPS ports from the JMX console:

1 Launch a Web browser and enter the following address:
http://localhost.<domain_name>:8080/jmx-console.

2 Enter the JMX console authentication credentials, which by default are:

➤ Login name = **sysadmin**

➤ Password = **sysadmin**

3 Locate **UCMDB:service=Ports Management Services** and click the link to open the Operations page.

4 To enable or disable the HTTP port, locate the **HTTPSetEnable** operation and set the value.

➤ **True**: the port is enabled. **False**: the port is disabled.

5 To enable or disable the HTTPS port, locate the **HTTPSSetEnable** operation and set the value.

➤ **True**: the port is enabled. **False**: the port is disabled.

6 To enable or disable the HTTPS port with client authentication, locate the **HTTPSClientAuthSetEnable** operation and set the value.

➤ **True**: the port is enabled. **False**: the port is disabled.

⚓ Map the UCMDB Web Components to Ports

You can configure the mapping of each UCMDB component to the available ports from the JMX console.

To view the current component configurations:

1 Launch a Web browser and enter the following address:
http://localhost.<domain_name>:8080/jmx-console.

2 Enter the JMX console authentication credentials, which by default are:

➤ Login name = **sysadmin**

➤ Password = **sysadmin**

3 Locate **UCMDB:service=Ports Management Services** and click the link to open the Operations page.

4 Locate the **ComponentsConfigurations** method and click **Invoke**.

5 For each component, the valid ports and current mapped ports are displayed.

To map the components:

1 Locate **UCMDB:service=Ports Management Services** and click the link to open the Operations page.

2 Locate the **mapComponentToConnectors** method.

3 Enter a component name in the Value box. Select **True** or **False** for each of the ports corresponding to your selection. Click **Invoke**. The selected component is mapped to the selected ports. You can find the component names by invoking the **serverComponentsNames** method.

4 Repeat the process for each relevant component.

Note:

➤ Every component must be mapped to at least one port. If you do not map a component to any port, it is mapped by default to the HTTP port.

➤ If you map a component to both the HTTPS port and the HTTPS port with client authentication, only the client authentication option is mapped (the other option is redundant in this case).

You can also change the value assigned to each of the ports.

To set values for the ports:

1 Locate **UCMDB:service=Ports Management Services** and click the link to open the Operations page.

2 To set a value for the HTTP port, locate the **HTTPSetPort** method and enter a value in the Value box. Click **Invoke**.

3 To set a value for the HTTPS port, locate the **HTTPSSetPort** method and enter a value in the Value box. Click **Invoke**.

4 To set a value for the HTTPS port with client authentication, locate the **HTTPSClientAuthSetPort** method and enter a value in the Value box. Click **Invoke**.

20

Using a Reverse Proxy

This chapter includes:

Concepts

➤ Reverse Proxy Overview on page 318

➤ Security Aspects of Using a Reverse Proxy Server on page 320

Tasks

➤ Configure a Reverse Proxy Using Infrastructure Settings on page 321

➤ Configure a Reverse Proxy Using the JMX Console on page 322

➤ Apache 2.0.x – Example Configuration on page 323

Concepts

🪐 Reverse Proxy Overview

Note: This chapter describes the security ramifications of reverse proxies and contains instructions for using a reverse proxy with HP Universal CMDB. Security aspects of a reverse proxy are discussed but not other aspects such as caching and load balancing.

A reverse proxy is an intermediate server that is positioned between the client machine and the Web servers. To the client machine, the reverse proxy appears to be a standard Web server that serves the client machine's HTTP protocol requests.

The client machine sends ordinary requests for Web content, using the name of the reverse proxy instead of the name of a Web server. The reverse proxy sends the request to one of the Web servers. Although the response is sent back to the client machine by the reverse proxy, it appears to the client machine as if it is being sent by the Web server.

It is possible to have multiple reverse proxies, with different urls, representing the same UCMDB instance. Alternatively, a single reverse proxy server can be used to access several UCMDB servers, by setting different root contexts for each UCMDB server.

HP Universal CMDB supports a reverse proxy in DMZ architecture. The reverse proxy is an HTTP mediator between the Data Flow Probe and the Web client and the HP Universal CMDB server.

Note:

➤ Different types of reverse proxies require different configuration syntaxes. For an example of an Apache 2.0.x reverse proxy configuration, see "Apache 2.0.x – Example Configuration" on page 323.

➤ It is only necessary to configure the reverse proxy settings when creating a direct link to a report using the Scheduler.

🍀 Security Aspects of Using a Reverse Proxy Server

A reverse proxy server functions as a bastion host. The proxy is configured to be the only machine addressed directly by external clients, and thus obscures the rest of the internal network. Use of a reverse proxy enables the application server to be placed on a separate machine in the internal network.

This section discusses the use of a DMZ and reverse proxy in a back-to-back topology environment.

The following are the main security advantages of using a reverse proxy in such an environment:

➤ No DMZ protocol translation occurs. The incoming protocol and outgoing protocol are identical (only a header change occurs).

➤ Only HTTP access to the reverse proxy is allowed, which means that stateful packet inspection firewalls can better protect the communication.

➤ A static, restricted set of redirect requests can be defined on the reverse proxy.

➤ Most of the Web server security features are available on the reverse proxy (authentication methods, encryption, and so on).

➤ The reverse proxy screens the IP addresses of the real servers as well as the architecture of the internal network.

➤ The only accessible client of the Web server is the reverse proxy.

➤ This configuration supports NAT firewalls (as opposed to other solutions).

➤ The reverse proxy requires a minimal number of open ports in the firewall.

➤ The reverse proxy provides good performance compared to other bastion solutions.

Tasks

⚒ Configure a Reverse Proxy Using Infrastructure Settings

The following procedure explains how to access Infrastructure Settings to configure a reverse proxy. This configuration is only necessary when creating a direct link to a report using the Scheduler.

To configure a reverse proxy:

1 Select **Administration** > **Infrastructure Settings** > **General Settings** category.

2 Change the **Frontend URL** setting. Enter the address, for example, **https://my_proxy_server:443/**.

⚒ Configure a Reverse Proxy Using the JMX Console

The following procedure explains how to make changes to the reverse proxy configuration by using the JMX console on the HP Universal CMDB server machine. This configuration is only necessary when creating a direct link to a report using the Scheduler.

To change a reverse proxy configuration:

1 On the HP Universal CMDB server machine, launch the Web browser and enter the following address:

```
http://<machine name or IP address>.<domain_name>:8080/jmx-console
```

where **<machine name or IP address>** is the machine on which HP Universal CMDB is installed. You may have to log in with the user name and password.

2 Click the **UCMDB-UI** > **UCMDB-UI:name=UI Server frontend settings** link.

3 In the **setUseFrontendURLBySettings** field, enter the server proxy URL, for example, **https://my_proxy_server:443/**.

4 Click **Invoke**.

5 To see the value of this setting, use the **showFrontendURLInSettings** method.

🔧 Apache 2.0.x – Example Configuration

Below is a sample configuration file that supports the use of an Apache 2.0.x reverse proxy in a case where both Data Flow Probes and application users connect to HP Universal CMDB.

Note:

➤ In the example below, the HP Universal CMDB machine's DNS name is **UCMDB_server**.

➤ Only users with a knowledge of Apache administration should make this change.

---

1 Open the <**Apache machine root directory**>**Webserver****conf****httpd.conf** file.

2 Enable the following modules:

➤ LoadModule proxy_module modules/mod_proxy.so

➤ LoadModule proxy_http_module modules/mod_proxy_http.so

3 Add the following lines to the httpd.conf file:

```
ProxyRequests off
<Proxy *>
Order deny,allow
Deny from all
Allow from all
</Proxy>
ProxyPass /mam http://UCMDB_server/mam
ProxyPassReverse /mam http://UCMDB_server/mam
ProxyPass /mam_images http://UCMDB_server/mam_images
ProxyPassReverse /mam_images http://UCMDB_server/mam_images
ProxyPass /mam-collectors http://UCMDB_server/mam-collectors
ProxyPassReverse /mam-collectors http://UCMDB_server/mam-collectors
ProxyPass /ucmdb http://UCMDB_server/ucmdb
ProxyPassReverse /ucmdb http://UCMDB_server/ucmdb
ProxyPass /site http://UCMDB_server/site
ProxyPassReverse /site http://UCMDB_server/site
ProxyPass /ucmdb-ui http://UCMDB_server/ucmdb-ui
ProxyPassReverse /ucmdb-ui http://UCMDB_server/ucmdb-ui
ProxyPass /status http://UCMDB_server/status
ProxyPassReverse /status http://UCMDB_server/status
ProxyPass /jmx-console http://UCMDB_server/jmx-console
ProxyPassReverse /jmx-console http://UCMDB_server/jmx-console
ProxyPass /axis2 http://UCMDB_server/axis2
ProxyPassReverse /axis2 http://UCMDB_server/axis2
ProxyPass /icons http://UCMDB_server/icons
ProxyPassReverse /icons http://UCMDB_server/icons
ProxyPass /ucmdb-api http://UCMDB_server/ucmdb-api
ProxyPassReverse /ucmdb-api http://UCMDB_server/ucmdb-api
ProxyPass /ucmdb-docs http://UCMDB_server/ucmdb-docs
ProxyPassReverse /ucmdb-docs http://UCMDB_server/ucmdb-docs
ProxyPass /ucmdb-api/8.0 http://UCMDB_server/ucmdb-api/8.0
ProxyPassReverse /ucmdb-api/8.0 http://UCMDB_server/ucmdb-api/8.0
ProxyPass /cm http://UCMDB_Server/cm
ProxyPassReverse /cm http://UCMDB_Server /cm
```

4 Save your changes.

21

Data Flow Credentials Management

This chapter includes:

Concepts

Tasks

Reference

Concepts

🍥 Data Flow Credentials Management Overview

To perform discovery or run integration, you must set up the credentials to access the remote system. Credentials are configured in the Data Flow Probe Setup window and saved in the UCMDB Server. For details, see "Data Flow Probe Setup Window" on page 57.

Credentials storage is managed by the Confidential Manager (CM) component. For details, see "Confidential Manager" on page 397.

The Data Flow Probe can access the credentials using the CM client. The CM client resides on the Data Flow Probe and communicates with the CM server, which resides on the UCMDB Server. Communication between the CM client and the CM server is encrypted, and authentication is required by the CM client when it connects to the CM server.

The CM client's authentication on the CM server is based on a LW-SSO component. Before connecting to the CM server, the CM client first sends an LW-SSO cookie. The CM server verifies the cookie and upon successful verification, communication with the CM client begins. For details about LW-SSO, see "Configure LW-SSO Settings on the UCMDB Server" on page 334.

The communication between the CM client and the CM server is encrypted. For details about updating the encryption configuration, see "Configure CM Communication Encryption on the UCMDB Server" on page 335.

Important: The CM authentication uses the universal time defined on the computer (UTC). In order for the authentication to succeed, ensure that the universal time on the Data Flow probe and the UCMDB Server are the same. The server and probe may be located in different time zones, as UTC is independent of time zone or daylight savings time.

The CM client maintains a local cache of the credentials. The CM client is configured to download all credentials from the CM server and store them in a cache. The credentials changes are automatically synchronized from CM server on a continuous basis. The cache can be a file-system or in-memory cache, depending on the preconfigured settings. In addition, the cache is encrypted and cannot be accessed externally. For details about updating the cache settings, see "Configure the CM Client's Cache Mode on the Probe" on page 341. For details about updating the cache encryption, see "Configure the CM Client's Cache Encryption Settings on the Probe" on page 342.

For details on troubleshooting, see "Change Confidential Manager (CM) Client Log File Message Level" on page 346.

You can copy credentials information from one UCMDB server to another. For details, see "Export and Import Credential and Range Information in Encrypted Format" on page 344.

Note: The **DomainScopeDocument** (DSD) that was used for credentials storage on the Probe (in UCMDB version 9.01 or earlier) no longer contains any credentials-sensitive information. The file now contains a list of Probes and network range information. It also contains a list of credential entries for each domain, where each entry includes the credential ID and a network range (defined for this credential entry) only.

This section includes the following topics:

➤ "Basic Security Assumptions" on page 330

➤ "Data Flow Probe Running in Separate Mode" on page 330

➤ "Keeping the Credentials Cache Updated" on page 330

➤ "Synchronizing All Probes with Configuration Changes" on page 330

➤ "Secured Storage on the Probe" on page 332

Basic Security Assumptions

Note the following security assumption:

You have secured the UCMDB Server and Probe JMX console to enable access to UCMDB system administrators only, preferably through localhost access only.

Data Flow Probe Running in Separate Mode

When the Probe Gateway and Manager run as separate processes, the Confidential Manager (CM) client component becomes part of the Manager process. Credentials information is cached and used by the Probe Manager only. To access the CM server on the UCMDB system, the CM client request is handled by the Gateway process and from there is forwarded to the UCMDB system.

This configuration is automatic when the Probe is configured in separate mode.

Keeping the Credentials Cache Updated

On its first successful connection to the CM server, the CM client downloads all relevant credentials (all credentials that are configured in the probe's domain). After the first successful communication, the CM client retains continuous synchronization with the CM server. Differential synchronization is performed at one-minute intervals, during which only differences between the CM server and the CM client are synchronized. If the credentials are changed on the UCMDB server side (such as new credentials being added, or existing credentials being updated or deleted), the CM client receives immediate notification from the UCMDB server and performs additional synchronization.

Synchronizing All Probes with Configuration Changes

For successful communication, the CM client must be updated with the CM server authentication configuration (LW-SSO init string) and encryption configuration (CM communication encryption). For example, when the init string is changed on the server, the probe must know the new init string in order to authenticate.

The UCMDB server constantly monitors for changes in the CM communication encryption configuration and CM authentication configuration. This monitoring is done every 15 seconds; in case a change has occurred, the updated configuration is sent to the probes. The configuration is passed to the probes in encrypted form and stored on the probe side in secured storage. The encryption of configuration being sent is done using a symmetric encryption key. By default, the UCMDB server and Data Flow Probe are installed with same default symmetric encryption key. For optimal security, it is highly recommended to change this key before adding credentials to the system. For details, see "Generate or Update the Encryption Key" on page 348.

Note:

➤ Due to the 15 second monitoring interval, it is possible that the CM client, on the Probe side, may not be updated with the latest configuration for a period of 15 seconds.

➤ If you choose to disable the automatic synchronization of CM communication and authentication configuration between the UCMDB server and the Data Flow Probe, each time you update the CM communication and authentication configuration on the UCMDB server side, you should update all Probes with the new configuration as well. For details, see "Disable Automatic Synchronization of the CM Client Authentication and Encryption Settings Between the UCMDB Server and Probes" on page 337.

Secured Storage on the Probe

All sensitive information (such as the CM communication and authentication configuration and the encryption key) is stored on the Probe in secure storage in the **secured_storage.bin** file, located in the **C:\hp\UCMDB\DataFlowProbe\conf\security** directory. This secured storage is encrypted using DPAPI, which relies on the Windows user password in the encryption process. DPAPI is a standard method used to protect confidential data—such as certificates and private keys—on Windows systems. The Probe should always run under the same Windows user, so that even if the password is changed, the Probe can still read the information stored in secure storage.

Viewing Credentials Information (Data Direction: CMDB to HP Universal CMDB)

Passwords are not sent from the CMDB to the application. That is, HP Universal CMDB displays asterisks (*****) in the password field, regardless of content:

🍧 Updating Credentials (Data Direction: HP Universal CMDB to CMDB)

➤ The communication in this direction is not encrypted, therefore you should connect to the UCMDB Server using https\SSL, or ensure connection through a trusted network.

Although the communication is not encrypted, passwords are not being sent as clear text on the network. They are encrypted using a default key and, therefore, it is highly recommended to use SSL for effective confidentiality in transit.

➤ You can use special characters and non-English characters as passwords.

Tasks

🔧 Configure CM Client Authentication and Encryption Settings on the UCMDB Server

This task includes the following steps:

➤ "Configure LW-SSO Settings on the UCMDB Server" on page 334

➤ "Configure CM Communication Encryption on the UCMDB Server" on page 335

Configure LW-SSO Settings on the UCMDB Server

This procedure describes how to change the LW-SSO init string on the UCMDB server. This change is automatically sent to Probes (as an encrypted string), unless the UCMDB server is configured to not automatically do this. For details, see "Disable Automatic Synchronization of the CM Client Authentication and Encryption Settings Between the UCMDB Server and Probes" on page 337.

1 On the UCMDB server, launch the Web browser and enter the following address: **http://localhost:8080/jmx-console**.

2 Click **UCMDB-UI:name=LW-SSO Configuration** to open the JMX MBEAN View page.

3 Locate the **setInitString** method.

4 Enter a new LW-SSO init string.

5 Click **Invoke**.

Configure CM Communication Encryption on the UCMDB Server

This procedure describes how to change the CM communication encryption settings. These settings specify how the communication between the CM client and the CM server is encrypted. This change is automatically sent to Probes (as an encrypted string), unless the UCMDB server is configured to not automatically do this. For details, see "Disable Automatic Synchronization of the CM Client Authentication and Encryption Settings Between the UCMDB Server and Probes" on page 337.

 1 On the UCMDB server, launch the Web browser and enter the following address: **http://localhost:8080/jmx-console**.

 2 Click **UCMDB:service=Security Services** to open the JMX MBEAN View page.

 3 Click the **CMGetConfiguration** method.

 4 Click **Invoke**.

   The XML of the current CM configuration is displayed.

 5 Copy the contents of the displayed XML.

 6 Navigate back to the **Security Services** JMX MBean View page.

 7 Click the **CMSetConfiguration** method.

 8 Paste the copied XML into the **Value** field.

 9 Update the relevant transport-related settings.

   For details about the values that can be updated, see "CM Encryption Settings" on page 354.

Example:

```
<transport>
    <encryptTransportMode>true</encryptTransportMode>
    <CMEncryptionDecryption>
        <encryptDecryptInitString>radiohead</encryptDecryptInitString>
        <cryptoSource>lw</cryptoSource>
        <lwJCEPBECompatibilityMode>true</lwJCEPBECompatibilityMode>
        <cipherType>symmetricBlockCipher</cipherType>
        <engineName>AES</engineName>
        <algorithmModeName>CBC</algorithmModeName>
        <algorithmPaddingName>PKCS7Padding</algorithmPaddingName>
        <keySize>256</keySize>
        <pbeCount>20</pbeCount>
        <pbeDigestAlgorithm>SHA1</pbeDigestAlgorithm>
        <encodingMode>Base64Url</encodingMode>
        <useMacWithCrypto>false</useMacWithCrypto>
        <macType>hmac</macType>
        <macKeySize>256</macKeySize>
        <macHashName>SHA256</macHashName>
    </CMEncryptionDecryption>
</transport>
```

 10 Click **Invoke**.

🔧 Configure CM Client Authentication and Encryption Settings Manually on the Probe

This task includes the following steps:

➤ "Disable Automatic Synchronization of the CM Client Authentication and Encryption Settings Between the UCMDB Server and Probes" on page 337

➤ "Configure CM Client Authentication and Encryption Settings on the Probe" on page 338

➤ "Configure CM Communication Encryption on the Probe" on page 339

Disable Automatic Synchronization of the CM Client Authentication and Encryption Settings Between the UCMDB Server and Probes

By default, the UCMDB Server is configured to automatically send the CM/LW-SSO settings to all Probes. This information is sent as an encrypted string to the Probes, which decrypt the information upon retrieval. You can configure the UCMDB Server to not send the CM/LW-SSO configuration files automatically to all Probes. In this case, it is your responsibility to manually update all Probes with the new CM/LW-SSO settings.

To disable automatic synchronization of CM/LW-SSO settings:

1 In UCMDB, click **Administration** > **Infrastructure Settings Manager** > **General Settings**.

2 Select **Enable automatic synchronization of CM/LW-SSO configuration and init string with probe**.

3 Click the **Value** field and change **True** to **False**.

4 Click the **Save** button.

5 Restart the UCMDB server.

Configure CM Client Authentication and Encryption Settings on the Probe

This procedure is relevant if the UCMDB Server has been configured to not send LW-SSO/CM configuration and settings automatically to Probes. For details, see "Disable Automatic Synchronization of the CM Client Authentication and Encryption Settings Between the UCMDB Server and Probes" on page 337.

1 On the Probe machine, launch the Web browser and enter the following address: **http://localhost:1977**.

Note: If the Probe Manager and the Probe Gateway are running as separate processes, the address should be entered on the machine that is running the Probe Manager as follows: **http://localhost:1978**.

---

2 Click **type=CMClient** to open the JMX MBEAN View page.

3 Locate the **setLWSSOInitString** method and provide the same init string that was provided for UCMDB's LW-SSO configuration.

4 Click the **setLWSSOInitString** button.

Configure CM Communication Encryption on the Probe

This procedure is relevant if the UCMDB Server has been configured to not send LW-SSO/CM configuration and settings automatically to Probes. For details, see "Disable Automatic Synchronization of the CM Client Authentication and Encryption Settings Between the UCMDB Server and Probes" on page 337.

1 On the Probe machine, launch the Web browser and enter the following address: **http://localhost:1977**.

Note: If the Probe Manager and the Probe Gateway are running as separate processes, the address should be entered on the machine that is running the Probe Manager as follows: **http://localhost:1978**.

---

2 Click **type=CMClient** to open the JMX MBEAN View page.

3 Update the following transport-related settings:

Note: You must update the same settings that you updated on the UCMDB server. To do this, some of the methods that you update on the Probe may require more than one parameter. To see the current probe configuration, click **displayTransportConfiguration** in the JMX MBEAN View page. For details, see "Configure CM Communication Encryption on the UCMDB Server" on page 335. For details about the values that can be updated, see "CM Encryption Settings" on page 354.

---

   a **setTransportInitString** changes the **encryptDecryptInitString** setting.

   b **setTransportEncryptionAlgorithm** changes CM settings on the Probe according to the following map:

      ➤ **Engine name** refers to the <engineName> entry

      ➤ **Key size** refers to the <keySize> entry

> ➤ **Algorithm padding name** refers to the <algorithmPaddingName> entry

> ➤ **PBE count** refers to the <pbeCount> entry

> ➤ **PBE digest algorithm** refers to the <pbeDigestAlgorithm> entry

  c **setTransportEncryptionLibrary** changes CM settings on the Probe according to the following map:

> ➤ **Encryption Library name** refers to the <cryptoSource> entry

> ➤ **Support previous lightweight cryptography versions** refers to the <lwJCEPBECompatibilityMode> entry

  d **setTransportMacDetails** change CM settings on the Probe according to the following map:

> ➤ **Use MAC with cryptography** refers to the <useMacWithCrypto> entry

> ➤ **MAC key size** refers to the <macKeySize> entry

4 Click the **reloadTransportConfiguration** button to make the changes effective on the Probe.

For details about the different settings and their possible values, see "CM Encryption Settings" on page 354.

🪓 Configure the Confidential Manager (CM) Client Cache

This task includes the following steps:

➤ "Configure the CM Client's Cache Mode on the Probe" on page 341

➤ "Configure the CM Client's Cache Encryption Settings on the Probe" on page 342

Configure the CM Client's Cache Mode on the Probe

The CM client stores credentials information in the cache and updates it when the information changes on the Server. The cache can be stored on the file system or in memory:

➤ **When stored on the file system**, even if the Probe is restarted and cannot connect to the Server, the credentials information is still available.

➤ **When stored in memory**, if the Probe is restarted, the cache is cleared and all information is retrieved again from the Server. If the Server is not available, the Probe does not include any credentials, so no discovery or integration can run.

To change this setting:

1 Open the **DiscoveryProbe.properties** file in a text editor. This file is located in the **c:\hp\UCMDB\DataFlowProbe\conf** directory.

2 Locate the following attribute:
com.hp.ucmdb.discovery.common.security.storeCMData=true

➤ To store the information on the file system, leave the default (**true**).

➤ To store the information in memory, enter **false**.

3 Save the **DiscoveryProbe.properties** file.

4 Restart the Probe.

Configure the CM Client's Cache Encryption Settings on the Probe

This procedure describes how to change the encryption settings of the CM client's file system cache file. Note that changing the encryption settings for the CM client's file system cache causes the file system cache file to be recreated. This recreation process requires restarting the Probe and full synchronization with the UCMDB Server.

1 On the Probe machine, launch the Web browser and enter the following address: **http://localhost:1977**.

Note: If the Probe Manager and the Probe Gateway are running as separate processes, the address should be entered on the machine that is running the Probe Manager as follows: **http://localhost:1978**.

---

2 Click **type=CMClient** to open the JMX MBEAN View page.

3 Update the following cache-related settings:

Note: Some of the methods that you update on the Probe may require more than one parameter. To see the current probe configuration, click **displayCacheConfiguration** in the JMX MBEAN View page.

---

a **setCacheInitString** changes the file system cache <encryptDecryptInitString> setting.

b **setCacheEncryptionAlgorithm** changes the file system cache settings according to the following map:

➤ **Engine name** refers to the <engineName> entry

➤ **Key size** refers to the <keySize> entry

➤ **Algorithm padding name** refers to the <algorithmPaddingName> entry

> ➤ **PBE count** refers to the <pbeCount> entry

> ➤ **PBE digest algorithm** refers to the <pbeDigestAlgorithm> entry

  c **setCacheEncryptionLibrary** changes the cache file system settings according to the following map:

> ➤ **Encryption Library name** refers to the <cryptoSource> entry

> ➤ **Support previous lightweight cryptography versions** refers to the <lwJCEPBECompatibilityMode> entry

  d **setCacheMacDetails** changes the cache file system settings according to the following map:

> ➤ **Use MAC with cryptography** refers to the <useMacWithCrypto> entry

> ➤ **MAC key size** refers to the <macKeySize> entry

4 Click the **reloadCacheConfiguration** button to make the changes effective on the Probe. This causes the Probe to restart.

Note: Make sure that no job is running on the Probe during this action.

For details about the different settings and their possible values, see "CM Encryption Settings" on page 354.

🔧 Export and Import Credential and Range Information in Encrypted Format

You can export and import credentials and network range information in encrypted format in order to copy the credentials information from one UCMDB Server to another. For example, you might perform this operation during recovery following a system crash or during upgrade.

➤ **When exporting credentials information**, you must enter a password (of your choosing). The information is encrypted with this password.

➤ **When importing credentials information**, you must use the same password that was defined when the DSD file was exported.

Note: The exported credentials document also contains ranges information that is defined on the system from which the document was exported. During the import of the credentials document, ranges information is imported as well.

Important: To import credentials information from a UCMDB version 8.02 domainScopeDocument, you must use the **key.bin** file located on the version 8.02 system.

To export credentials information from the UCMDB Server:

1 On the UCMDB Server, launch the Web browser and enter the following address: **http://localhost:8080/jmx-console**. You may have to log in with a user name and password.

2 Click **UCMDB:service=DiscoveryManager** to open the JMX MBEAN View page.

3 Locate the **exportCredentialsAndRangesInformation** operation. Do the following:

> ➤ Enter your customer ID (the default is 1).

> ➤ Enter a name for the exported file.

> ➤ Enter your password.

> ➤ Set **isEncrypted=True** if you want the exported file to be encrypted with the provided password, or **isEncrypted=False** if you want the exported file to not be encrypted (in which case passwords and other sensitive information are not exported).

4 Click **Invoke** to export.

When the export process completes successfully, the file is saved to the following location: **c:\hp\UCMDB\UCMDBServer\conf\discovery\<customer_dir>** directory.

To import credentials information from the UCMDB Server:

1 On the UCMDB Server, launch the Web browser and enter the following address: **http://localhost:8080/jmx-console**.

You may have to log in with a user name and password.

2 Click **UCMDB:service=DiscoveryManager** to open the JMX MBEAN View page.

3 Locate one of the following operations:

> ➤ Locate the **importCredentialsAndRangesInformation** operation if the file that you are importing was exported from a UCMDB Server that is later than version 8.02.

> ➤ Locate the **importCredentialsAndRangesWithKey** operation if the file that you are importing was exported from a UCMDB version 8.02 Server.

4 Enter your customer ID (the default is 1).

5 Enter the name of the file to import. This file must be located in the **c:\hp\UCMDB\UCMDBServer\conf\discovery\<customer_dir>** directory.

6 Enter the password. This must be the same password that was used when the file was exported.

7 If the file was exported from a UCMDB version 8.02 system, enter the **key.bin** file name. This file must be located in the **c:\hp\UCMDB\ UCMDBServer\conf\discovery\<customer_dir>** directory, together with the file to be imported.

8 Click **Invoke** to import the credentials.

🔍 Change Confidential Manager (CM) Client Log File Message Level

The Probe provides two log files that contain information regarding CM-related communication between the CM server and the CM client. The files are:

➤ "CM Client Log File" on page 346

➤ "LW-SSO Log File" on page 347

CM Client Log File

The **security.cm.log** file is located in the **c:\hp\UCMDB\DataFlowProbe\runtime\log** directory.

The log contains information messages exchanged between the CM server and the CM client. By default, the log level of these messages is set to INFO.

To change the log level of the messages to DEBUG level:

1 On the Data Flow Probe Manager server, navigate to **c:\hp\UCMDB\DataFlowProbe\conf\log**.

2 Open the **security.properties** file in a text editor.

3 Change the line:

> loglevel.cm=INFO

to:

> loglevel.cm=DEBUG

4 Save the file.

LW-SSO Log File

The **security.lwsso.log** file is located in the
c:\hp\UCMDB\DataFlowProbe\runtime\log directory.

The log contains information messages related to LW-SSO. By default, the
log level of these messages is set to INFO.

To change the log level of the messages to DEBUG level:

1 On the Data Flow Probe Manager server, navigate to
c:\hp\UCMDB\DataFlowProbe\conf\log.

2 Open the **security.properties** file in a text editor.

3 Change the line:

> loglevel.lwsso=INFO

to:

> loglevel.lwsso=DEBUG

4 Save the file.

🔍 Generate or Update the Encryption Key

You can generate or update an encryption key to be used for encryption or decryption of CM communication and authentication configurations exchanged between the UCMDB Server and the Data Flow Probe. In each case (generate or update), the UCMDB Server creates a new encryption key based on parameters that you supply (for example, key length, extra PBE cycles, JCE provider) and distributes it to the Probes.

The result of running the **generateEncryptionKey** method is a new generated encryption key. This key is stored only in secured storage and its name and details are not known. If you reinstall an existing Data Flow Probe, or connect a new Probe to the UCMDB Server, this new generated key is not recognized by the new Probe. In these cases, it is preferable to use the **changeEncryptionKey** method to change encryption keys. This way, when you reinstall a Probe or install a new Probe, you can import the existing key (whose name and location you know) by running the **importEncryptionKey** method on the Probe JMX console.

Note:

➤ The difference between the methods used to create a key (**generateEncryptionKey**) and update a key (**changeEncryptionKey**) is that **generateEncryptionKey** creates a new, random encryption key, while **changeEncryptionKey** imports an encryption key whose name you provide.

➤ Only one encryption key can exist on a system, no matter how many Probes are installed.

This task includes the following steps:

➤ "Generate a New Encryption Key" on page 349

➤ "Update an Encryption Key on a UCMDB Server" on page 350

➤ "Update an Encryption Key on a Probe" on page 351

➤ "Manually Change the Encryption Key when the Probe Manager and Probe Gateway are Installed on Separate Machines" on page 352

➤ "Generate a New Encryption Key" on page 349

Generate a New Encryption Key

You can generate a new key to be used by the UCMDB Server and Data Flow Probe for encryption or decryption. The UCMDB Server replaces the old key with the new generated key, and distributes this key among the Probes.

To generate a new encryption key through the JMX console:

1 On the UCMDB server, launch the Web browser and enter the following address: **http://localhost:8080/jmx-console**.

You may have to log in with a user name and password.

2 Click **UCMDB:service=DiscoveryManager** to open the JMX MBEAN View page.

3 Locate the generateEncryptionKey operation.

  a In the **customerId** parameter box, enter **1** (the default).

  b For **keySize**, specify the length of the encryption key. Valid values are 128, 192, or 256.

  c For **usePBE**, specify **True** or **False**:

   ➤ **True**: use additional PBE hash cycles.

   ➤ **False:** do not use additional PBE hash cycles.

  d For **jceVendor**, you can choose to use a non-default JCE provider. If the box is empty, the default provider is used.

  e For **autoUpdateProbe**, specify **True** or **False**:

   ➤ **True**: the server distributes the new key to the Probes automatically.

   ➤ **False:** the new key should be placed on the Probes manually.

 f For **exportEncryptionKey**, specify **True** or **False**.

   ➤ **True**: In addition to creating the new password and storing it in secured storage, the Server exports the new password to the file system (**c:\hp\UCMDB\UCMDBServer\conf\discovery\key.bin**). This option enables you to update Probes manually with the new password.

   ➤ **False**: The new password is not exported to the file system. To update Probes manually, set **autoUpdateProbe** to **False** and **exportEncryptionKey** to **True**.

   Important: Make sure that the Probe is up and connected to the server. If the Probe goes down, the key cannot reach the Probe. If you change the key before the Probe goes down, once the Probe is up again, the key is sent again to the Probe. However, if you have changed the key more than once before the Probe goes down, you must change the key manually through the JMX console. (Select **False** for **exportEncryptionKey**).

 4 Click **Invoke** to generate the encryption key.

Update an Encryption Key on a UCMDB Server

You use the **changeEncryptionKey** method to import your own encryption key to the UCMDB server and distribute it among all Probes.

To update an encryption key through the JMX Console:

 1 On the UCMDB Server, launch the Web browser and enter the following address: **http://localhost:8080/jmx-console**.

   You may have to log in with a user name and password.

 2 Click **UCMDB:service=DiscoveryManager** to open the JMX MBEAN View page.

 3 Locate the **changeEncryptionKey** operation.

   a In the **customerId** parameter box, enter **1** (the default).

   b For **newKeyFileName**, enter the name of the new key.

   c For **keySizeInBits**, specify the length of the encryption key. Valid values are 128, 192, or 256.

d For **usePBE**, specify **True** or **False**:

➤ **True**: use additional PBE hash cycles.

➤ **False:** do not use additional PBE hash cycles.

e For **jceVendor**, you can choose to use a non-default JCE provider. If the box is empty, the default provider is used.

f For **autoUpdateProbe**, specify **True** or **False**:

➤ **True**: the server distributes the new key to the Probes automatically.

➤ **False:** the new key should be distributed manually using the Probe JMX console.

Important: Make sure that the Probe is up and connected to the server. If the Probe goes down, the key cannot reach the Probe. If you change the key before the Probe goes down, once the Probe is up again, the key is sent again to the Probe. However, if you have changed the key more than once before the Probe goes down, you must change the key manually through the JMX console. (Select **False** for **autoUpdateProbe**).

4 Click **Invoke** to generate and update the encryption key.

Update an Encryption Key on a Probe

If you choose not to distribute an encryption key from the UCMDB Server to all Probes automatically (because of security concerns), you should download the new encryption key to all Probes and run the **importEncryptionKey** method on the Probe:

1 Place the encryption key file in the **C:\hp\UCMDB\DataFlowProbe \conf\security** directory.

2 On the Probe machine, launch the Web browser and enter the following address: **http://localhost:1977**.

You may have to log in with a user name and password.

351

> **Note:** If the Probe Manager and the Probe Gateway are running as separate processes, the address should be entered on the machine that is running the Probe Manager as follows: **http://localhost:1978**.

 3 On the Probe domain, click **type=SecurityManagerService**.

 4 Locate the **importEncryptionKey** method.

 5 Enter the name of the encryption key file that resides in the **C:\hp\UCMDB\DataFlowProbe\conf\security** directory. This file contains the key to be imported.

 6 Click the **importEncryptionKey** button.

 7 Perform a restart of the probe.

Manually Change the Encryption Key when the Probe Manager and Probe Gateway are Installed on Separate Machines

 1 On the Probe Manager machine, start the Probe Manager service (**Start** > **Programs** > **HP UCMDB** > **Probe** Manager).

 2 Import the key from the server, using the Probe Manager JMX. For details, see "Generate a New Encryption Key" on page 349.

 3 After the encryption key is imported successfully, restart the Probe Manager and Probe Gateway services.

Define Several JCE Providers

When you generate an encryption key through the JMX Console, you can define several JCE providers, using the **changeEncryptionKey** and **generateEncryptionKey** methods.

To change the default JCE provider:

1 Register the JCE provider jar files in the **$JRE_HOME/lib/ext** directory.

2 Copy the jar files to the $JRE_HOME directory:

 ➤ For the UCMDB Server: $JRE_HOME resides at:
 c:\hp\UCMDB\UCMDBServer\bin\jre

 ➤ For the Data Flow Probe: $JRE_HOME resides at:
 c:\hp\UCMDB\DataFlowProbe\bin\jre

3 Add the provider class at the end of the provider list in the **$JRE_HOME\lib\security\java.security** file.

4 Update the **local_policy.jar** and **US_export_policy.jar** files to include unlimited JCE policies. You can download these jar files from the Sun Web site.

5 Restart the UCMDB Server and the Data Flow Probe.

6 Locate the JCE vendor field for the **changeEncryptionKey** or **generateEncryptionKey** method, and add the name of the JCE provider.

Reference

🔐 CM Encryption Settings

This table lists the encryption settings that can be changed using various JMX methods. These encryption settings are relevant for encryption of communications between the CM client and the CM server, as well as for encryption of the CM client's cache.

UCMDB CM Setting Name	Probe CM Setting Name	Setting Description	Possible Values	Default Value
cryptoSource	Encryption Library name	This setting defines which encryption library to use.	lw, jce, windowsDPAPI, lwJCECompatible	lw
lwJCEPBECompatibilityMode	Support previous lightweight cryptography versions	This setting defines whether to support previous lightweight cryptography or not.	true, false	true
engineName	Engine name	Encryption mechanism name	AES, DES, 3DES, Blowfish	AES
keySize	Key size	encryption key length in bits	For AES - 128, 192 or 256; For DES - 64; For 3DES - 192; For Blowfish - any number between 32 and 448	256
algorithmPaddingName	Algorithm padding name	Padding standards	PKCS7Padding, PKCS5Padding	PKCS7Padding

UCMDB CM Setting Name	Probe CM Setting Name	Setting Description	Possible Values	Default Value
pbeCount	PBE count	The number of times to run the hash to create the key from password (init string)	Any positive number	20
pbeDigestAlgorithm	PBE digest algorithm	Hashing type	SHA1, SHA256, MD5	SHA1
useMacWithCrypto	Use MAC with cryptography	Indication if to use MAC with the cryptography	true, false	false
macKeySize	MAC key size	Depends on MAC algorithm	256	256

🔍 Troubleshooting and Limitations

If you change the default domain name on the UCMDB server, you must first verify that the Data Flow Probe is not running. After the default domain name is applied, you must execute the **DataFlowProbe\tools\clearProbeData.bat script** on the Data Flow Probe side.

Note: Execution of the **clearProbeData.bat** script will cause a discovery cycle on the Probe side once the Probe is up.

22

Data Flow Probe Hardening

This chapter includes:

Tasks

➤ Set the MySQL Database Encrypted Password on page 358

➤ Set the JMX Console Encrypted Password on page 360

➤ Restrict the Data Flow Probe's Access to the MySQL Server on page 362

➤ Enable SSL Between UCMDB Server and Data Flow Probe with Mutual
  Authentication on page 362

➤ Enable Authentication on the Data Flow Probe with Basic HTTP
  Authentication on page 371

➤ Connect the Data Flow Probe by Reverse Proxy on page 372

➤ Control the Location of the domainScopeDocument File on page 373

➤ Create a Keystore for the Data Flow Probe on page 374

➤ Encrypt the Probe Keystore and Truststore Passwords on page 374

Reference

➤ UCMDB and Data Flow Probe Default Keystore and Truststore
  on page 376

Tasks

🔧 Set the MySQL Database Encrypted Password

This section explains how to encrypt the password for the MySQL database user.

1 Create the Encrypted Form of a Password (AES, 192-bit key)

a Access the Data Flow Probe JMX console. Launch a Web browser and enter the following address: **http://<Data Flow Probe machine name or IP address>:1977**. If you are running the Data Flow Probe locally, enter **http://localhost:1977**.

You may have to log in with a user name and password.

Note: If you have not created a user, use the default user name **sysadmin** and the password **sysadmin** to log in.

---

b Locate the **Type=MainProbe** service and click the link to open the Operations page.

c Locate the **getEncryptedDBPassword** operation.

d In the **DB Password** field, enter the password to be encrypted.

e Invoke the operation by clicking the **getEncryptedDBPassword** button.

The result of the invocation is an encrypted password string, for example:

```
66,85,54,78,69,117,56,65,99,90,86,117,97,75,50,112,65,53,67,114,112,65,61,61
```

2 Stop the Data Flow Probe

Start > **All Programs** > **HP UCMDB** > **Stop Data Flow Probe**

3 Run the set_dbuser_password.cmd Script

This script is located in the following folder:
**C:\hp\UCMDB\DataFlowProbe\tools\dbscripts
\set_dbuser_password.cmd**

Run the **set_dbuser_password.cmd** script with the new password as an argument, for example, **set_dbuser_password <my_password>**.

The password must be entered in its unencrypted form (as plain text).

4 Update the Password in the Data Flow Probe Configuration Files

a The password must reside encrypted in the configuration files. To retrieve the password's encrypted form, use the **getEncryptedDBPassword** JMX method, as explained in page 358.

b Add the encrypted password to the following properties in the **C:\hp\UCMDB\DataFlowProbe\conf\DiscoveryProbe.properties** file.

➤ **appilog.agent.probe.jdbc.pwd**

For example:

```
appilog.agent.probe.jdbc.user = mamprobe
appilog.agent.probe.jdbc.pwd =
66,85,54,78,69,117,56,65,99,90,86,117,97,75,50,112,65,53,67,114,112,65,6
1,61
```

➤ **appilog.agent.local.jdbc.pwd**

5 Start the Data Flow Probe

Start > **All Programs** > **HP UCMDB** > **Start Data Flow Probe**

The clearProbeData.bat Script: Usage

The **clearProbeData.bat** script recreates the database user with a password that is provided as an argument to the script.

After you set a password, each time you execute the **clearProbeData.bat** script, it retrieves the database password as an argument.

After running the script:

➤ Review the following file for errors:
   C:\hp\UCMDB\DataFlowProbe\runtime\log\probe_setup.log

➤ Delete the following file, as it contains the database password:
   C:\hp\UCMDB\DataFlowProbe\runtime\log\probe_setup.log

⚓ Set the JMX Console Encrypted Password

This section explains how to encrypt the password for the JMX user. The encrypted password is stored in the **DiscoveryProbe.properties** file. Users must log in to access the JMX console.

1 Create the Encrypted Form of a Password (AES, 192-bit key)

  a Access the Data Flow Probe JMX console. Launch a Web browser and enter the following address: **http://<Data Flow Probe machine name or IP address>:1977**. If you are running the Data Flow Probe locally, enter **http://localhost:1977**.

     You may have to log in with a user name and password.

     Note: If you have not created a user, use the default user name **sysadmin** and the password **sysadmin** to log in.

---

  b Locate the **Type=MainProbe** service and click the link to open the Operations page.

  c Locate the **getEncryptedKeyPassword** operation.

  d In the **Key Password** field, enter the password to be encrypted.

  e Invoke the operation by clicking the **getEncryptedKeyPassword** button.

The result of the invocation is an encrypted password string, for example:

```
85,-9,-61,11,105,-93,-81,118
```

2 Stop the Data Flow Probe

Start > **All Programs** > **HP UCMDB** > **Stop Data Flow Probe**

3 Add the Encrypted Password

Add the encrypted password to the following property in the
C:\hp\UCMDB\DataFlowProbe\conf\DiscoveryProbe.properties file.

appilog.agent.Probe.JMX.BasicAuth.Pwd

For example:

```
appilog.agent.Probe.JMX.BasicAuth.User=admin
appilog.agent.Probe.JMX.BasicAuth.Pwd=-85,-9,-61,11,105,-93,-81,118
```

Note: To disable authentication, leaves these fields empty. If you do so,
users can open the main page of the Probe's JMX console without
entering authentication.

4 Start the Data Flow Probe

a **Start** > **All Programs** > **HP UCMDB** > **Start Data Flow Probe**

b Test the result in a Web browser.

👕 Restrict the Data Flow Probe's Access to the MySQL Server

This section explains how to permit access to the Data Flow Probe's MySQL database from the local machine only.

To restrict MySQL access:

Run the following script in a command prompt window or by double-clicking it: **C:\hp\UCMDB\DataFlowProbe\tools\dbscripts\ remove_remote_user_access.cmd**.

Any user (other than the root user) trying to connect from a remote computer will now be denied access.

Note: Users who have root credentials to the MySQL database will still be able to access the database from the remote machine.

👕 Enable SSL Between UCMDB Server and Data Flow Probe with Mutual Authentication

You can set up authentication for both the Data Flow Probe and the UCMDB Server with certificates. The certificate for each component is sent and authenticated before the connection is established.

Important: The following method of enabling SSL on the Data Flow Probe with mutual authentication is the most secure of the methods and is therefore the recommended communication mode. This method replaces the procedure for basic authentication.

This section includes the following topics:

➤ "Overview" on page 363

➤ "Keystores and Truststores" on page 363

➤ "Enable Mutual Certificate Authentication" on page 364

➤ "Enable SSL with Server Authentication" on page 368

Overview

UCMDB supports the following modes of communication between the UCMDB Server and the Data Flow Probe:

➤ **Mutual Authentication**. This mode uses SSL and enables both Server authentication by the Probe and client authentication by the Server. For details, see "Enable Mutual Certificate Authentication" on page 364.

➤ **Server Authentication**. This mode uses SSL, and the Probe authenticates the UCMDB Server certificate. For details, see "Enable SSL with Server Authentication" on page 368.

➤ **Standard HTTP**. No SSL communication. This is the default mode, and the Data Flow Probe component in UCMDB does not require any certificates. Data Flow Probe communicates with the server through the standard HTTP protocol.

Keystores and Truststores

The UCMDB Server and the Data Flow Probe work with keystores and truststores:

➤ **Keystore**. A file holding key entries (a certificate and a matching private key).

➤ **Truststore**. A file holding certificates that are used to verify a remote host (for example, when using server authentication, the Data Flow Probe's truststore should include the UCMDB Server certificate).

Enable Mutual Certificate Authentication

This mode uses SSL and enables both Server authentication by the Probe and client authentication by the Server. Both the Server and the Probe send their certificates to the other entity for authentication.

Note: The following instructions use the **cKeyStoreFile** keystore as the Probe keystore. This is a predefined client keystore that is part of the UCMDB installation. For details, see "UCMDB and Data Flow Probe Default Keystore and Truststore" on page 376. However, it is recommended to create a new, unique keystore containing a newly generated private key. For details, see "Create a Keystore for the Data Flow Probe" on page 374.

---

1 Verify that both UCMDB and Data Flow Probe are running. If the Probe is installed in separate mode, these instructions refer to the Probe Gateway.

2 Harden the Data Flow Probe connector in UCMDB:

   a Access the UCMDB JMX console: Launch a Web browser and enter the following address: **http://<UCMDB machine name or IP address>:8080/jmx-console**.

     You may have to log in with a user name and password.

   b Locate **UCMDB:service=Ports Management Services** and click the link to open the Operations page.

   c Locate the **PortsDetails** operation and click **Invoke**. Make a note of the HTTPS with client authentication port number. The default is 8444 and it should be enabled.

   d Return to the Operations page.

   e To map the Data Flow Probe connector to the mutual authentication mode, invoke the **mapComponentToConnectors** method with the following parameters:

     ➤ **componentName**: mam-collectors

     ➤ **isHTTPSWithClientAuth**: true

     ➤ All other flags: false

The following message is displayed:

> Operation succeeded. Component mam-collectors is now mapped to:
> HTTPS_CLIENT_AUTH ports.

f Return to the Operations page.

g To map the Confidential Manager connector to the mutual authentication mode, invoke the **mapComponentToConnectors** method with the following parameters:

➤ **componentName**: cm

➤ **isHTTPSWithClientAuth**: true

➤ All other flags: false

The following message is displayed:

> Operation succeeded. Component cm is now mapped to:
> HTTPS_CLIENT_AUTH ports.

3 Copy the keystore to be used as the Probe keystore to the following location in the Data Flow Probe file system: **C:\HP\UCMDB\DataFlowProbe\conf\security**

Note:

➤ If you created a new keystore, use its name, otherwise, use **cKeyStoreFile**.

➤ If you are using the default client keystore (**cKeyStoreFile**), skip to step 6 on page 366.

---

4 Export the Probe certificate from its keystore.

   a On the Probe machine, run the following command:

```
C:\HP\UCMDB\DataFlowProbe\bin\jre\bin\keytool.exe -export -alias clientcert -
keystore <pKeyStoreFile> -file
C:\HP\UCMDB\DataFlowProbe\conf\security\probe.cert
```

   b Enter the Keystore password (**pKeyStorePass**).

   c Verify that the certificate is created in the following directory:
C:\HP\UCMDB\DataFlowProbe\conf\security\probe.cert

5 Import the exported Probe certificate to the UCMDB Truststore.

   a On the UCMDB machine, copy the created **probe.cert** file to the
following directory on UCMDB:
C:\HP\UCMDB\UCMDBServer\conf\security

   b Run the following command:

```
C:\HP\UCMDB\UCMDBServer\bin\jre\bin\keytool.exe -import -v -keystore
<sTrustStoreFile> -file C:\HP\UCMDB\UCMDBServer\conf\security\probe.cert -
alias probecert
```

   c Enter the UCMDB Server Truststore password (**sTrustStorePass**).

   d When asked, **Trust this certificate?**, press **y** and then ENTER.

   e Make sure the output is Certificate was added to keystore.

6 Export the UCMDB certificate from its keystore.

   a On the UCMDB machine, run the following command:

```
C:\HP\UCMDB\UCMDBServer\bin\jre\bin\keytool.exe -export -alias hpcert -
keystore <sKeyStoreFile> -file
C:\HP\UCMDB\UCMDBServer\conf\security\server.cert
```

   b Enter the Keystore password (**sKeyStorePass**).

   c Verify that the certificate is created in the following directory:
C:\HP\UCMDB\UCMDBServer\conf\security\server.cert

7 Import the exported UCMDB certificate to the Probe's truststore.

   a On the Probe machine, copy the created **server.cert** file to the Data Flow Probe at the following location: **C:\HP\UCMDB\DataFlowProbe\conf\security**

   b Run the following command:

```
C:\HP\UCMDB\DataFlowProbe\bin\jre\bin\keytool.exe -import -v -keystore
<pTrustStoreFile> -file C:\HP\UCMDB\DataFlowProbe\conf\security\server.cert -
alias ucmdbcert
```

   c Enter the Data Flow Probe truststore password (**pTrustStorePass**).

   d When asked, **Trust this certificate?**, press **y** and then ENTER.

   e Make sure the output is Certificate was added to keystore.

8 Update the Probe **ssl.properties** file, located in the following directory: **C:\HP\UCMDB\DataFlowProbe\conf\security**

   a Define the path of the keystore in the **javax.net.ssl.keyStore** property (**pKeyStoreFile**). For a limitation, see "Mutual Authentication Limitation" on page 368.

   b Define the keystore password in the **javax.net.ssl.keyStorePassword** property (encrypted **pKeyStorePass**).

   c Define the path of the truststore in the **javax.net.ssl.trustStore property** (**pTrustStoreFile**).

   d Define the truststore password in the **javax.net.ssl.trustStorePassword** property (encrypted, **pTrustStorePass**).

Note: The keystore password and truststore password properties are encrypted. For encryption instructions, see "Encrypt the Probe Keystore and Truststore Passwords" on page 374.

---

9 Update the **DiscoveryProbe.properties** file, located in the following directory: **C:\HP\UCMDB\DataFlowProbe\conf**.

    a Update the **appilog.agent.probe.protocol** property to **HTTPS**.

    b Update the **serverPortHttps** property to the relevant port number, as noted in step 2 on page 364.

10 Restart the UCMDB Server and Data Flow Probe.

Mutual Authentication Limitation

The Data Flow Probe keystore (as defined in **C:\HP\UCMDB\DataFlowProbe\conf\security\ssl.properties**) must contain only 1 (one) key entry.

Enable SSL with Server Authentication

To enable Server authentication:

1 Verify that both UCMDB and Data Flow Probe are running. If the Probe is installed in separate mode, these instructions refer to the Probe Gateway.

2 Harden the Data Flow Probe connector in UCMDB:

    a Access the UCMDB JMX console: Launch a Web browser and enter the following address: **http://<UCMDB machine name or IP address>:8080/jmx-console**.

    You may have to log in with a user name and password.

    b Locate **UCMDB:service=Ports Management Services** and click the link to open the Operations page.

    c Locate the **PortsDetails** operation and click **Invoke**. Make a note of the HTTPS port number. The default is 8443 and it should be enabled.

    d Return to the Operations page.

    e To map the Data Flow Probe connector to the mutual authentication mode, invoke the **mapComponentToConnectors** method with the following parameters:

        ➤ **componentName**: mam-collectors

        ➤ **isHTTPS**: true

➤ All other flags: false

The following message is displayed:

> Operation succeeded. Component mam-collectors is now mapped to: HTTPS ports.

f Return to the Operations page.

g To map the Confidential Manager connector to the mutual authentication mode, invoke the **mapComponentToConnectors** method with the following parameters:

➤ **componentName**: cm

➤ **isHTTPS**: true

➤ All other flags: false

The following message is displayed:

> Operation succeeded. Component cm is now mapped to: HTTPS ports.

3 Export the UCMDB certificate from its keystore.

a On the UCMDB machine, run the following command:

> C:\HP\UCMDB\UCMDBServer\bin\jre\bin\keytool.exe -export -alias hpcert -keystore <sKeyStoreFile> -file
> C:\HP\UCMDB\UCMDBServer\conf\security\server.cert

b Enter the Keystore password (**sKeyStorePass**).

c Verify that the certificate is created at **C:\HP\UCMDB\UCMDBServer\conf\security\server.cert**.

 4 Import the exported UCMDB certificate to the Probe's truststore.

 a On the Probe machine, copy the created **server.cert** file to the Data Flow Probe at the following location: **C:\HP\UCMDB\DataFlowProbe\conf\security**

 b Run the following command:

```
C:\HP\UCMDB\DataFlowProbe\bin\jre\bin\keytool.exe -import -v -keystore
<pTrustStoreFile> -file C:\HP\UCMDB\DataFlowProbe\conf\security\server.cert -
alias ucmdbcert
```

 c Enter the Data Flow Probe Truststore password (**pTrustStorePass**).

 d When asked, **Trust this certificate?**, press **y** and then ENTER.

 e Make sure the output is Certificate was added to keystore.

 5 Update the Probe **ssl.properties** file, located in the following directory: **C:\HP\UCMDB\DataFlowProbe\conf\security**

 a Define the path of the Truststore in the **javax.net.ssl.trustStore** property (**pTrustStoreFile**).

 b Define the Truststore password in the **javax.net.ssl.trustStorePassword** property (encrypted **pTrustStorePass**).

Note: The Truststore password property is encrypted. For encryption instructions, see "Encrypt the Probe Keystore and Truststore Passwords" on page 374.

---

 6 Update the **DiscoveryProbe.properties** file, located in the following directory: **C:\HP\UCMDB\DataFlowProbe\conf**

 a Update the **appilog.agent.probe.protocol** property to **HTTPS**.

 b Update the **serverPortHttps** property to the relevant port number, as noted in step 2 on page 368.

 7 Restart the UCMDB Server and Data Flow Probe.

⚒ Enable Authentication on the Data Flow Probe with Basic HTTP Authentication

Important:

➤ The basic authentication method of enabling authentication on the Data Flow Probe is the least preferred method. It is recommended to use mutual authentication security, as it is a much more effective method of security (it combines data encryption and certificate authentication). For details, see "Enable SSL Between UCMDB Server and Data Flow Probe with Mutual Authentication" on page 362.

➤ If SSL is not enabled, credentials are transmitted to UCMDB as plain-text.

To set basic authentication:

 1 Locate the following file: **C:\hp\UCMDB\DataFlowProbe\conf\ DiscoveryProbe.properties**.

 2 Remove the comment markers (#) from the following properties, and enter the relevant credentials:

```
appilog.agent.Probe.BasicAuth.Realm=
appilog.agent.Probe.BasicAuth.User=
appilog.agent.Probe.BasicAuth.Pwd=
```

The credentials should match those defined on the UCMDB server.

🔧 Connect the Data Flow Probe by Reverse Proxy

Perform the following procedure to connect the Data Flow Probe by reverse proxy.

Note: Enabling mutual authentication when using SSL between the UCMDB Server and the Data Flow Probe is not supported when the connection is made by reverse proxy.

To configure the Data Flow Probe to work against a reverse proxy:

1 Edit the **discoveryProbe.properties** file (located in **C:\hp\UCMDB\DataFlowProbe\conf**).

2 Set the **serverName** property to the reverse proxy server's IP or DNS name.

3 Set the **serverPort** and **serverPortHttps** properties to the reverse proxy server's ports.

4 Save the file.

The following proxy server configuration is required if Data Flow Probes only are connected via a reverse proxy to HP Universal CMDB:

Requests for... on the Reverse Proxy Server	Proxy Request to be Served by:
/mam-collectors	http://[HP Universal CMDB server]/mam-collectors

The following configuration is required if a SOAP adapter is used for replication via a reverse proxy to a secure (hardened) HP Universal CMDB:

Requests for... on the Reverse Proxy Server	Proxy Request to be Served by:
/axis2	http://[HP Universal CMDB server]/axis2

Connecting the Data Flow Probe and Web Clients by Reverse Proxy

The following configuration is required if both Data Flow Probes and application users are connected via a reverse proxy to HP Universal CMDB:

Requests for... on the Reverse Proxy Server	Proxy Request to be Served by:
/mam	[HP Universal CMDB server]/mam
/mam_images	[HP Universal CMDB server]/mam_images
/mam-collectors	[HP Universal CMDB server]/mam-collectors
/ucmdb	[HP Universal CMDB server]/ucmdb
/site	[HP Universal CMDB server]/site

Control the Location of the domainScopeDocument File

The Probe's file system holds (by default) both the encryption key and the domainScopeDocument file. Each time the Probe is started, the Probe retrieves the domainScopeDocument file from the server and stores it on its file system. To prevent unauthorized users from obtaining these credentials, you can configure the Probe so that the domainScopeDocument file is held in the Probe's memory and is not stored on the Probe file system.

To control the location of the domainScopeDocument file:

1 Open **C:\hp\UCMDB\DataFlowProbe\conf\DiscoveryProbe.properties** and change:

```
appilog.collectors.storeDomainScopeDocument=true
```

to:

```
appilog.collectors.storeDomainScopeDocument=false
```

The Probe Gateway and Probe Manager serverData folders no longer contain the domainScopeDocument file.

> For details on using the domainScopeDocument file to harden DFM, see "Data Flow Credentials Management" on page 327.

2 Restart the Probe.

🏌 Create a Keystore for the Data Flow Probe

1 On the Probe machine, run the following command:

```
C:\HP\UCMDB\DataFlowProbe\bin\jre\bin\keytool -genkey -alias probekey -keyalg
RSA -keystore C:\HP\UCMDB\DataFlowProbe\conf\security\client.keystore
```

2 Enter a password for the new keystore.

3 Enter your information when asked.

4 When asked **Is CN=... C=... Correct?** enter **yes**, and press ENTER.

5 Press ENTER again to accept the keystore password as the key password.

6 Verify that **client.keystore** is created in the following directory: **C:\HP\UCMDB\DataFlowProbe\conf\security**.

🏌 Encrypt the Probe Keystore and Truststore Passwords

The Probe keystore and truststore passwords are stored encrypted in **C:\HP\UCMDB\DataFlowProbe\conf\security\ssl.properties**. This procedure explains how to encrypt the password.

1 Start Data Flow Probe (or verify that it is already running).

2 Access the Data Flow Probe JMX console: Launch a Web browser and enter the following address: **http://<Data Flow Probe machine name or IP address>:1977**. If you are running the Data Flow Probe locally, enter **http://localhost:1977**.

> **Note:** You may have to log in with a user name and password. If you have not created a user, use the default user name **sysadmin** and the password **sysadmin** to log in.

3 Locate the **Type=MainProbe** service and click the link to open the Operations page.

4 Locate the **getEncryptedKeyPassword** operation.

5 Enter your keystore or truststore password in the **Key Password** field and invoke the operation by clicking **getEncryptedKeyPassword**.

6 The result of the invocation is an encrypted password string, for example:

```
66,85,54,78,69,117,56,65,99,90,86,117,97,75,50,112,65,53,67,114,112,65,61,61
```

7 Copy and paste the encrypted password into the line relevant to either the keystore or the truststore in the following file: **C:\HP\UCMDB\DataFlowProbe\conf\security\ssl.properties**.

Reference

🔍 UCMDB and Data Flow Probe Default Keystore and Truststore

This section includes the following topics:

➤ "UCMDB" on page 376

➤ "Data Flow Probe" on page 377

UCMDB

The files are located in the following directory:
C:\HP\UCMDB\UCMDBServer\conf\security.

Entity	File Name/Term	Password/Term	Alias
Server keystore	server.keystore (sKeyStoreFile)	hppass (sKeyStorePass)	hpcert
Server truststore	server.truststore (sTrustStoreFile)	hppass (sTrustStorePass)	clientcert (default trusted entry)
Client keystore	client.keystore (cKeyStoreFile)	clientpass (cKeyStorePass)	clientcert

Data Flow Probe

The files are located in the following directory:
C:\HP\UCMDB\DataFlowProbe\conf\security.

Entity	File Name/Term	Password/Term	Alias
Probe keystore	MAMKeyStoreExp.jks (pKeyStoreFile)	logomania (pKeyStorePass)	mam
Data Flow Probe uses the **cKeyStoreFile** keystore as the default keystore during the mutual authentication procedure. This is a client keystore that is part of the UCMDB installation.			
Probe truststore	MAMTrustStoreExp.jks (pTrustStoreFile)	logomania (pTrustStorePass)	mam (default trusted entry)
The **cKeyStorePass** password is the default password of **cKeyStoreFile**.			

23

Lightweight Single Sign-On Authentication (LW-SSO) – General Reference

This chapter includes:

Concepts

➤ LW-SSO Authentication Overview on page 380

Reference

➤ LW-SSO System Requirements on page 382

➤ LW-SSO Security Warnings on page 383

Troubleshooting and Limitations on page 385

Concepts

🔧 LW-SSO Authentication Overview

LW-SSO is a method of access control that enables a user to log on once and gain access to the resources of multiple software systems without being prompted to log on again. The applications inside the configured group of software systems trust the authentication, and there is no need for further authentication when moving from one application to another.

The information in this section applies to LW-SSO version 2.2 and 2.3.

This section includes the following topics:

➤ "LW-SSO Token Expiration" on page 380

➤ "Recommended Configuration of the LW-SSO Token Expiration" on page 380

➤ "GMT Time" on page 381

➤ "Multi-domain Functionality" on page 381

➤ "Get SecurityToken for URL Functionality" on page 381

LW-SSO Token Expiration

The LW-SSO Token's expiration value determines the application's session validity. Therefore, its expiration value should be at least the same value as that of the application session expiration value.

Recommended Configuration of the LW-SSO Token Expiration

Each application using LW-SSO should configure token expiration. The recommended value is 60 minutes. For an application that does not require a high level of security, it is possible to configure a value of 300 minutes.

GMT Time

All applications participating in an LW-SSO integration must use the same GMT time with a maximum difference of 15 minutes.

Multi-domain Functionality

Multi-domain functionality requires that all applications participating in LW-SSO integration configure the trustedHosts settings (or the **protectedDomains** settings), if they are required to integrate with applications in different DNS domains. In addition, they must also add the correct domain in the **lwsso** element of the configuration.

Get SecurityToken for URL Functionality

To receive information sent as a **SecurityToken for URL** from other applications, the host application should configure the correct domain in the **lwsso** element of the configuration.

Reference

🔍 LW-SSO System Requirements

The following table lists LW-SSO configuration requirements:

Application	Version	Comments
Java	1.5 and higher	
HTTP Sevlets API	2.1 and higher	
Internet Explorer	6.0 and higher	Browser should enable HTTP session cookie and HTTP 302 Redirect functionality.
FireFox	2.0 and higher	Browser should enable HTTP session cookie and HTTP 302 Redirect functionality.
JBoss Authentications	JBoss 4.0.3 JBoss 4.3.0	
Tomcat Authentications	Standalone Tomcat 5.0.28 Standalone Tomcat 5.5.20	
Acegi Authentications	Acegi 0.9.0 Acegi 1.0.4	
Spring Security Authentication	Spring Security 2.0.4	
Web Services Engines	Axis 1 - 1.4 Axis 2 - 1.2 JAX-WS-RI 2.1.1	

🔍 LW-SSO Security Warnings

This section describes security warnings that are relevant to the LW-SSO configuration:

➤ **Confidential InitString parameter in LW-SSO.** LW-SSO uses Symmetric Encryption to validate and create a LW-SSO token. The **initString** parameter within the configuration is used for initialization of the secret key. An application creates a token, and each application using the same initString parameter validates the token.

Caution:

➤ It is not possible to use LW-SSO without setting the **initString** parameter.

➤ The **initString** parameter is confidential information and should be treated as such in terms of publishing, transporting, and persistency.

➤ The **initString** parameter should be shared only between applications integrating with each other using LW-SSO.

➤ The **initString** parameter should have a minimum length of 12 characters.

➤ **Enable LW-SSO only if required.** LW-SSO should be disabled unless it is specifically required.

➤ **Level of authentication security.** The application that uses the weakest authentication framework and issues a LW-SSO token that is trusted by other integrated applications determines the level of authentication security for all the applications.

It is recommended that only applications using strong and secure authentication frameworks issue an LW-SSO token.

➤ **Symmetric encryption implications.** LW-SSO uses symmetric cryptography for issuing and validating LW-SSO tokens. Therefore, any application using LW-SSO can issue a token to be trusted by all other applications sharing the same **initString** parameter. This potential risk is relevant when an application sharing an initString either resides on, or is accessible from, an untrusted location.

➤ **User mapping (Synchronization).** The LW-SSO framework does not ensure user mapping between the integrated applications. Therefore, the integrated application must monitor user mapping. We recommend that you share the same user registry (as LDAP/AD) among all integrated applications.

Failure to map users may cause security breaches and negative application behavior. For example, the same user name may be assigned to different real users in the various applications.

In addition, in cases where a user logs onto an application (AppA) and then accesses a second application (AppB) that uses container or application authentication, the failure to map the user will force the user to manually log on to AppB and enter a user name. If the user enters a different user name than was used to log on to AppA, the following behavior can arise: If the user subsequently accesses a third application (AppC) from AppA or AppB, then they will access it using the user names that were used to log on to AppA or AppB respectively.

➤ **Identity Manager.** Used for authentication purposes, all unprotected resources in the Identity Manager must be configured with the **nonsecureURLs** setting in the LW-SSO configuration file.

➤ **LW-SSO Demo mode**.

➤ The Demo mode should be used for demonstrative purposes only.

➤ The Demo mode should be used in unsecured networks only.

➤ The Demo mode must not be used in production. Any combination of the Demo mode with the production mode should not be used.

🔍 Troubleshooting and Limitations

Known Issues

This section describes known issues for LW-SSO authentication.

➤ **Security context.** The LW-SSO security context supports only one attribute value per attribute name.

Therefore, when the SAML2 token sends more than one value for the same attribute name, only one value is accepted by the LW-SSO framework.

Similarly, if the IdM token is configured to send more than one value for the same attribute name, only one value is accepted by the LW-SSO framework.

➤ **Multi-domain logout functionality when using Internet Explorer 7**. Multi-domain logout functionality may fail under the following conditions:

  ➤ The browser used is Internet Explorer 7 and the application is invoking more than three consecutive HTTP 302 redirect verbs in the logout procedure.

In this case, Internet Explorer 7 may mishandle the HTTP 302 redirect response and display an **Internet Explorer cannot display the webpage** error page instead.

As a workaround, it is recommended to reduce, if possible, the number of application redirect commands in the logout sequence.

Limitations

Note the following limitations when working with LW-SSO authentication:

➤ **Client access to the application**.

  If a domain is defined in the LW-SSO configuration:

  ➤ The application clients must access the application with a Fully Qualified Domain Name (FQDN) in the login URL, for example, http://myserver.**companydomain**.com/WebApp.

  ➤ LW-SSO cannot support URLs with an IP address, for example, http://192.168.12.13/WebApp.

➤ LW-SSO cannot support URLs without a domain, for example, http://myserver/WebApp.

If a domain is not defined in the LW-SSO configuration: The client can access the application without a FQDN in the login URL. In this case, a LW-SSO session cookie is created specifically for a single machine without any domain information. Therefore, the cookie is not delegated by the browser to another, and does not pass to other computers located in the same DNS domain. This means that LW-SSO does not work in the same domain.

➤ **LW-SSO framework integration.** Applications can leverage and use LW-SSO capabilities only if integrated within the LW-SSO framework in advance.

➤ **Multi-Domain Support**.

  ➤ Multi-domain functionality is based on the HTTP referrer. Therefore, LW-SSO supports links from one application to another and does not support typing a URL into a browser window, except when both applications are in the same domain.

  ➤ The first cross domain link using **HTTP POST** is not supported.

  Multi domain functionality does not support the first **HTTP POST** request to a second application (only the **HTTP GET** request is supported). For example, if your application has an HTTP link to a second application, an **HTTP GET** request is supported, but an **HTTP FORM** request is not supported. All requests after the first can be either **HTTP POST** or **HTTP GET**.

  ➤ LW-SSO Token size:

  The size of information that LW-SSO can transfer from one application in one domain to another application in another domain is limited to 15 Groups/Roles/Attributes (note that each item may be an average of 15 characters long).

➤ Linking from Protected (HTTPS) to non-protected (HTTP) in a multi-domain scenario:

Multi domain functionality does not work when linking from a protected (HTTPS) to a non-protected (HTTP) page. This is a browser limitation where the referrer header is not sent when linking from a protected to a non-protected resource. For an example, see: http://support.microsoft.com/support/kb/articles/Q178/0/66.ASP

➤ Third-Party cookie behavior in Internet Explorer:

Microsoft Internet Explorer 6 contains a module that supports the "Platform for Privacy Preferences (P3P) Project," meaning that cookies coming from a Third Party domain are blocked by default in the Internet security zone. Session cookies are also considered Third Party cookies by IE, and therefore are blocked, causing LW-SSO to stop working. For details, see: http://support.microsoft.com/kb/323752/en-us.

To solve this issue, add the launched application (or a DNS domain subset as ***.mydomain.com**) to the Intranet/Trusted zone on your computer (in Microsoft Internet Explorer, select **Menu** > **Tools** > **Internet Options** > **Security** > **Local intranet** > **Sites** > **Advanced**), which causes the cookies to be accepted.

Caution: The LW-SSO session cookie is only one of the cookies used by the Third Party application that is blocked.

➤ **SAML2 token.**

  ➤ Logout functionality is not supported when the SAML2 token is used.

  Therefore, if the SAML2 token is used to access a second application, a user who logs out of the first application is not logged out of the second application.

  ➤ The SAML2 token's expiration is not reflected in the application's session management.

  Therefore, if the SAML2 token is used to access a second application, each application's session management is handled independently.

➤ **JAAS Realm.** The JAAS Realm in Tomcat is not supported.

➤ **Using spaces in Tomcat directories.** Using spaces in Tomcat directories is not supported.

It is not possible to use LW-SSO when a Tomcat installation path (folders) includes spaces (for example, Program Files) and the LW-SSO configuration file is located in the **common\classes** Tomcat folder.

➤ **Load balancer configuration.** A load balancer deployed with LW-SSO must be configured to use sticky sessions.

➤ **Demo mode**. In Demo mode, LW-SSO supports links from one application to another but does not support typing a URL into a browser window, due to an HTTP referrer header absence in this case.

24

HP Universal CMDB Login Authentication

This chapter includes:

Concepts

➤ Set Up an Authentication Method on page 390

Tasks

➤ Enable and Define the LDAP Authentication Method on page 391

➤ Set a Secure Connection with the SSL (Secure Sockets Layer) Protocol on page 392

➤ Use the JMX Console to Test LDAP Connections on page 393

➤ Configure LDAP Settings Using the JMX Console on page 394

➤ Enable Login to HP Universal CMDB with LW-SSO on page 395

➤ Retrieve Current LW-SSO Configuration in Distributed Environment on page 396

Concepts

🍥 Set Up an Authentication Method

To perform authentication, you can work:

➤ **Against the internal HP Universal CMDB service.**

➤ **Through the Lightweight Directory Access Protocol (LDAP)**. You can use a dedicated, external LDAP server to store the authentication information instead of using the internal HP Universal CMDB service. The LDAP server must reside on the same subnet as all the HP Universal CMDB servers.

For details on LDAP, see "LDAP Mapping" in the *HP Universal CMDB Administration Guide*.

The default authentication method uses the internal HP Universal CMDB service. If you use the default method, you do not have to make any changes to the system.

These options apply to logins performed through Web services as well as through the user interface.

➤ **Through LW-SSO**. HP Universal CMDB is configured with LW-SSO. LW-SSO enables you to log in to HP Universal CMDB and automatically have access to other configured applications running on the same domain, without needing to log in to those applications.

When LW-SSO Authentication Support is enabled (it is disabled by default), you must ensure that the other applications in the Single Sign-On environment have LW-SSO enabled and are working with the same initString parameter.

Tasks

🔧 Enable and Define the LDAP Authentication Method

You can enable and define the LDAP authentication method for an
HP Universal CMDB system.

To enable and define the LDAP authentication method:

1 Select **Administration** > **Infrastructure Settings** > **LDAP General** category.

2 Select **LDAP server URL** and enter the LDAP URL value, using the format:

```
ldap://<ldapHost>[:<port>]/[<baseDN>][??scope]
```

For example:

```
ldap://my.ldap.server:389/ou=People,o=myOrg.com??sub
```

3 Select the **LDAP Group Definition** category, locate **Groups base DN**, and
enter the distinguished name of the general group.

4 Locate **Root groups base DN** and enter the distinguished name of the root
group.

5 Select the **LDAP General** category, locate **Enable User Synchronization**,
and verify that the value is set to **True.**

6 Select the **LDAP General Authentication** category, locate **Password of
Search-Entitled User**, and fill in the password.

7 Save the new values. To replace an entry with the default value, click
Restore Default.

8 Map LDAP user groups to UCMDB user roles. For details, see
"HP Universal CMDB Login Authentication" on page 389.

The default protocol used to communicate with the LDAP server is TCP, but
you can change the protocol to SSL. For details, see "Set a Secure Connection
with the SSL (Secure Sockets Layer) Protocol" on page 392.

🔨 Set a Secure Connection with the SSL (Secure Sockets Layer) Protocol

Since the login process involves the passing of confidential information between HP Universal CMDB and the LDAP server, you can apply a certain level of security to the content. You do this by enabling SSL communication on the LDAP server and configuring HP Universal CMDB to work using SSL.

HP Universal CMDB supports SSL that uses a certificate issued by a trusted Certification Authority (CA). This CA is included with the Java runtime environment.

Most LDAP servers, including Active Directory, can expose a secure port for an SSL based connection. If you are using Active Directory with a private CA, you may need to add your CA to the trusted CAs in Java.

For details on configuring the HP Universal CMDB platform to support communication using SSL, see "Enabling Secure Sockets Layer (SSL) Communication" on page 303.

To add a CA to trusted CAs to expose a secure port for an SSL based connection:

1 Export a certificate from your CA and import it into the JVM that is used by HP Universal CMDB, using the following steps:

  a On the UCMDB Server machine, access the **UCMDBServer\bin\JRE\bin** folder.

  b Run the following command:

```
Keytool -import -file <your certificate file> -keystore
C:\hp\UCMDB\UCMDBServer\bin\JRE\lib\security\cacerts
```

For example:

```
Keytool -import -file c:\ca2ss_ie.cer -keystore
C:\hp\UCMDB\UCMDBServer\bin\JRE\lib\security\cacerts
```

2 Select **Administration** > **Infrastructure Settings** > **LDAP General** category.

> **Note:** It is also possible to configure these settings using the JMX console. For details, see "Configure LDAP Settings Using the JMX Console" on page 394.

3 Locate **LDAP Server URL**, and enter a value, using the format:

```
ldaps://<ldapHost>[:<port>]/[<baseDN>][??scope]
```

For example:

```
ldaps://my.ldap.server:389/ou=People,o=myOrg.com??sub
```

Note the **s** in **ldaps**.

4 Click **Save** to save the new value or **Restore Default** to replace the entry with the default value (a blank URL).

🔧 Use the JMX Console to Test LDAP Connections

This section describes a method of testing the LDAP authentication configuration using the JMX console.

1 Launch your Web browser and enter the following address: **http://<server_name>:8080/jmx-console**, where **<server_name>** is the name of the machine on which HP Universal CMDB is installed.

You may need to log in with a user name and password.

2 Under **UCMDB**, click **UCMDB-UI:name=LDAP Settings** to open the Operations page.

3 Locate **testLDAPConnection**.

4 In the **Value** box for the parameter **customer id**, enter the customer ID.

5 Click **Invoke**.

The JMX MBEAN Operation Result page indicates whether the LDAP connection is successful. If the connection is successful, the page also shows the LDAP root groups.

🦜 Configure LDAP Settings Using the JMX Console

This section describes how to configure LDAP authentication settings using the JMX console.

To configure LDAP authentication settings:

1 Launch your Web browser and enter the following address: **http://<server_name>:8080/jmx-console**, where **<server_name>** is the name of the machine on which HP Universal CMDB is installed.

You may need to log in with a user name and password.

2 Under **UCMDB**, click **UCMDB-UI:name=LDAP Settings** to open the Operations page.

3 To view the current LDAP authentication settings, locate the **getLDAPSettings** method. Click **Invoke**. A table displays all the LDAP settings and their values.

4 To change the values of LDAP authentication settings, locate the **configureLDAP method**. Enter the values for the relevant settings and click **Invoke**. The JMX MBEAN Operation Result page indicates whether the LDAP authentication settings were updated successfully.

Note: If you do not enter a value for a setting, the setting retains its current value.

---

5 After configuring the LDAP settings, you can verify the LDAP user credentials. Locate the **verifyLDAPCredentials** method. Enter the customer ID, username, and password and click **Invoke**. The JMX MBEAN Operation Result page indicates whether the user passes LDAP authentication.

🔨 Enable Login to HP Universal CMDB with LW-SSO

To enable LW-SSO for HP Universal CMDB, use one of the following procedures:

Enable LW-SSO Through the JMX Console

1 Access the JMX console by entering the following address into your Web browser: **http://<server_name>:8080/jmx-console**, where **<server_name>** is the name of the machine on which HP Universal CMDB is installed.

2 Under **UCMDB-UI**, click the **name=LW-SSO Configuration** to open the Operations page.

3 Set the init string using the **setInitString** method.

4 Set the domain name of the machine on which UCMDB is installed using the **setDomain** method.

5 Invoke the method **setEnabledForUI** with the parameter set to **True**.

6 **Optional**. If you want to work using multi-domain functionality, select the **addTrustedDomains** method, enter the domain values and click **Invoke**.

7 **Optional**. If you want to work using a reverse proxy, select the **updateReverseProxy** method, set the **Is reverse proxy enabled** parameter to **True**, enter a URL for the **Reverse proxy full server URL** parameter, and click **Invoke**. If you want to access UCMDB both directly and using a reverse proxy, set the following additional configuration: select the **setReverseProxyIPs** method, enter the IP address for the **Reverse proxy ip/s** parameter and click **Invoke**.

8 **Optional**. If you want to access UCMDB using an external authentication point, select the **setValidationPointHandlerEnable** method, set the **Is validation point handler enabled** parameter to **True**, enter the URL for the authentication point in the **Authentication point server** parameter, and click **Invoke**.

9 To view the LW-SSO configuration as it is saved in the settings mechanism, invoke the **retrieveConfigurationFromSettings** method.

10 To view the actual loaded LW-SSO configuration, invoke the **retrieveConfiguration** method.

Enable LW-SSO Through UCMDB Infrastructure Settings

1 Log on to HP Universal CMDB.

2 Select **Administration** > **Infrastructure Settings** > **General Settings** category.

3 Enter domain name and initString parameter values for the **LW-SSO domain** and **LW-SSO init string** options.

4 Change **UI LW-SSO enabling state** to **True**.

5 Optional. Set additional LW-SSO configuration parameters, using the relevant settings entries. For details about additional parameters, see "LW-SSO Authentication Overview" on page 380.

6 Restart the server.

🔧 Retrieve Current LW-SSO Configuration in Distributed Environment

When UCMDB is embedded in a distributed environment, for example, in a BSM deployment, perform the following procedure to retrieve the current LW-SSO configuration on the processing machine.

To retrieve the current LW-SSO configuration:

1 Launch a Web browser and enter the following address: http://localhost.<domain_name>:8080/jmx-console.

You may be asked for a user name and password.

2 Locate **UCMDB:service=Security Services** and click the link to open the Operations page.

3 Locate the **retrieveLWSSOConfiguration** operation.

4 Click **Invoke** to retrieve the configuration.

25

Confidential Manager

This chapter includes:

Concepts

➤ Confidential Manager Overview on page 398

➤ Security Considerations on page 398

Tasks

➤ Configure the HP Universal CMDB Server on page 399

Reference

➤ Definitions on page 401

➤ Encryption Properties on page 402

Concepts

🔩 Confidential Manager Overview

The Confidential Manager (CM) framework solves the problem of managing and distributing sensitive data for HP Universal CMDB and other HP Software products.

CM consists of two main components: the client and the server. These two components are responsible for transferring data in a secured manner.

➤ The CM client is a library used by applications to access sensitive data.

➤ The CM server receives requests from CM clients, or from third party clients, and performs the required tasks. The CM server is responsible for saving the data in a secure manner.

CM encrypts credentials in transport, in the client cache, in persistency, and in memory. CM uses symmetric cryptography for transporting credentials between the CM client and the CM server by using a shared secret. CM uses various secrets for encryption of cache, persistency, and transport according to the configuration.

For detailed guidelines for managing credential encryption on the Data Flow Probe, see "Data Flow Credentials Management" on page 327.

🔩 Security Considerations

➤ You can use the following key sizes for the security algorithm: 128-, 192-, and 256-bits. The algorithm runs faster with the smaller key but it is less secure. The 128-bit size is secure enough in most cases.

➤ To make the system more secure, use MAC: set **useMacWithCrypto** to **true**. For details, see "Encryption Properties" on page 402. However, this parameter setting increases the database size.

➤ To leverage strong customer security providers, you can use the JCE mode.

Tasks

⚒ Configure the HP Universal CMDB Server

When working with HP Universal CMDB, you should configure the secret and crypto-properties of the encryption, using the following JMX methods:

1 On the HP Universal CMDB Server machine, launch the Web browser and enter the Server address, as follows: **http://<UCMDB Server Host Name or IP>:8080/jmx-console**.

You may have to log in with a user name and password.

2 Under UCMDB, click **UCMDB:service=Security Services** to open the Operations page.

3 To retrieve the current configuration, locate the **CMGetConfiguration** operation.

Click **Invoke** to display the CM server configuration XML file.

4 To make changes to the configuration, copy the XML that you invoked in the previous step to a text editor. Make changes according to the table in "Encryption Properties" on page 402.

Locate the **CMSetConfiguration** operation. Copy the updated configuration into the **Value** box and click **Invoke**. The new configuration is written to the UCMDB Server.

5 To add users to Confidential Manager for authorization and replication, locate the **CMAddUser** operation. This process is also useful in the replication process. In replication, the server slave should communicate with the server master, using a privileged user.

> ➤ **username**. The user name.

> ➤ **customer**. The default is ALL_CUSTOMERS.

> ➤ **resource**. The resource name. The default is ROOT_FOLDER.

➤ **permission**. Choose between ALL_PERMISSIONS, CREATE, READ, UPDATE, and DELETE. The default is ALL_PERMISSIONS.

Click **Invoke**.

6 If necessary, restart HP Universal CMDB.

Note:

In most cases there is no need to restart the Server. You may need to restart the Server when changing one of the following resources:

➤ Storage type

➤ Database table name or column names

➤ The creator of the database connection

➤ The connection properties to the database (that is, URL, user, password, driver class name)

➤ Database type

Note:

➤ It is important that the UCMDB Server and its clients have the same transport crypto-properties. If these properties are changed on the UCMDB Server, you must change them on all clients. (This is not relevant for Data Flow Probe, because it runs on the same process with the UCMDB Server—that is, there is no need for the Transport crypto-configuration.)

➤ CM Replication is not configured by default, and can be configured if needed.

➤ If CM Replication is enabled, and the Transportation **initString** or any other crypto-property of the master changes, all slaves must adopt the changes.

Reference

🔍 Definitions

Storage crypto-properties. The configuration that defines how the server holds and encrypts the data (in database or file, which crypto-properties must encrypt or decrypt the data, and so on), how credentials are stored in a secure manner, how encryption is processed, and according to which configuration.

Transport crypto-properties. Transport configuration defines how the server and the clients encrypt the transportation between them, which configuration is used, how credentials are transferred in a secure manner, how encryption is processed, and according to which configuration. You must use the same crypto-properties for transport encryption and decryption, in both server and client.

Replications and replication crypto-properties. Data held securely by CM is securely replicated between several servers. These properties define how the data is to be transferred between slave server and master server.

Note:

➤ The database table that holds the CM server configuration is named: **CM_CONFIGURATION**.

➤ The CM Server default configuration file is located in **app-infra.jar** and is named **defaultCMServerConfig.xml**.

🔍 Encryption Properties

The following table describes encryption properties. For details on using these parameters, see "Configure the HP Universal CMDB Server" on page 399.

Parameter	Description	Recommended value
encryptTransportMode	Encrypt the transported data: ➤ true ➤ false	true
encryptDecryptInitString	Password for encryption	Longer than 8 characters
cryptoSource	Encryption implementation library to use: ➤ lw ➤ jce ➤ windowsDPAPI ➤ lwJCECompatible	lw
lwJCEPBECompatibilityMode	Support previous versions of lightweight cryptography: ➤ true ➤ false	true
cipherType	The type of cipher that CM uses. CM supports one value only: **symmetricBlockCipher**	symmetric BlockCipher
engineName	➤ AES ➤ Blowfish ➤ DES ➤ 3DES ➤ Null (no encryption)	AES

Parameter	Description	Recommended value
algorithmModeName	Mode of block encryption algorithm: ➤ CBC	CBC
algorithmPaddingName	Padding standards: ➤ PKCS7Padding ➤ PKCS5Padding	PKCS7Padding
keySize	Depends on algorithm (what **engineName** supports)	256
pbeCount	The number of times to run the hash to create the key from **encryptDecryptInitString**. Any positive number.	1000
pbeDigestAlgorithm	Hashing type: ➤ SHA1 ➤ SHA256 ➤ MD5	SHA256
encodingMode	ASCII representation of the encrypted object: ➤ Base64 ➤ Base64Url	Base64Url
useMacWithCrypto	Defines whether MAC is used with the cryptography: ➤ true ➤ false	false
macType	Type of message authentication code (MAC): ➤ hmac	hmac

Parameter	Description	Recommended value
macKeySize	Depends on Mac algorithm	256
macHashName	The Hash Mac algorithm: ➤ SHA256	SHA256

Part VII

Disaster Recovery

26

Disaster Recovery Setup

This chapter includes:

Concepts

➤ Disaster Recovery Overview on page 408

Tasks

➤ Prepare the Disaster Recovery Environment on page 409

➤ Prepare the HP Universal CMDB Failover Instance for Activation
  on page 412

➤ Perform Startup Cleanup Procedure on page 412

Concepts

🔵 Disaster Recovery Overview

This chapter describes the basic principles and guidelines on how to set up a Disaster Recovery system, and the required steps to make a secondary HP Universal CMDB system become the new primary system. The chapter covers a typical HP Universal CMDB environment consisting of one HP Universal CMDB server and one database server containing HP Universal CMDB database schemas.

Note:

➤ This chapter is a high level guide to introduce concepts of enabling disaster recovery.

➤ Disaster Recovery involves manual steps in moving various configuration files and updates to the HP Universal CMDB database schemas. This procedure requires at least one HP Universal CMDB administrator and one database administrator who is familiar with the HP Universal CMDB databases and schemas.

➤ There are a number of different possible deployment and configurations for HP Universal CMDB. To validate that the Disaster Recovery scenario works in a particular environment, it should be thoroughly tested and documented. You should contact HP Professional Services to ensure best practices are used in the design and failover workflow for any Disaster Recovery scenario.

Tasks

🔧 Prepare the Disaster Recovery Environment

Preparing the Disaster Recovery environment comprises the following stages:

➤ "Install HP Universal CMDB Software in the Failover Environment" on page 409

➤ "Configure System and Data Backup" on page 410

Install HP Universal CMDB Software in the Failover Environment

Install a second instance of HP Universal CMDB that matches your current production environment.

➤ Install exactly the same version of HP Universal CMDB in your backup environment, as that used in your production environment.

➤ To simplify issues with disparate capacities and deployments, the backup environment should be the same as your production environment.

➤ Do not run the Server and Database Configuration utility and do not create any databases.

➤ Do not start the Backup system.

Note: The Disaster Recovery environment should closely resemble the HP Universal CMDB production environment. The hardware, deployment, and versions should all be matched to prevent any loss of functionality when moving to the Failover system.

Configure System and Data Backup

This stage includes copying configuration directories to the Failover instance and configuring database log file shipping.

Copying Configuration Directories to the Failover Instance

Copy from the HP Universal CMDB Production instance to the same server type in the Failover instance, any files changed in the following directories:

➤ UCMDBServer\conf

➤ UCMDBServer\content\

Also copy any other files or directories in the system that are customized.

Note: It is recommended that you perform backups of HP Universal CMDB servers at least daily. Depending on the number and interval of configuration changes, it may be necessary to incorporate a faster interval to prevent a large loss of configuration changes in the event of losing the Production instance.

Microsoft SQL Server–Configure Database Log File Shipping

To provide the most up-to-date monitoring and configuration data, it is critical to enable log file shipping to minimize the time in data gaps. By using log file shipping, you can create an exact duplicate of the original database, out of date only by the delay in the copy-and-load process. You then have the ability to make the standby database server a new primary database server, if the original primary database server becomes unavailable. When the original primary server becomes available again, you can make it a new standby server, effectively reversing the servers' roles.

The log file shipping must be configured for the following HP Universal CMDB databases:

➤ HP Universal CMDB database

➤ HP Universal CMDB History database

This section does not contain the specific steps to configure log file shipping. The HP Universal CMDB database administrator can use the following links as a guide to configure log file shipping for the appropriate version of database software that is used in the HP Universal CMDB environment:

Microsoft SQL Server 2005:

➤ msdn.microsoft.com/en-us/library/ms188625(v=SQL.90).aspx

➤ msdn.microsoft.com/en-us/library/ms190016(v=SQL.90).aspx

➤ msdn.microsoft.com/en-us/library/ms187016(v=SQL.90).aspx

Microsoft SQL Server 2008:

➤ msdn2.microsoft.com/en-us/library/ms188625.aspx

➤ msdn2.microsoft.com/en-us/library/ms190016.aspx

➤ msdn2.microsoft.com/en-us/library/ms187016.aspx

Oracle–Configure the Standby Database (Data Guard)

Oracle only has logs at the database level, not for each schema. This means that you cannot make a standby database on the schema level, and must create copies of the production system databases on your backup system.

Note: HP recommends that if Oracle is the database platform, Oracle 11i should be used to utilize Data Guard.

This section does not contain the specific steps to configure a Standby database. The HP Universal CMDB database administrator can use the following link as a guide to configure a Standby database for Oracle 11i:

http://download.oracle.com/docs/cd/B19306_01/server.102/b14239/toc.htm

Upon successful completion of the Backup database configuration, the HP Universal CMDB Failover database should be synchronized with the HP Universal CMDB Production database.

⚒ Prepare the HP Universal CMDB Failover Instance for Activation

When it is time to activate the Failover instance, perform the following steps in the Failover environment:

➤ Activate the Backup system, including its database.

➤ Ensure that all the latest database logs have been updated into the Failover environment's databases.

➤ Run the Perform Startup Cleanup Procedure to remove any localization in the databases. For details, see "Perform Startup Cleanup Procedure" on page 412.

⚒ Perform Startup Cleanup Procedure

This procedure cleans up all the machine specific references in the configurations from the Production instance. It is needed to reset the database on the Backup system.

Note:

➤ Before starting the activation procedures, the HP Universal CMDB Administrator should ensure that the appropriate license has been applied to the Failover instance.

➤ HP recommends that an experienced database administrator perform the SQL statements included in this procedure.

---

 1 Empty and update tables:

```
update CUSTOMER_REGISTRATION set CLUSTER_ID=null;
truncate table CLUSTER_SERVER;
truncate table SERVER;
truncate table CLUSTERS;
```

2 Run the Server and Database Configuration utility.

Run the Server and Database Configuration utility on each machine to re-initialize the needed tables in the database. To run the Server and Database Configuration utility, select **Start** > **All Programs** > **HP UCMDB** > **Start HP Universal CMDB Configuration Wizard**.

Note:

➤ When running the Server and Database Configuration utility, make sure to reconnect to the same databases that were created for the Failover environment (that is, the one to which the backup data was shipped). A complete loss of configuration data may result if the utility is run on the Production instance.

➤ When prompted for the databases by the Server and Database Configuration utility, ensure that you enter the names of the new databases in the Failover environment.

---

3 Start the servers.

To perform disaster recovery from a high availability system, start one of the HP Universal CMDB servers, run the System Configuration tool on that server to configure a cluster, and add new Failover servers to this cluster.

4 Bring up the Backup Environment.

Start HP Universal CMDB in the Failover environment.

Part VIII

Getting Started With HP Universal CMDB

27

Accessing HP Universal CMDB Through the IIS Web Server

This chapter includes:

Concepts

➤ Accessing HP Universal CMDB Through IIS Overview on page 418

Tasks

➤ Set Up IIS to Enable Access to UCMDB – Windows 2003 on page 419

➤ Set Up IIS to Enable Access to UCMDB – Windows 2008 on page 423

➤ Configure the Data Flow Probe on page 427

Concepts

Accessing HP Universal CMDB Through IIS Overview

This chapter describes how to access HP Universal CMDB using the Microsoft Internet Information Services (IIS) Web server.

You can set up the IIS Web server to enable end users and clients of HP Universal CMDB (for example, the Data Flow Probe) to access the system via the IIS Web server. In this setup, end users and clients of HP Universal CMDB use the IIS machine's URL to access UCMDB, instead of using the UCMDB machine URL.

This section includes the following topics:

➤ "Software Required for Integration" on page 418

➤ "Supported Configurations 9.04" on page 418

Software Required for Integration

The following table describes the software required for integration:

IIS Web Server	Version 6.0, 7.X
HP Universal CMDB Server	Version 9.04 or later

Supported Configurations 9.04

The following configurations are supported for this integration:

➤ Windows 2003/8 64-bit, HP Universal CMDB 9.04 or later and IIS 6 or 7.X on the **same** server.

➤ Windows 2003/8 64-bit, HP Universal CMDB 9.04 or later and IIS 6 or 7.X on **separate** servers.

Tasks

🔨 Set Up IIS to Enable Access to UCMDB – Windows 2003

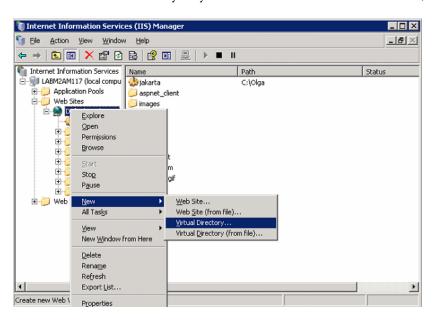This section outlines the procedure to integrate HP Universal CMDB and IIS for Windows 2003.

To manually integrate HP Universal CMDB and IIS:

1 If the HP Universal CMDB server does not reside on the same machine as IIS, copy all the files from the **C:\hp\UCMDB\UCMDBServer\tools\iis_integration** directory to the **c:\ucmdb_iis** folder on the IIS machine. On the IIS machine, modify the following files:

  a In the **workers.properties.minimal** file, change the string **worker.localAjp.host=localhost** to the UCMDB server hostname.

  b In the **isapi_redirect.properties** file:

    ➤ The **log_file** should point to a folder containing the integration logs, for example, **c:\ucmdb_iis\isapi.log**.

    ➤ The **worker_file** should contain the location of the **workers.properties.minimal** file, for example, **C:\ucmdb_iis\workers.properties.minimal**.

    ➤ The **worker_mount_file** should contain the location of the **uriworkermap.properties** file, for example **C:\ucmdb_iis\uriworkermap.properties**.

2 If the HP Universal CMDB server resides on the same machine as IIS, modify the **isapi_redirect.properties** file in the **C:\hp\UCMDB\UCMDBServer\tools\iis_integration** directory as follows:

  a The **log_file** should point to a folder containing the integration logs, for example, **C:\hp\UCMDB\UCMDBServer\runtime\log\isapi.log**.

  b The **worker_file** should contain the location of the **workers.properties.minimal** file, for example, **C:\hp\UCMDB\UCMDBServer\tools\iis_integration\ workers.properties.minimal**.

      c The **worker_mount_file** should contain the location of the
  uriworkermap.properties file, for example
  **C:\hp\UCMDB\UCMDBServer\tools\iis_integration\uriworkermap.p
  roperties**.

3 Change the string **worker.localAjp.host=localhost** to the UCMDB server
 hostname (if the HP Universal CMDB server does not reside on the same
 machine as IIS).

4 Open the IIS management console. Run **inetmgr** from the command line.

5 Add a new virtual directory to your IIS Web site for **Windows 2003/IIS6**:

 6 The Virtual Directory Creation Wizard window is displayed. The alias of the virtual directory must be **jakarta**. Its physical path should be **C:\hp\UCMDB\UCMDBServer\tools\iis_integration.** If the UCMDB server and the IIS server are running on separate machines, the path should be the directory on the IIS machine. Allow **Execute** access to the new virtual directory:

 7 Open the **Default Web Site Properties** dialog box and add **isapi_redirect.dll** as an ISAPI filter to your IIS Web site. The name of the filter should reflect its task (for example, **tomcat**) and its executable must be **isapi_redirect.dll.** If the UCMDB server and the IIS server are running on separate machines, the executable must be **isapi_redirect.dll** in the directory where you copied it on the IIS machine.

 8 Open **Web Service Extensions**, select **All Unknown ISAPI Extensions** from the list, and click **Allow.**

 9 Restart IIS (stop and start the IIS service) and make sure that the **tomcat** filter is marked with a green up arrow:

 10 Set the IIS server as the front-end server for UCMDB. This can be done in one of the following ways:

  ➤ In the Infrastructure Settings Manager:

   ➤ Click **General Settings**.

   ➤ Change the value of the **Frontend URL** field to the address of the IIS server (http://<IIS server name>:<port>).

   ➤ Change the value of the **Is Frontend URL from settings enabled?** field to **True**.

  ➤ In the JMX console:

   ➤ Launch the Web browser and enter the following address: **http://<UCMDB server name>:<port>/jmx-console**.

   ➤ Click **UCMDB-UI:name=UI Server frontend settings** to open the JMX MBEAN View page.

➤ Click the **setUseFrontendURLBySettings** method and enter the address of the IIS server as the value (http://<IIS server name>:<port>).

➤ Click **Invoke**.

Set Up IIS to Enable Access to UCMDB – Windows 2008

This section outlines the procedure to integrate HP Universal CMDB and IIS for Windows 2008.

To manually integrate HP Universal CMDB and IIS:

1 If the HP Universal CMDB server does not reside on the same machine as IIS, copy all the files from the **C:\hp\UCMDB\UCMDBServer\tools\iis_integration** directory to the **c:\ucmdb_iis** folder on the IIS machine. On the IIS machine, modify the following files:

a In the **workers.properties.minimal** file, change the string **worker.localAjp.host=localhost** to the UCMDB server hostname.

b In the **isapi_redirect.properties** file:

➤ The **log_file** should point to a folder containing the integration logs, for example, **c:\ucmdb_iis\isapi.log**.

➤ The **worker_file** should contain the location of the **workers.properties.minimal** file, for example, **C:\ucmdb_iis\workers.properties.minimal**.

➤ The **worker_mount_file** should contain the location of the **uriworkermap.properties** file, for example **C:\ucmdb_iis\uriworkermap.properties**.

 2 If the HP Universal CMDB server resides on the same machine as IIS,
   modify the **isapi_redirect.properties** file in the
   C:\hp\UCMDB\UCMDBServer\tools\iis_integration directory as follows:

   a The **log_file** should point to a folder containing the integration logs,
      for example, **C:\hp\UCMDB\UCMDBServer\runtime\log\isapi.log**.

   b The **worker_file** should contain the location of the
      workers.properties.minimal file, for example,
      **C:\hp\UCMDB\UCMDBServer\tools\iis_integration\
      workers.properties.minimal**.

   c The **worker_mount_file** should contain the location of the
      uriworkermap.properties file, for example
      **C:\hp\UCMDB\UCMDBServer\tools\iis_integration\uriworkermap.
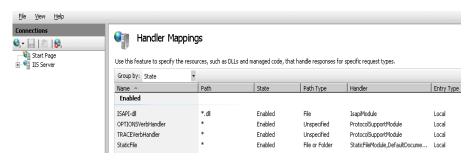   properties**.

 3 Change the string **worker.localAjp.host=localhost** to the UCMDB server
   hostname (if the HP Universal CMDB server does not reside on the same
   machine as IIS).

 4 Open the **IIS management console**. Run **inetmgr** from the command line.

 5 Double-click **ISAPI** Filters.

 6 Right-click the main window in the **IIS Management Console** and select
   Add.

 7 Add **isapi_redirect.dll** as an ISAPI filter to your IIS Web site. The name of
   the filter should reflect its task (for example, **tomcat**) and its executable
   must be **isapi_redirect.dll.** If the UCMDB server and the IIS server are
   running on separate machines, the executable must be **isapi_redirect.dll**
   in the directory where you copied it on the IIS machine.

 8 Add a new virtual directory to your IIS Web site. The alias of the virtual directory must be **jakarta**. The virtual directory must point to **C:\hp\UCMDB\UCMDBServer\tools\iis_integration** (if the folder resides on the same server as UCMDB) or to the directory that **iis_integration** was copied to, if it resides on a different server.

 9 Select the name of the IIS server from the **Connections** pane.

10 Double-click **ISAPI and CGI Restrictions**.

11 Right-click and enter the same information you added in step 7 above.

12 Check the box to allow the **Path** to execute.

13 Open **Handler Mappings**.

14 Select **ISAPI-dll**. Right-click and select **Edit Feature Permissions**. Click **Execute**.

15 Restart IIS.

16 In UCMDB, access Infrastructure Settings (**Administration** > **Infrastructure Settings** > **General Settings**). Change the **Enable AJP connections** option to **True** and restart the UCMDB Server.

17 Set the IIS server as the front-end server for UCMDB. This can be done in one of the following ways:

➤ In the Infrastructure Settings Manager:

➤ Click **General Settings**.

➤ Change the value of the **Frontend URL** field to the address of the IIS server (http://<IIS server name>:<port>).

➤ Change the value of the **Is Frontend URL from settings enabled?** field to **True**.

➤ In the JMX console:

➤ Launch the Web browser and enter the following address: **http://<UCMDB server name>:<port>/jmx-console**.

➤ Click **UCMDB-UI:name=UI Server frontend settings** to open the JMX MBEAN View page.

➤ Click the **setUseFrontendURLBySettings** method and enter the address of the IIS server as the value (http://<IIS server name>:<port>).

➤ Click **Invoke**.

Troubleshooting and Limitations

You cannot open the JMX Console from IIS. That is, basic authentication cannot be passed from Jetty.

🔖 Configure the Data Flow Probe

For Data Flow Probe configuration, change the following strings in the following file: **C:\hp\UCMDB\DataFlowProbe\conf\ DiscoveryProbe.properties**:

➤ serverName = <IIS host name>

➤ serverPort = <IIS HTTP port>, by default 80

The IIS URL (for example, **http://<IIS hostname>/ucmdb**) can now be used to access UCMDB, the JMX console, the UCMDB SDK, and so on.

28

Accessing HP Universal CMDB

This chapter includes:

Concepts

➤ Accessing HP Universal CMDB Overview on page 430

➤ Local Installation Mode on page 431

Tasks

➤ Access HP Universal CMDB and its Components on page 432

➤ Enable Automatic Login on page 434

➤ Change Default Time Limit for User Inactivity Log Out on page 435

➤ Change the Root Context for UCMDB Components on page 436

Concepts

🔧 Accessing HP Universal CMDB Overview

You access HP Universal CMDB using a supported Web browser, from any computer with a network connection (intranet or Internet) to the HP Universal CMDB Server. The level of access granted a user depends on the user's permissions. For details on granting user permissions, see "Set Up Users" in the *HP Universal CMDB Administration Guide*.

For details on Web browser requirements, as well as minimum requirements to successfully view HP Universal CMDB, see "HP Universal CMDB Support Matrix" on page 35.

For details on accessing HP Universal CMDB securely, see Part VI, "Hardening HP Universal CMDB."

For details on login authentication strategies that can be used in HP Universal CMDB, see "Set Up an Authentication Method" on page 390.

For login troubleshooting information, see "Login Troubleshooting" in the *HP Universal CMDB Administration Guide*.

Tip: Click the **Help** button on the login page for complete login help.

Local Installation Mode

Local installation mode is a method of loading UCMDB which reduces the applet loading time significantly. When using local installation mode, the applet files (jars) are loaded to a local directory called **UcmdbAppletJars**, located under the environment's temporary directory. The classes are loaded using a customized class loader which works faster, but does not verify the signature of the signed jars. Local installation mode is thus considered an unsecured mode.

To select local installation mode, select the **Enable local installation mode** check box on the login screen. This check box is only visible if you have set the **Local installation mode permission** setting to **True** in the Infrastructure Settings Manager. You can set the default status of the check box using the **Local installation mode initial status** setting. When the setting is set to **True**, the check box is selected by default. When it is set to **False**, the check box is cleared by default.

Note: If you select the **Remember me on this machine** check box at login, the status of the **Enable local installation mode** check box remains the same for the next login, regardless of the infrastructure setting.

For HP Software-as-a-Service customers, the installation settings are on a per customer basis.

Tasks

🔧 Access HP Universal CMDB and its Components

This section explains how to access the HP Universal CMDB components.

1 In the Web browser, enter the URL of the HP Universal CMDB Server, for example, **http://<server name or IP address>.<domain name>:8080** where **<server name or IP address>.<domain name>** represents the fully qualified domain name (FQDN) of the HP Universal CMDB server.

If HP Universal CMDB is set up to work through a reverse proxy, enter **https://<proxy_server_name>:443** where **proxy_server_name** is the name or IP address of the proxy server.

If the correct Java version is not installed on your machine, you can choose to download the version from sun.com or from the UCMDB server. (If you log in without installing Java, you will not be able to view pages that need a Java applet to display correctly.) For details, see "Troubleshooting and Limitations" on page 42.

2 Click a link to work with HP Universal CMDB:

a **UCMDB Application**. Opens the login page. For details, see "Log In to HP Universal CMDB" on page 433.

Note: You can also access the login page by entering **http://<server name or IP address>.<domain name>:8080/ucmdb**.

---

b **Server Status**. Opens the Server Status page. For details, see "HP Universal CMDB Services" on page 123.

c **JMX Console**. Enables you to perform operations on the CMDB through the JMX console interface.

d **API Connection Test**. Displays information about the HP Universal CMDB Server for you to use when running an API to the CMDB.

    e **API Client Download**. Downloads the UCMDB API jar file.

    f **API Reference**. Opens the HP UCMDB API Reference documentation.

Log In to HP Universal CMDB

1 Enter the default superuser login parameters:

> ➤ **User Login**=admin, **User Password**=admin.

> ➤ If HP Universal CMDB is installed in a multiple customer or multiple state environment (for example, HP Software-as-a-Service or HP Universal CMDB Configuration Manager), a Customer field is displayed. Choose the Customer name from the list.

Note for HP Universal CMDB Configuration Manager users: The Data Flow Management modules are available only when you are logged in to UCMDB in Actual state.

> ➤ Select **Open in new window** to open the application in another browser window.

> ➤ **Remember me on this machine**: Select for automatic login. That is, the next time you log in to UCMDB, you do not need to enter your user name and password.

> ➤ **Enable local installation mode**: Select to load UCMDB in local installation mode. For details, see "Local Installation Mode" on page 431.

2 Click **Login**. After logging in, the user name appears at the top right of the screen.

3 (Recommended) Change the superuser password immediately to prevent unauthorized entry. For details on changing the password, see "Reset Password Dialog Box" in the *HP Universal CMDB Administration Guide*.

4 (Recommended) Create additional administrative users to enable HP Universal CMDB administrators to access the system. For details on creating users in the HP Universal CMDB system, see "Add New User Wizard" in the *HP Universal CMDB Administration Guide*.

Log Out

When you have completed your session, it is recommended that you log out of the Web site to prevent unauthorized entry.

To log out:

Click **Logout** at the top of the page.

🦖 Enable Automatic Login

Advanced login options enables you to automate login, limit login access, and provide direct login capabilities to specific pages in HP Universal CMDB.

When automatic login is enabled from the login page, the next time the user enters the URL to access HP Universal CMDB, the login page does not open, the login name and password do not have to be entered, and the default page that is set to open for the user opens automatically.

To enable automatic login:

1 In the HP Universal CMDB login page, select the option **Remember me on this machine**.

2 When completing your session, do not click **Logout** at the top of the page, but close the browser window.

Logging out disables the automatic login option, in which case you must enter the login name and password the next time you access HP Universal CMDB.

Guidelines for Using Automatic Login

Keep the following in mind when using this option:

➤ Using the **Logout** option at the top of the HP Universal CMDB page cancels the option. If a user has logged out, the next time the user logs in, the Login page opens and the user must enter a login name and password. This can be useful if another user must log in on the same machine using a different user name and password.

➤ This option could be considered a security risk and should be used with caution.

Change Default Time Limit for User Inactivity Log Out

HP Universal CMDB includes an automatic logout feature which logs out when the system is inactive for a set time period. The default period is 1440 minutes (24 hours). After that time, a message appears with a 30-second countdown until logout.

This task describes how to adjust the time limit UCMDB stays open without any user input before automatically logging out.

To change the default logout time:

1 Select **Administration** > **Infrastructure Settings** > **General Settings** category > **Inactive allowed time** setting.

2 From the **Value** column enter a value.

3 Enter a new time interval in minutes. All values for inactive allowed time are located in the Properties window. Right-click **Inactive Allowed Time** Properties or double-click the **Inactive Allowed Time** setting.

🔧 Change the Root Context for UCMDB Components

The default root context for all HP Universal CMDB components is /. This root context can be configured in the Infrastructure Settings Manager.

To change the root context:

1 Go to **Administration** > **Infrastructure Settings Manager** and select the **Root context** setting under **General Settings**.

2 Edit the setting and save your changes.

3 Restart HP Universal CMDB.

One application of this feature is the ability to access multiple UCMDB servers using one reverse proxy server. Each UCMDB server can be configured with its own root context.

Caution: After changing the root context from its default value, all UCMDB components are only available using the new root context. For example, if the new root context is /ucmdb1, the user interface will be accessible from the following url: **http://<server name or IP address>.<domain name>:8080/ucmdb1/ucmdb-ui.**

29

Navigating HP Universal CMDB

This chapter includes:

Concepts

➤ Navigating the HP Universal CMDB User Interface on page 438

➤ Working with the HP Universal CMDB Documentation on page 440

Reference
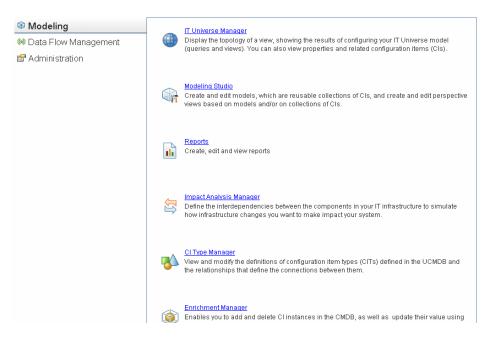
➤ Menus and Options on page 443

Concepts

🍀 Navigating the HP Universal CMDB User Interface

HP Universal CMDB runs in a Web browser. You move around HP Universal CMDB using the following navigation functions:

➤ **Navigation Bar.** Enable quick navigation between modules. Click the category in the lower part of the bar and select the module from the icons in the upper part of the bar.

➤ **Orientation Map.** For each category, you can display a map with brief descriptions of each of the modules included by selecting **Managers > Orientation Map**.

➤ **Status Bar.** Provides information on the CMDB application and enables you to configure certain aspects of your interface.

➤ **Collapse/Expand Arrows.** Enable collapsing and expanding of panes with a single click.

Note: The Web browser **Back** function is not supported in HP Universal CMDB. Using the **Back** function does not always revert the current context to the previous context. To navigate to a previous context, use the breadcrumb function.

Suggested Values in Dialog Boxes

In some dialog box text fields in HP Universal CMDB, such as the New CI dialog box and the Query Node Properties dialog box, suggested attribute values for entered data are automatically provided when you begin to enter an attribute value. The suggested values match the text entered up to this point and are taken from existing values for the same attribute for the selected CIT or any of its children. The values are sorted alphabetically and a number appears next to each suggested value indicating the number of occurrences of that value. If the number of suggested values exceeds a set maximum limit, no suggestions are displayed. You can set the maximum by changing the **Maximum CI Count for Attribute Value Suggestions** setting in the Infrastructure Settings Manager.

When working in a multi-tenancy environment, the suggested values are only taken from CIs that the user has permission to view (at least one tenant associated with the View CIs permission assignment for the user is included among the CI's owner tenant or consumer tenants).

Note: This feature is only relevant for the following attribute types: string, integer, long, double, and float.

Working with the HP Universal CMDB Documentation

The following sections describe how to navigate and use the HP Universal CMDB documentation.

Navigating the UCMDB Help

UCMDB Help is an integrated help system that can be navigated in the following ways:

➤ **From the home page.** To access the home page, select **UCMDB Help** in the Help menu.

The home page includes links to the various guides, either contained in the UCMDB Help or in PDF format.

➤ **From the navigation pane.** To access the navigation pane if it is not being displayed, click the **Search and Navigate** button.

The navigation pane is divided into the following tabs:

➤ **Contents tab.** The Contents tab organizes the various guides in a hierarchical tree, enabling direct navigation to a specific guide or topic.

➤ **Index tab.** The Index tab enables you to select a specific topic to display. Double-click the index entry to display the corresponding page. If your selection occurs in multiple documents, a dialog box is displayed enabling you to select a context.

➤ **Search tab.** The Search tab enables you to search for specific topics or keywords. Results are returned in ranked order.

➤ **Favorites tab.** The Favorites tab enables bookmarking specific pages for quick reference. Note that the Favorites tab is only available when using the Java implementation of UCMDB Help. If your browser does not support Java, the JavaScript implementation is automatically used and the Favorites tab is not displayed.

Documentation Library Functionality

The following functionality is available from the top frame in the Documentation Library main pane.

➤ **Search and Navigate button.** Click to display the navigation pane, which includes the Contents, Index, Search, and Favorites tabs. For details on the Navigation pane, see "Working with the HP Universal CMDB Documentation" on page 440. Note that this button is only displayed when the navigation pane is closed.

➤ **Show in Contents button.** Click to highlight, in the Contents tab, the entry corresponding to the currently displayed page. Note that this button is only displayed when the navigation pane is open.

➤ **Previous and Next buttons.** Click to move forward or backward in the guide currently displayed.

➤ **Send Documentation Feedback to HP button.** Click to open your email client and send feedback to HP. An email message opens with the **To** and **Subject** fields already completed and a link to the current page in the message body. Make sure to complete the email by entering your feedback. Note that you must have an email client configured on the machine for this function to operate correctly.

➤ **Print button.** Click to print the currently displayed page.

Organization of Information into Topics

The material in most of the Documentation Library guides is organized by topic types. Three main topic types are in use: Concepts, Tasks, and Reference. The topic types are differentiated visually using icons. Below is an explanation of each topic type along with its corresponding icon:

➤ **Concepts.** Concept topics provide background, descriptive, or conceptual information. Read concept topics to get general information about what a feature does and how it works.

➤ **Tasks**. Task topics provide step-by-step guidance on how to complete specific tasks that are typically required to administer or use the software. Task topics also include scenarios for certain tasks. Read task topics and follow the steps listed to get a task done.

➤ **Reference**. Reference topics provide detailed lists and explanations of parameters, common user interface elements, and other reference-oriented material. Read reference topics when you need to look up some specific piece of reference information relevant to a particular context.

➤ **User Interface**. User Interface topics are a specialized form of reference topics that are used mainly for context-sensitive help. Help links from the software generally open the user interface topics.

➤ **Troubleshooting and Limitations**. Troubleshooting and limitations topics are a specialized form of reference topics that provide troubleshooting and list limitations of the feature. Read troubleshooting and limitations topics if you encounter unexpected behavior of the software. It is recommended that you review a feature's limitations before using it.

Reference

⚓ Menus and Options

The following categories are available in the lower part of the Navigation Bar:

Category	Description
Modeling	Click to open the Modeling menu, where you build and manage a model of your IT universe in the CMDB. For details, see "Modeling" in the *HP Universal CMDB Modeling Guide*.
Data Flow Management	Click to open the Data Flow Management (DFM) menu, where you set up and run the DFM process to populate the IT Universe model with configuration items (CIs), and where you work with Integration Studio. For details, see the *HP Universal CMDB Data Flow Management Guide*. For details on DFM content, see the *HP Universal CMDB Discovery and Integration Content Guide* PDF.
Administration	Click to open the Administration menu, where you configure infrastructure settings, users, roles, permissions, and schedules and work with the Package Manager. For details see the *HP Universal CMDB Administration Guide*.

Help Menu

You access the following online resources from the HP Universal CMDB Help menu:

➤ **Help on this page.** Opens the UCMDB Help to the topic that describes the current page or context.

➤ **UCMDB Help.** Opens the home page. The home page provides quick links to the main help topics.

➤ **Troubleshooting & Knowledge Base.** Opens the HP Software Support Web Site directly to the HP Software Self-solve knowledge base landing page. The URL for this Web site is http://support.openview.hp.com.

➤ **HP Software Support.** Opens the HP Software Support Web Site. This site enables you to browse the knowledge base and add your own articles, post to and search user discussion forums, submit support requests, download patches and updated documentation, and more. The URL for this Web site is http://support.openview.hp.com.

➤ **HP Software Web Site.** Opens the HP Software Web site, which contains information and resources about HP Software products and services. The URL for this Web site is http://www.hp.com/managementsoftware.

➤ **What's New?** Opens the What's New document, which describes the new features and enhancements of the version.

➤ **Discovery and Integrations Content Help.** Describes the default, out-of-the-box content: what is being discovered, the credentials required in discovery, how to troubleshoot the discovery results, and how to work with integration adapters.

➤ **UCMDB Best Practices.** Opens an HTML page with direct links and information about the following:

> ➤ HP Live Network where the Best Practice documentation is accessed.

> ➤ Support site where all documentation and knowledge base articles can be accessed.

> ➤ Guidance videos and feature movies.

> ➤ HP UCMDB online documentation.

➤ **About HP Universal CMDB.** Opens the HP Universal CMDB dialog box, which provides version, license, patch, and third-party notice information.

Note: For information on high availability, see "High Availability Mode Installation" on page 275.

30

Available Troubleshooting Resources

This chapter includes:

Troubleshooting Resources on page 445

🔍 Troubleshooting Resources

➤ **Installation troubleshooting.** Use to troubleshoot common problems that you may encounter when installing HP Universal CMDB, and the solutions to those problems. For details, see "Troubleshooting and Limitations" on page 42.

➤ **Login troubleshooting.** Use to troubleshoot possible causes of failure to log in to HP Universal CMDB. For details, see "Troubleshooting and Limitations" on page 42.

➤ **HP Software Self-solve knowledge base.** Use to search for specific troubleshooting information on a wide variety of topics. Located on the HP Software Support Web site, the HP Software Self-solve knowledge base can be accessed by selecting **Troubleshooting & Knowledge Base** from the HP Universal CMDB Help menu.

Note that only registered customers can access the resources on the HP Software Support Web site. Customers who have not yet registered can do so from this site.

➤ **HP Universal CMDB Log files.** Use to troubleshoot CMDB runtime problems. For details, see "CMDB Log Files" in the *HP Universal CMDB Administration Guide*.

➤ **Data Flow Management log files.** Use to troubleshoot DFM problems. For details, see "Data Flow Management Log Files" in the *HP Universal CMDB Administration Guide*.

➤ **Query log files.** Use to view definitions for query parameter log files. For details, see "CMDB Log Files" in the *HP Universal CMDB Administration Guide*.

31

Working in Non-English Locales

This chapter includes:

Reference

➤ Installation and Deployment Issues on page 448

➤ Database Environment Issues on page 449

➤ Administration Issues on page 449

➤ Report Issues on page 449

➤ Multi-Lingual User (MLU) Interface Support on page 450

Reference

🔍 Installation and Deployment Issues

➤ If you use the Japanese, Chinese, or Korean language in your browser, you must ensure that the HP Universal CMDB server has East Asian languages installed. On the machine on which the HP Universal CMDB server is installed, you must select **Control Panel** > **Regional and Language Options** > **Languages** > **Install files for East Asian languages**.

➤ Installing HP Universal CMDB in an I18N environment is supported for HP Universal CMDB installed on a Windows or Linux platform. For details on installing HP Universal CMDB on a Windows platform, see "HP Universal CMDB Installation on a Windows Platform" on page 71.

➤ When logging on to HP Universal CMDB, the user password cannot include Japanese or Chinese characters, when the UCMDB server is installed on a Windows 2003 machine with a Japanese or Chinese operating system.

➤ The installation path for all HP Universal CMDB components must not contain non-English language characters.

➤ The Upgrade Wizard for versions 9.00 and 9.01 does not support the non-English user interface. (The upgrade itself works properly.)

Database Environment Issues

➤ To work in a non-English language HP Universal CMDB environment, you can use either an Oracle Server database or a Microsoft SQL Server database. The OS Windows regional settings language of the database should be the same as that of the UCMDB Server. When using an Oracle Server database, the encoding of the database can also be UTF-8 or AL32UTF-8, which supports both non-English languages as well as multiple languages.

➤ When you create a new Oracle instance in an Oracle database, you must specify the character set for the instance. All character data, including data in the data dictionary, is stored in the instance's character set. For details, see "Oracle Summary Checklist" in the *HP Universal CMDB Database Guide* PDF.

➤ The Database Query Monitor can connect to an Oracle database, but the Oracle user names and passwords must contain only English characters.

Administration Issues

➤ To support non-English characters, the encoding for HP Universal CMDB databases must be defined as UTF-8 or AL32UTF-8, or set to the specific language. For further details, see "Database Environment Issues" on page 449.

Report Issues

➤ HP Universal CMDB does not support Custom Report names that contain more than 50 multi-byte characters.

➤ Reports downloaded from HP Universal CMDB to Excel cannot be displayed properly on an operating system whose language differs from the data language.

When using Microsoft Office version 2007 or later, with the latest updates installed, this issue is not relevant because the data is saved in Unicode format.

➤ If a report is created in one language locale and sent by email from another language locale, the report contains system information in the languages of the server and the original locale.

➤ If a report file name contains multi-byte characters (for example, in Japanese, Chinese, or Korean) and the report is sent as an email attachment, the name becomes unreadable.

➤ When exporting a CI instance to a PDF file, multi-byte characters (such as Japanese, Chinese, Korean, and so on) may not be displayed properly in the PDF file.

Multi-Lingual User (MLU) Interface Support

Note: The following support matrix is relevant for version 9.00 (but not for version 9.01 or any other minor patches).

The HP Universal CMDB user interface can be viewed in the following languages in your Web browser:

Language	Localized UI	Localized Materials	Availability
English	Yes	Yes	Part of initial product release
French	Yes		Part of initial product release
Japanese	Yes	Yes	Media pack B
Korean	Yes		Part of initial product release
Simplified Chinese	Yes		Part of initial product release
Dutch	Yes		Media pack A

Language	Localized UI	Localized Materials	Availability
German	Yes		Part of initial product release
Portuguese	Yes		Media pack A
Russian	Yes		Media pack A
Spanish	Yes		Part of initial product release
Italian	Yes		Media pack A

Note: Complementary media packs are released within 90 days of the product release.

Use the language preference option in your browser to select how to view HP Universal CMDB. The language preference chosen affects only your local machine (the client machine) and not the HP Universal CMDB Server machine or any other user accessing the same HP Universal CMDB machine.

To set up and view HP Universal CMDB in a specific language:

1 Install the appropriate language's fonts on your local machine if they are not yet installed. If you choose a language in your Web browser whose fonts have not been installed, HP Universal CMDB displays the characters as squares.

2 If you are logged in to HP Universal CMDB, you must log out. Click **LOGOUT** at the top of the HP Universal CMDB window.

Close every open browser window or, alternatively, clear the cache.

3 If HP Universal CMDB is running on Internet Explorer, configure the Web browser on your local machine to select the language in which you want to view HP Universal CMDB (**Tools** > **Internet Options**).

   a Click the **Languages** button and in the Language Preference dialog box, highlight the language in which you want to view HP Universal CMDB.

   b If the language you want is not listed in the dialog box, click **Add** to display the list of languages. Select the language you want to add and click **OK**.

   c Click **Move Up** to move the selected language to the first row.

   d Click **OK** to save the settings.

   e Display the HP Universal CMDB login window.

   f From the Internet Explorer menu, select **View** > **Refresh**. HP Universal CMDB immediately refreshes and the user interface is displayed in the selected language.

Note: For details on viewing Web pages in Internet Explorer that are written in a different language, see http://support.microsoft.com/kb/306872/en-us.

Notes and Limitations

➤ There is no language pack installation. All translated languages included with the initial release are integrated into the HP Universal CMDB Multi-lingual User Interface (MLU).

➤ Data remains in the language it is entered in, even if the language of the Web browser changes. Changing the language of the Web browser on your local machine does not change the language of the data input definitions and configurations.

➤ You cannot deploy a package if the server locale is different than the client locale and the package name contains non-English characters. For details, see "Package Manager" in the *HP Universal CMDB Administration Guide*.

➤ You cannot create a package that contains resources (for example, views and queries) having non-English characters in their names, if the server locale is different from the client locale. For details, see "Package Manager" in the *HP Universal CMDB Administration Guide*.

➤ You cannot create a new user in Users and Roles if the name of the new user contains more than 20 East Asian characters. For details, see "Users and Roles" in the *HP Universal CMDB Administration Guide*.

➤ In Modeling Studio, you cannot create a new view if the view's name contains more than 18 Japanese characters. For details, see "Modeling Studio" in the *HP Universal CMDB Modeling Guide*.

➤ The following pages appear only in English. They are not translated into any other language. For details, see "Working in Non-English Locales" on page 447:

➤ HP Universal CMDB server status HTML page

➤ HP Universal CMDB Login page

➤ JMX Console page

➤ API Connect Test page

➤ If you select languages on the client machine that are not supported by UCMDB MLU, HP Universal CMDB is displayed with the same system locale language as that running on the UCDMB Server machine.

➤ When using multi-byte characters in fields such as **Name**, **Display Name** and **Description**, make sure that the number of characters conforms to the byte limit of the field. For example, if a field has a limit of 100 single-byte characters, up to 33 multi-byte characters of 3 bytes each can be used.