HP Universal CMDB

for the Windows and Linux operating systems

Software Version: 9.00

Deployment

Document Release Date: June 2010

Software Release Date: June 2010

Legal Notices

Warranty

The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

The information contained herein is subject to change without notice.

Restricted Rights Legend

Confidential computer software. Valid license from HP required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Copyright Notices

Trademark Notices

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

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

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

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

Java™ is a US trademark of Sun Microsystems, Inc.

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

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

UNIX® is a registered trademark of The Open Group.

Acknowledgements

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

- 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

Welcome to This Guide....13
How This Guide Is Organized....13
Who Should Read This Guide....14
HP Universal CMDB Online Documentation....15
Additional Online Resources....16
Documentation Updates....17

PART I: INTRODUCTION

Chapter 1: Introduction to HP Universal CMDB....21
HP Universal CMDB Overview....21
Installation Procedure Overview....26
HP Universal CMDB on VMware....28
Change Memory Allocation for Applets....29

Chapter 2: HP Universal CMDB Support Matrix....31
Server Hardware Requirements....32
Server Software Requirements....33
Server Database Requirements....36
Client Software Requirements....37
Capacity Planning Requirements....38

Chapter 3: Licensing Models for HP Universal CMDB....39
Licensing Models – Overview....39
Upgrade to the Integrations or DDM Advanced Licenses....42
Troubleshooting and Limitations....43

Chapter 4: Getting Started with HP Universal CMDB....45
Predeployment Planning....45
Get Started....48
Basic Administration Tasks....49

Chapter 5: HP Universal CMDB Services..51
View the Status of HP Universal CMDB Services 51
HP Universal CMDB Services 53
Troubleshooting and Limitations 54

PART II: INSTALLATION

Chapter 6: HP Universal CMDB Installation on a Windows Platform 59
Concepts..59
Installation Prerequisites 59
Install UCMDB 61
Configure the UCMDB Mail Server..70
Uninstall UCMDB 71

Chapter 7: HP Universal CMDB Installation on a Linux Platform 73
Installation Prerequisites 73
Install HP Universal CMDB...74
Configure the UCMDB Mail Server..82
Uninstall UCMDB 83

Chapter 8: UCMDB Server Configuration 85
Choosing the Database or Schema..85
Required Information for Setting Database Parameters......................87
Allocating Memory to Processes 89
Access the UCMDB Server Configuration Wizard 89
Create a Microsoft SQL Server Database 90
Create an Oracle Schema..94
Connect to an Existing Microsoft SQL Server Database 96
Connect to an Existing Oracle Schema..96
Restart the Server..96

Chapter 9: HP Universal CMDB Server Service..................................97
Change the HP Universal CMDB Server Service User.........................97
Start and Stop the HP Universal CMDB Server Service.......................99

PART III: DATA FLOW PROBE INSTALLATION

Chapter 10: UCMDB Data Flow Probe Installation 103
Install the UCMDB Data Flow Probe 103
Upgrade the Probe...113
Run Probe Manager and Probe Gateway on Separate Machines 113
Configure the Probe Manager and Probe Gateway Components.....114

PART IV: UPGRADING HP UNIVERSAL CMDB FROM VERSION 8.0X TO 9.0X

Chapter 11: Upgrading HP Universal CMDB to Version 9.00 121
Upgrade Prerequisites 121
Upgrade Summary 123
Input Parameters, Class Model, and Log Files 123
Uninstall UCMDB 8.0x 125
Upgrade to UCMDB 9.00 125
Post Upgrade Procedures 134
Ordered Summary of Upgrade Steps 134
Troubleshooting and Limitations 205

Chapter 12: Upgrading Packages from Version 8.04 to 9.00..........207
Package Migration Utility – Overview..........208
Migrate a Custom Package 209
Troubleshooting and Limitations 211

PART V: HIGH AVAILABILITY AND CAPACITY PLANNING

Chapter 13: HP Universal CMDB High Availability..........215
Best Practices for the HP Universal CMDB High Availability Solution215
Install HP Universal CMDB in High Availability Mode..........217
Configure Network High Availability 220
Configure Full Site..........221

Chapter 14: HP Universal CMDB Large Capacity Planning..........223
Large Capacity Planning Overview..........224
Managed Hosts and Host-Related CIs 225
UCMDB Server Configuration..........226
Oracle Database Configuration..........226
System Test Setup..........227
System Test Results..........228

PART VI: HARDENING HP UNIVERSAL CMDB

Chapter 15: Introduction to Hardening 231
Hardening Overview 231
Hardening Preparations..........233
Deploy HP Universal CMDB in a Secure Architecture..........234
Change User Name or Password for the JMX Console..........235

Chapter 16: Enabling Secure Sockets Layer (SSL) Communication .237
Enable SSL on the Server Machine With a Self-Signed Certificate ...237
Enable SSL on the Server Machine With a Certificate from a Certification Authority ...239
Enable SSL on the Client Machines ...241
Enable SSL on the Client SDK ...242
Change the Server Keystore Passwords ...242
Enable or Disable HTTP/HTTPS Ports ...244

Chapter 17: Using a Reverse Proxy ...245
Reverse Proxy Overview ...246
Security Aspects of Using a Reverse Proxy Server ...247
Configure a Reverse Proxy Using Infrastructure Settings ...248
Configure a Reverse Proxy Using the JMX Console ...249
Apache 2.0.x – Example Configuration ...250

Chapter 18: Hardening Data Flow Management ...253
Hardening Data Flow Management Overview ...254
Credentials Encryption With Confidential Manager ...256
Manage the Storage of Credentials ...257
Generate or Update the Encryption Key ...259
Export and Import the domainScopeDocument (DSD) File in Encrypted Format ...265

Chapter 19: Hardening the Data Flow Probe ...267
Set the MySQL Database Encrypted Password ...268
Set the JMX Console Encrypted Password ...270
Enable SSL Between UCMDB Server and UCMDB Data Flow Probe with Mutual Authentication ...272
Enable SSL on the Data Flow Probe with Basic Authentication ...278
Connect the Data Flow Probe by Reverse Proxy ...278
Control the Location of the domainScopeDocument File ...280

Chapter 20: Lightweight Single Sign-On Authentication – General Reference 281
LWSSO Authentication Overview ...282
Retrieve Current LW-SSO Configuration In Distributed Environment283
Enable Login to HP Universal CMDB with Lightweight Single Sign-On (LW-SSO) ...284
LW-SSO System Requirements ...285
LW-SSO Security Warnings ...286
Troubleshooting and Limitations ...288

Chapter 21: Confidential Manager 295
Confidential Manager Overview 296
Security Considerations...296
Configure the HP Universal CMDB Server...297
Definitions 299
Encryption Properties 300

PART VII: DISASTER RECOVERY

Chapter 22: Disaster Recovery Setup..305
Disaster Recovery Overview 306
Prepare the Disaster Recovery Environment....................................307
Prepare the HP Universal CMDB Failover Instance for Activation...310
Perform Startup Cleanup Procedure...311

PART VIII: GETTING STARTED WITH HP UNIVERSAL CMDB

Chapter 23: Starting and Stopping the Server.................................315
Start and Stop the Server on the Windows Platform........................315

Chapter 24: Accessing HP Universal CMDB Through the IIS Web Server317
Accessing HP Universal CMDB Through IIS Overview.....................317
Set Up IIS to Enable Access to UCMDB – Windows 2003.................318
Set Up IIS to Enable Access to UCMDB – Windows 2008.................322
Configure the Data Flow Probe 325

Chapter 25: HP Universal CMDB Login Authentication 327
Authentication for HP Universal CMDB Login 327
Set Up an Authentication Method...328
Enable and Define the LDAP Authentication Method 328
Set a Secure Connection with the SSL (Secure Sockets Layer) Protocol329
Using the JMX Console to Test LDAP Connections.........................331

Chapter 26: Logging In to HP Universal CMDB 333
Accessing HP Universal CMDB 333
Log In and Log Out 334
Automatic Login...336
Change Default Time Limit for User Inactivity Log Out..................337
Troubleshooting and Limitations 338

Chapter 27: Navigating HP Universal CMDB...................................341
Navigating the HP Universal CMDB User Interface..........................341
Working with the HP Universal CMDB Documentation 344
Menus and Options...346

Chapter 28: Available Troubleshooting Resources...........................349
Troubleshooting Resources 349

Chapter 29: Working in Non-English Locales 351
Installation and Deployment Issues..352
Database Environment Issues 353
Administration Issues...353
Report Issues...353
Multi-Lingual User (MLU) Interface Support....................................354

Index..359

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 13
- Who Should Read This Guide on page 14
- HP Universal CMDB Online Documentation on page 15
- Additional Online Resources on page 16
- Documentation Updates on page 17

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 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 9.00, and for migrating packages from version 8.04 to 9.00.

Part V High Availability and Capacity Planning

Describes the installation, startup, and configuration procedures so that HP Universal CMDB version 9.00 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:

- **Deployment**. 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.
- **Databases**. Explains how to set up the database (MS SQL Server or Oracle) needed by HP Universal CMDB.
- **Discovery and Integration Content**. Explains how to run discovery to discover applications, operating systems, and network components running on your system. Also explains how to discover data in other data repositories through integration.

HP Universal CMDB Online Help includes:

- **Modeling**. Enables you to manage the content of your IT Universe model.
- **Data Flow Management**. Explains how to integrate HP Universal CMDB with other data repositories and how to set up HP Universal CMDB to discover network components.
- **Administration**. Explains how to work with HP Universal CMDB.

- **Developer Reference**. 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).

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 21
- Installation Procedure Overview on page 26
- HP Universal CMDB on VMware on page 28

Tasks

- Change Memory Allocation for Applets on page 29

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" on page 22
- "HP Universal CMDB System Architecture" on page 23
- "HP Universal CMDB Deployment" on page 24
- "The Configuration Management Database (CMDB)" on page 24
- "Data Flow Management Mapping" on page 25

- "Topology Query Language (TQL)" on page 25
- "Document Conventions" on page 26

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.

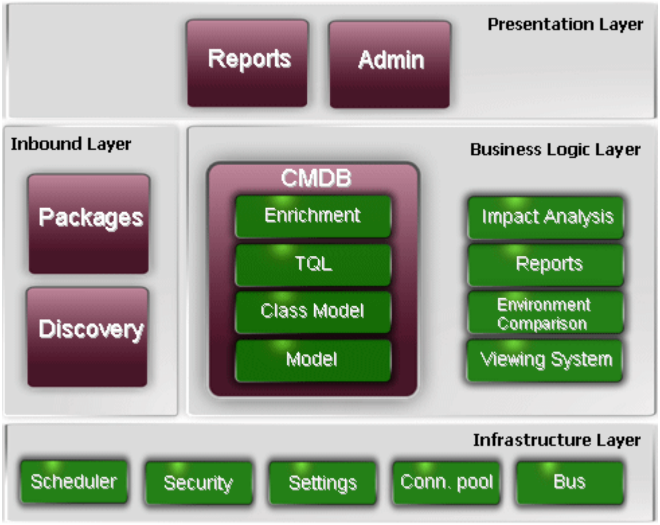
HP Universal CMDB addresses the following operational and functional needs:

- **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

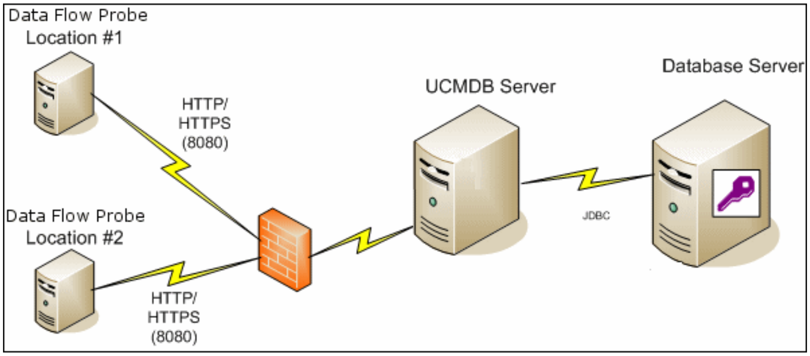
The following diagram provides a graphical overview of the HP Universal CMDB system architecture:



To set up an LDAP authentication method for logging in, see “HP Universal CMDB Login Authentication” on page 327.

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 configuration management database (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 configuration items (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**.

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 Models for HP Universal CMDB” on page 39)

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.

This section includes the following topics:

- "Installation Stages" on page 27
- "Launching HP Universal CMDB" on page 28

Installation Stages

The installation workflow contains the following main stages:

1. Set up the CMDB and History databases on Microsoft SQL Server or schemas on an 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. You must obtain the appropriate HP Universal CMDB license and place it on a machine that is accessible from the machine on which you are installing HP Universal CMDB. For details, see "Licensing Models for HP Universal CMDB" on page 39.

3. Install the HP Universal CMDB server. For details, see Chapter 6, "HP Universal CMDB Installation on a Windows Platform" or Chapter 7, "HP Universal CMDB Installation on a Linux Platform."

   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 Chapter 8, "UCMDB Server Configuration."

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

---

4 Install the collectors (Data Flow Probes). For details, see “UCMDB Data Flow Probe Installation” on page 103.

5 Set the UCMDB Server Service authentication permissions.

Launching HP Universal CMDB

For details, see “Logging In to HP Universal CMDB” on page 333.

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 can be expected to be slower than with a regular installation. A VMware platform is therefore not recommended for an enterprise deployment of HP Universal CMDB and is supported only for standard deployments. For deployment requirements, see “Server Hardware Requirements” on page 32.
- 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
- HP Data Flow Management

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%\\AppData\\LocalLow\\Sun\\Java\\Deployment\\deployment.properties**.
2. Change the line with the latest Java version by adding to the end of it the text **-XmxYYYm**, 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 340.

2

HP Universal CMDB Support Matrix

This chapter includes:

Reference

- Server Hardware Requirements on page 32
- Server Software Requirements on page 33
- Server Database Requirements on page 36
- Client Software Requirements on page 37
- Capacity Planning Requirements on page 38

Reference

Server Hardware Requirements

Computer/processor	**Windows:** 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:** 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 **Note:** ➤ The virtual memory for Windows should be at least 1.5 times 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

Platform	OS version and edition	Supported	Recommended
x64	Windows 2003 Enterprise SP2 and R2 SP2	Yes	
x64	Windows 2008 Enterprise SP2 and R2	Yes	Yes
x64	Red Hat Linux 5 Enterprise/Advanced	Yes	
x64	SUSE Linux 11 Enterprise	No	
32-bit x86	Windows 2000, 2003/2008	No	64-bit required
Sun SPARC	Solaris 8,9 or 10	No	
Any	SUSE Linux 9, 10 Enterprise	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**.
- Regardless of the operating system version, the entire Distribution (with OEM support) and the latest recommended Patch Cluster are required.

This section includes the following topics:

- "Supported Browsers" on page 34
- "Virtual Environments" on page 35

Supported Browsers

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

Virtual Environments

Virtual Environment	OS version and edition	Supported	Recommended
VMware ESX 4.0	Windows 2003 Standard/Enterprise SP2 and R2 SP2 Windows 2008 Standard/Enterprise SP2 and R2 Red Hat Linux 5 Enterprise/Advanced	Yes	Yes
VMware ESX versions 3.5 to 4.0	Windows 2003 Standard/Enterprise SP2 and R2 SP2 Windows 2008 Standard/Enterprise SP2 and R2 Red Hat Linux 5 Enterprise/Advanced	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

BIT Set	OS Version and Edition	Database	Supported	Recommended
64-bit	Any	Oracle 10g, 11g Enterprise versions: Oracle: 10.2, 11.1.0.7 and 11.2	Yes	Yes
64-bit	Any	Oracle 10g, 11g Enterprise RAC versions: Oracle 10.2 and 11.2	Yes	Yes
Any	Windows 2003/2008 Enterprise	MS SQL Server 2005 Enterprise SP3	Yes	
Any	Windows 2003/2008 Enterprise	MS SQL Server 2008 Enterprise SP1	Yes	Yes
32-bit	Any	All	No	64-bit is required for Oracle
Any	Any	Oracle 9i	No	
Any	Any	DB2	No	

Oracle System Requirements

Refer to the Oracle installation guide for the specific Oracle platform. Additional information is available in the Oracle software distribution media as well as in the online Oracle documentation (http://otn.oracle.com/documentation/index.html). Windows database servers.

For details on the certified and supported database types, see "Software Requirements" in the *HP Universal CMDB Database Guide* PDF.

Microsoft SQL Server System Requirements

For Windows platform only.

For details on the certified and supported database types, see "Software Requirements" in the *HP Universal CMDB Database Guide* PDF.

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 6u20 and the required version is 6u4 or later. 6u19 is not recommended because on every applet load a pop-up will open saying the applet contains a mix of signed and unsigned code. ➤ 1.5 family: supported. **Note:** The recommended JRE version is 6u20, 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: <**HP Universal CMDB root folder**>**\AppServer\webapps\site.war\static\JRE** 2 In the configuration file: <**HP Universal CMDB root folder**>**\AppServer\webapps\site.war\conf\CMSConfig**, change the key **jre.for.deployment.path** to match the new JRE deployment executable name. 3 Restart the server. For details on working with applets, see “Change Memory Allocation for Applets” on page 29. 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 **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 and 2007
Adobe PDF (to view exported data)	Versions 7.0, 8.1, and 9.1

Capacity Planning Requirements

For details, seeChapter 14, “HP Universal CMDB Large Capacity Planning.”

3

Licensing Models for HP Universal CMDB

This chapter includes:

Concepts

- Licensing Models – Overview on page 39

Tasks

- Upgrade to the Integrations or DDM Advanced Licenses on page 42

Troubleshooting and Limitations on page 43

Concepts

Licensing Models – Overview

This section includes the following topics:

- “Licensing Levels” on page 40
- “Defined Terms and Definitions” on page 40
- “License for HP Software-as-a-Service” on page 40
- “License for HP ServiceCenter/Service Manager and Other Integrations” on page 41
- “Data Flow Probe Licensing” on page 41

Licensing Levels

- **UCMDB Foundation License**. The Foundation license includes UCMDB as the backbone component for BTO products. This version enables data flow between multiple instances of UCMDB, and integration with BTO products to enable solution deployment.
- **UCMDB Integrations License.** The Integrations license adds 3rd party integrations on top of the UCMDB Foundation license.
- **UCMDB DDM Advanced License.** The DDM Advanced license includes all discovery capabilities to discover the IT infrastructure elements and feed that information as CIs and Relationships within the UCMDB.

Defined Terms and Definitions

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. This does not include personal computers (or any computer primarily serving a single individual).

The HP Universal CMDB Server uses a server OS instance-based licensing scheme for the DDM Advanced license with a minimum purchase requirement of 100 OS instances. An OS instance counts both physical and virtual systems including the physical system hosting one or more virtual systems. The DDM Advanced license entitles the licensee to integrate third party (non-HP) data sources to extend discovery. Server data integrations require one license for each Managed Server to extend discovery. The Licensee is entitled to one DDMi license for every DDM OS instance.

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

License for HP Software-as-a-Service

All packages.

License for HP ServiceCenter/Service Manager and Other Integrations

The following packages are available:

- UCMDB7-SCSM
- SAR_Integration
- DDMI_Integration
- NNM_Integration
- SE_Integration
- SM_Integration

Note:

- The name of the license file is ucmdb_license.xml.
- You are asked for the location of the license file during installation. The default location of the license is: **C:\hp\UCMDB\UCMDBServer\conf**.
- Two weeks before the license expires, a reminder message is displayed for you to renew the license.

Data Flow Probe Licensing

You should install the Data Flow Probe, no matter which license you are running. If you have the Foundation license, the Probe is needed to run the Integration jobs (NNMi, SE, and DDMi). For details, see "UCMDB Data Flow Probe Installation" on page 103.

Tasks

Upgrade to the Integrations or DDM Advanced Licenses

When you install HP Universal CMDB, you receive the Universal CMDB Foundation license. To obtain the file needed to upgrade to the Integrations or DDM Advanced licenses, 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.

3 Use the JMX console to force a license change:

- **a** Launch a Web browser and enter the address **http://<server_name>.<domain_name>:8080/jmx-console**, where **<server_name>** is the name of the machine on which UCMDB is installed. When prompted, enter the JMX Console authentication credentials (if you do not have these credentials, contact your system administrator).

- **b** Under CMDB, click **service=UCMDB UI** to open the JMX MBEAN View page.

- **c** Locate **java.lang.String getLicenseForCustomer()** and enter the following information:

  In the force parameter box, select **True**.

  In the ParamValue box for the parameter **customerId**, enter **1**.

  Click **Invoke**.

Note: To verify the type of license that is installed, select **False** and enter the customer ID. Details about the license are displayed.

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 procedure in "Discover the SE Oracle Database" in *Discovery and Integration Content Guide*.

- **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 i (NNMi) Integration with HP Universal CMDB"* in *Discovery and Integration Content Guide*.

4

Getting Started with HP Universal CMDB

This chapter includes:

Concepts

➤ Predeployment Planning on page 45

Tasks

➤ Get Started on page 48

➤ Basic Administration Tasks on page 49

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 (DDM) and ensure that the protocols are available for use.
	Verify that you have access rights for the protocols to be used for DDM. 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

✔	Step
	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)
	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 DDM. For details, see "Discovery Scheduler Dialog Box" in *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 13.

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 21.

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 45.

4 **Install HP Universal CMDB components.**

Install the Server (on a Windows system) and Data Flow Probe. For details, see "Installation Procedure Overview" on page 26 and Part II, "Installation."

5 **Log in to HP Universal CMDB.**

Launch HP Universal CMDB. For details, see Chapter 26, "Logging In to HP Universal CMDB."

6 **Initiate system administration.**

Set up the HP Universal CMDB system. For details, see "Administration" in *HP UCMDB 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 DDM users can run the discovery process to identify IT resources in the network infrastructure. For details, see *Data Flow Management Guide*.

2 **When setting up DDM, 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 UCMDB Administration Guide*.

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

For details, see "Reports" in *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 *Modeling Guide*.
- "Modeling Studio" in *Modeling Guide*.

5

HP Universal CMDB Services

This chapter includes:

Tasks

➤ View the Status of HP Universal CMDB Services on page 51

Reference

➤ HP Universal CMDB Services on page 53

Tasks

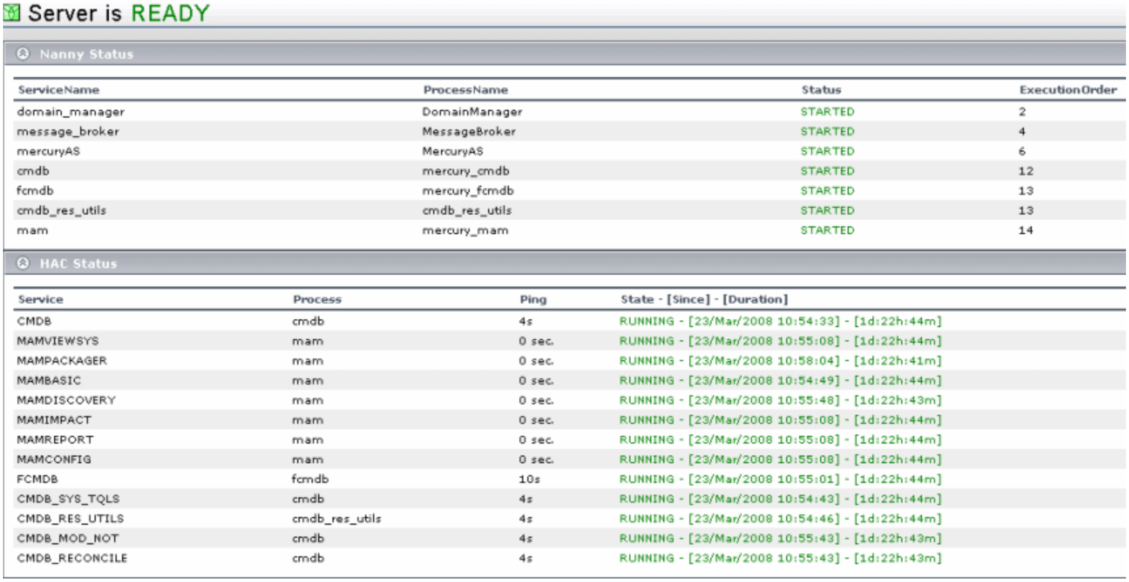
View the Status of HP Universal CMDB Services

Select **Start** > **Programs** > **HP UCMDB** > **UCMDB Server Status**.

Right-click the security warning above the HP Software title bar, select **Allow Blocked Content**, and click **Yes** in the dialog box that opens.

The line below the HP Software title bar indicates whether all the HP Universal CMDB services are running (Server is READY) or some are down (Server is NOT READY).

To view a list of all the services and their statuses, click the **Nanny Status** and **HAC Status** title bars.



Server is READY

Nanny Status

ServiceName	ProcessName	Status	ExecutionOrder
domain_manager	DomainManager	STARTED	2
message_broker	MessageBroker	STARTED	4
mercuryAS	MercuryAS	STARTED	6
cmdb	mercury_cmdb	STARTED	12
fcmdb	mercury_fcmdb	STARTED	13
cmdb_res_utils	cmdb_res_utils	STARTED	13
mam	mercury_mam	STARTED	14

HAC Status

Service	Process	Ping	State - [Since] - [Duration]
CMDB	cmdb	4s	RUNNING - [23/Mar/2008 10:54:33] - [1d:22h:44m]
MAMVIEWSYS	mam	0 sec.	RUNNING - [23/Mar/2008 10:55:08] - [1d:22h:44m]
MAMPACKAGER	mam	0 sec.	RUNNING - [23/Mar/2008 10:58:04] - [1d:22h:41m]
MAMBASIC	mam	0 sec.	RUNNING - [23/Mar/2008 10:54:49] - [1d:22h:44m]
MAMDISCOVERY	mam	0 sec.	RUNNING - [23/Mar/2008 10:55:48] - [1d:22h:43m]
MAMIMPACT	mam	0 sec.	RUNNING - [23/Mar/2008 10:55:08] - [1d:22h:44m]
MAMREPORT	mam	0 sec.	RUNNING - [23/Mar/2008 10:55:08] - [1d:22h:44m]
MAMCONFIG	mam	0 sec.	RUNNING - [23/Mar/2008 10:55:08] - [1d:22h:44m]
FCMDB	fcmdb	10s	RUNNING - [23/Mar/2008 10:55:01] - [1d:22h:44m]
CMDB_SYS_TQLS	cmdb	4s	RUNNING - [23/Mar/2008 10:54:43] - [1d:22h:44m]
CMDB_RES_UTILS	cmdb_res_utils	4s	RUNNING - [23/Mar/2008 10:54:46] - [1d:22h:44m]
CMDB_MOD_NOT	cmdb	4s	RUNNING - [23/Mar/2008 10:55:43] - [1d:22h:43m]
CMDB_RECONCILE	cmdb	4s	RUNNING - [23/Mar/2008 10:55:43] - [1d:22h:43m]

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

Reference

HP Universal CMDB Services

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

Service Name	Description of Service
CMDB	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.
CMDB_MOD_NOT	Responsible for notifications of changes that occur in the CMDB.
CMDB_ RECONCILE	The CMDB's data population reconciliation service. Responsible for the reconciliation engine of HP Universal CMDB.
CMDB_RES_UTILS	Responsible for storing the calculations of TQL and Enrichment results.
CMDB_SYS_TQLS	Responsible for the conditions applied to TQL nodes, and the condition results that are stored in the system TQL.
CMDBCLASS MODEL	Responsible for maintaining the class model in the CMDB.
CMDBMODEL UPDATE	Responsible for managing updates to the class model in the CMDB.
FCMDB	Responsible for retrieving federated data from external data sources for replication tasks and federated queries.
MAM BASIC	Responsible for user management, system parameters, and login/logout services.
MAM CONFIG	Responsible for snapshots, CI change queries, and TQL/View History queries.

Service Name	Description of Service
MAM DISCOVERY	Responsible for Data Flow Management-related services.
MAM IMPACT	Responsible for HP Universal CMDB impact, root cause, and correlation subsystems.
MAM PACKAGER	Responsible for packages. Packages are zip files containing resources that are structured in organized, predefined subdirectories.
MAM REPORT	Responsible for HP Universal CMDB report services, such as adding, editing, and removing System reports, calculation of Asset reports, Host Dependency reports.
MAMVIEWSYS	Responsible for the viewing system in HP Universal CMDB.

Troubleshooting and Limitations

Problem: UCMDB does not start automatically upon system restart.

Solution:

1. Select **Start** > **Program** > **HP UCMDB** > **Start UCMDB Server**.
2. Open the Window **Services** dialog box and select the **UCMDB Server** service.
3. Open the **Properties** dialog box.
4. 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**).

5 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 97.

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

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

Part II

Installation

6

HP Universal CMDB Installation on a Windows Platform

This chapter includes:

Concepts

- Installation Prerequisites on page 59

Tasks

- Install UCMDB on page 61
- Configure the UCMDB Mail Server on page 70
- Uninstall UCMDB on page 71

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 Chapter 1, "Introduction to HP Universal CMDB."
- 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 Chapter 3, "Licensing Models for HP Universal CMDB."
- For details on troubleshooting login, see Chapter 28, "Available Troubleshooting Resources."
- **Important:** If you are upgrading your current version to 9.00, read the chapter "Upgrading HP Universal CMDB to Version 9.00" on page 121 before uninstalling your current version. In that chapter, the section "Upgrade Federated CMDB Adapters" on page 207, 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 Chapter 8, "UCMDB Server Configuration."
  - 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 UCMDB

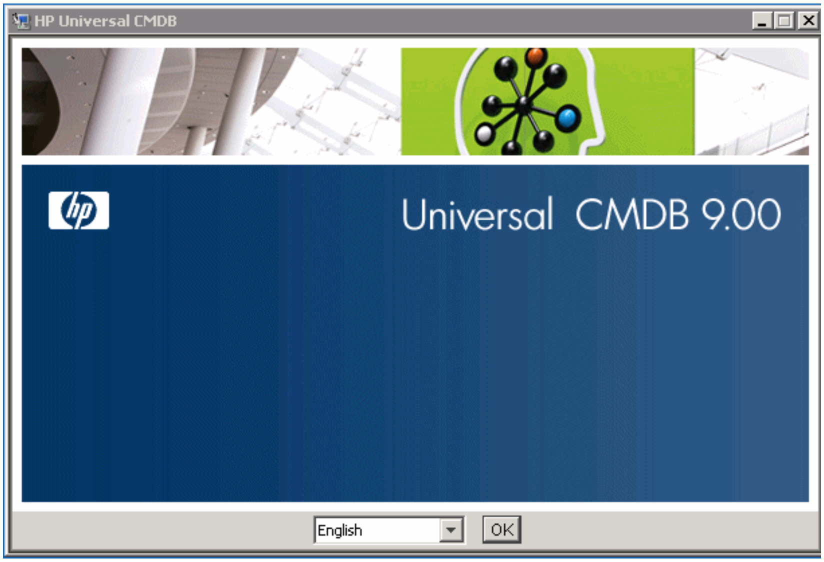
The following procedure explains how to install HP Universal CMDB.

1 Insert the **HP Universal CMDB Windows Installation** DVD into the drive from which you want to install. If you are installing from a network drive, connect to it.

2 Locate the UCMDB executable file: **HPUCMDB_Server_90.exe**.

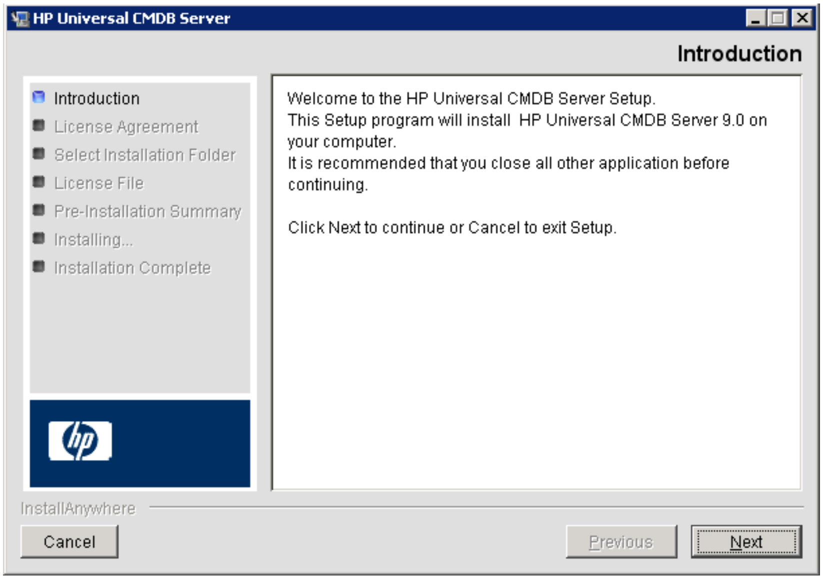
3 Double-click the file to open the splash screen.

If the digital signature is valid, the splash screen opens:



4 Choose the locale language and click **OK**.

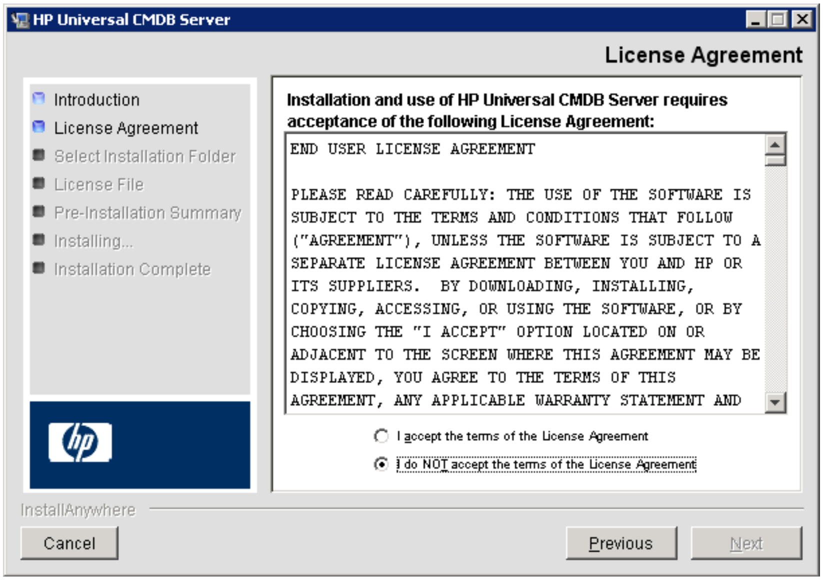
The Introduction dialog box opens.



Welcome to the HP Universal CMDB Server Setup.
This Setup program will install HP Universal CMDB Server 9.0 on your computer.
It is recommended that you close all other application before continuing.

Click Next to continue or Cancel to exit Setup.

5 Click **Next** to open the License Agreement dialog box.



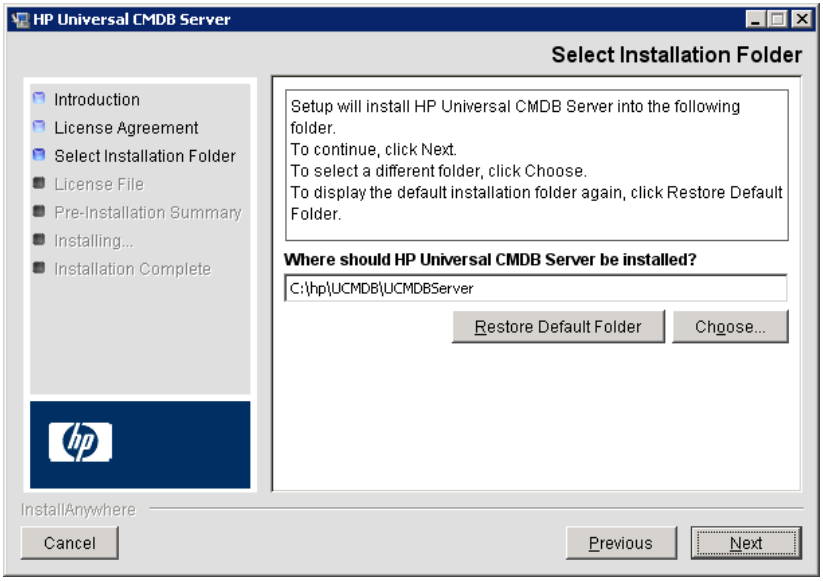
Installation and use of HP Universal CMDB Server requires acceptance of the following License Agreement:

```
END USER LICENSE AGREEMENT

PLEASE READ CAREFULLY: THE USE OF THE SOFTWARE IS
SUBJECT TO THE TERMS AND CONDITIONS THAT FOLLOW
("AGREEMENT"), UNLESS THE SOFTWARE IS SUBJECT TO A
SEPARATE LICENSE AGREEMENT BETWEEN YOU AND HP OR
ITS SUPPLIERS.  BY DOWNLOADING, INSTALLING,
COPYING, ACCESSING, OR USING THE SOFTWARE, OR BY
CHOOSING THE "I ACCEPT" OPTION LOCATED ON OR
ADJACENT TO THE SCREEN WHERE THIS AGREEMENT MAY BE
DISPLAYED, YOU AGREE TO THE TERMS OF THIS
AGREEMENT, ANY APPLICABLE WARRANTY STATEMENT AND
```

○ I accept the terms of the License Agreement
● I do NOT accept the terms of the License Agreement

Accept the terms of the license and click **Next** to open the Select Installation Folder dialog box.



Setup will install HP Universal CMDB Server into the following folder.
To continue, click Next.
To select a different folder, click Choose.
To display the default installation folder again, click Restore Default Folder.

Where should HP Universal CMDB Server be installed?

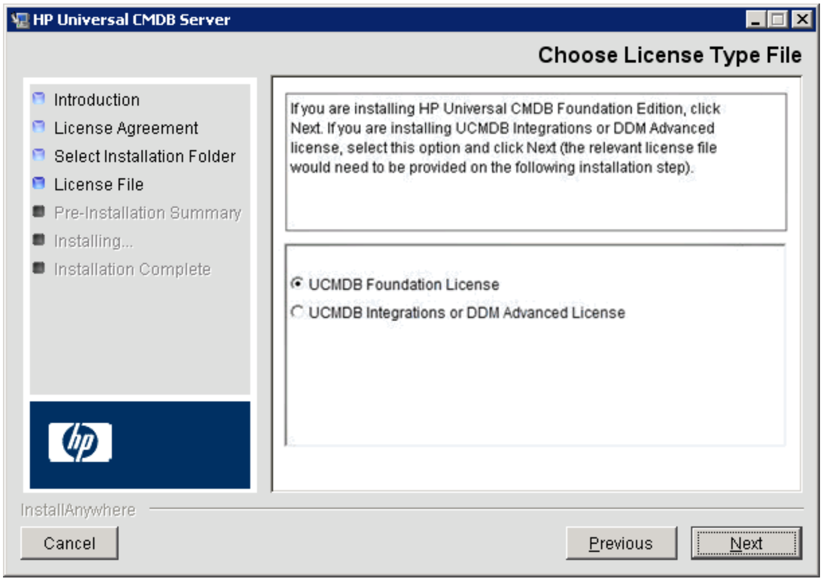
C:\hp\UCMDB\UCMDBServer

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**.

---

6 Click **Next** to open the Choose License Type File dialog box.



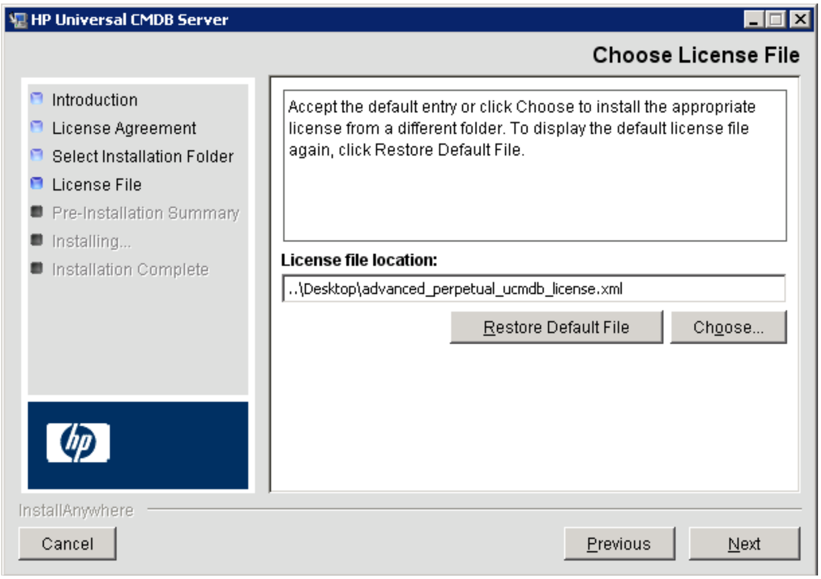
If you are installing HP Universal CMDB Foundation Edition, click Next. If you are installing UCMDB Integrations or DDM Advanced license, select this option and click Next (the relevant license file would need to be provided on the following installation step).

● UCMDB Foundation License
○ UCMDB Integrations or DDM Advanced License

To install the Foundation license, accept the default entry. To install the Integrations or DDM Advanced license, select **UCMDB Integrations or DDM Advanced license**. For details on licensing, see Chapter 3, “Licensing Models for HP Universal CMDB.”

If you select **UCMDB Foundation license**, skip to step 7.

If you select **UCMDB Integrations or DDM Advanced license**, click **Next** to open the Choose License File dialog box.



Accept the default entry or click Choose to install the appropriate license from a different folder. To display the default license file again, click Restore Default File.

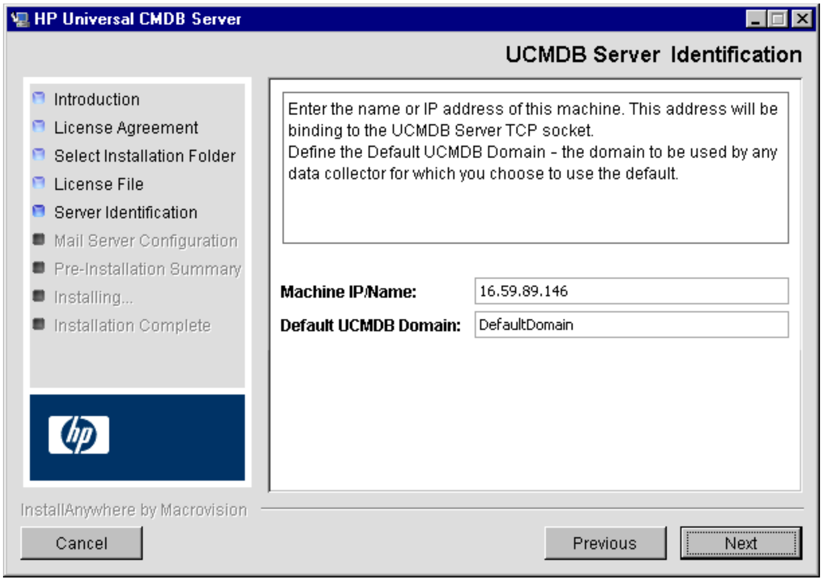
License file location: ..\Desktop\advanced_perpetual_ucmdb_license.xml

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**.

---

7 Click **Next** to open the UCMDB Server Identification dialog box.



Enter the name or IP address of this machine. This address will be binding to the UCMDB Server TCP socket.
Define the Default UCMDB Domain - the domain to be used by any data collector for which you choose to use the default.

Machine IP/Name: 16.59.89.146

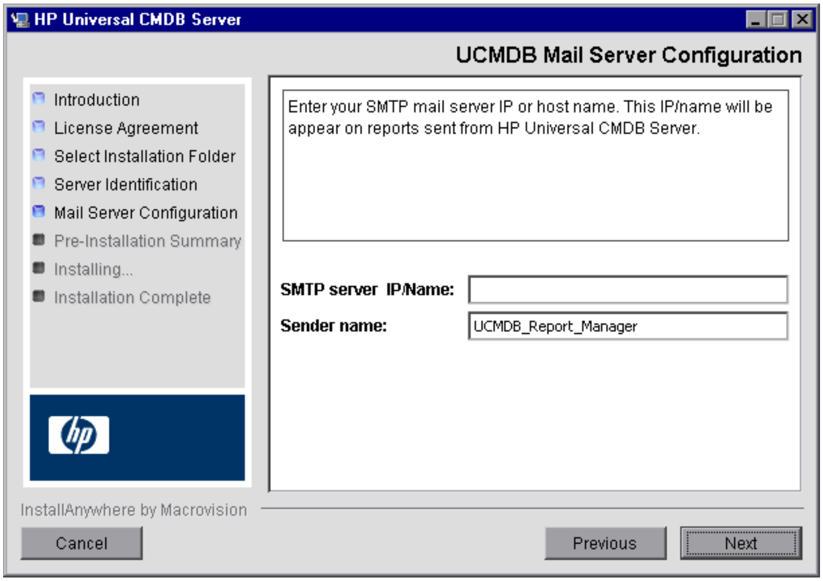
Default UCMDB Domain: DefaultDomain

Machine IP Name: Enter the IP address or the machine name of the workstation on which the HP Universal CMDB server is to be installed, or accept the existing entry. The TCP socket is mapped to this address and port.

Default UCMDB Domain: Accept the default entry (**DefaultDomain**) or enter another domain identifier. This is the domain that is used by data collectors, for example, the Data Flow Probe. The default domain is the domain name to be used for data collectors if no specific, separate domain is specified during their installation.

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

8 Click **Next** to open the UCMDB Mail Server Configuration dialog box.



Enter your SMTP mail server IP or host name. This IP/name will be appear on reports sent from HP Universal CMDB Server.

SMTP server IP/Name:

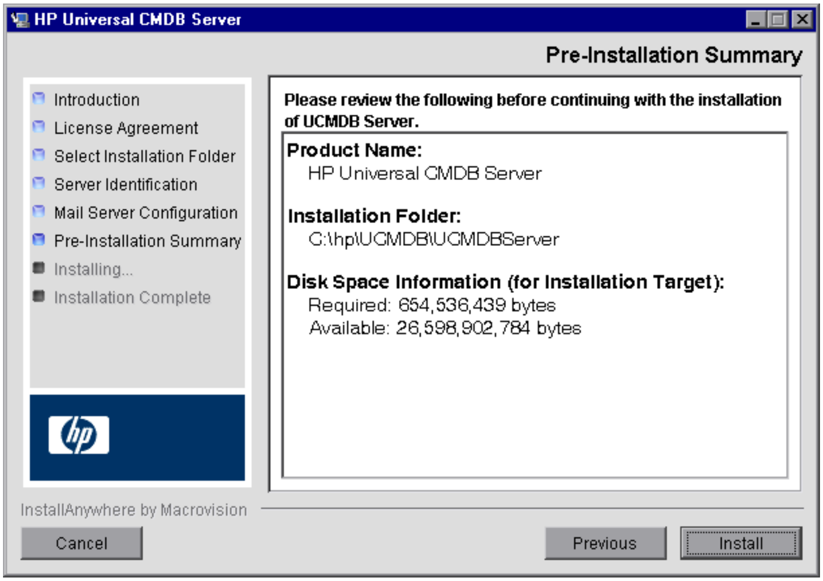
Sender name: UCMDB_Report_Manager

SMTP server IP/Name. Enter the server IP or name. It is recommended that you specify the complete Internet address of the SMTP server. Use only alphanumeric characters.

Sender name. Specify the name to appear in reports that HP Universal CMDB sends. Accept the default name (**UCMDB_Report_Manager**) or enter another sender name.

For an alternate method of configuring the UCMDB Mail Server, see "Configure the UCMDB Mail Server" on page 70.

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



Please review the following before continuing with the installation of UCMDB Server.

Product Name:
HP Universal CMDB Server

Installation Folder:
C:\hp\UCMDB\UCMDBServer

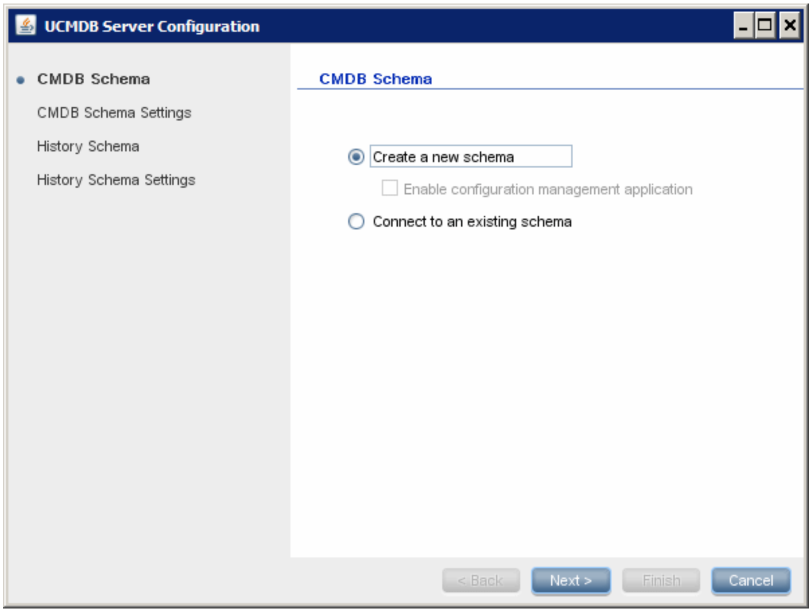
Disk Space Information (for Installation Target):
Required: 654,536,439 bytes
Available: 26,598,902,784 bytes

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

Launch the Configuration Wizard

11 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 and open the Introduction dialog box.

If you are performing an upgrade to UCMDB 9.00 or if you prefer, you can set up the database or schema later. Access the UCMDB Server Configuration Wizard from the Windows Start menu. For upgrade continuation information see “Upgrade to UCMDB 9.00” on page 125.



UCMDB Server Configuration

- CMDB Schema
- CMDB Schema Settings
- History Schema
- History Schema Settings

CMDB Schema

● Create a new schema

□ Enable configuration management application

○ Connect to an existing schema

During the following stages, you choose between creating a new schema (Microsoft SQL Server or Oracle Server), or connecting to an existing schema. You would probably create a new schema for a new installation of HP Universal CMDB and would connect to an existing schema 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 85.
- For the procedure for creating a Microsoft SQL Server database, see “Create a Microsoft SQL Server Database” on page 90.
- For the procedure for creating an Oracle schema, see “Create an Oracle Schema” on page 94.
- For the procedure for connecting to an existing Microsoft SQL Server database, see “Connect to an Existing Microsoft SQL Server Database” on page 96.
- For the procedure for connecting to an existing Oracle schema, see “Connect to an Existing Oracle Schema” on page 96.

Configure the UCMDB Mail Server

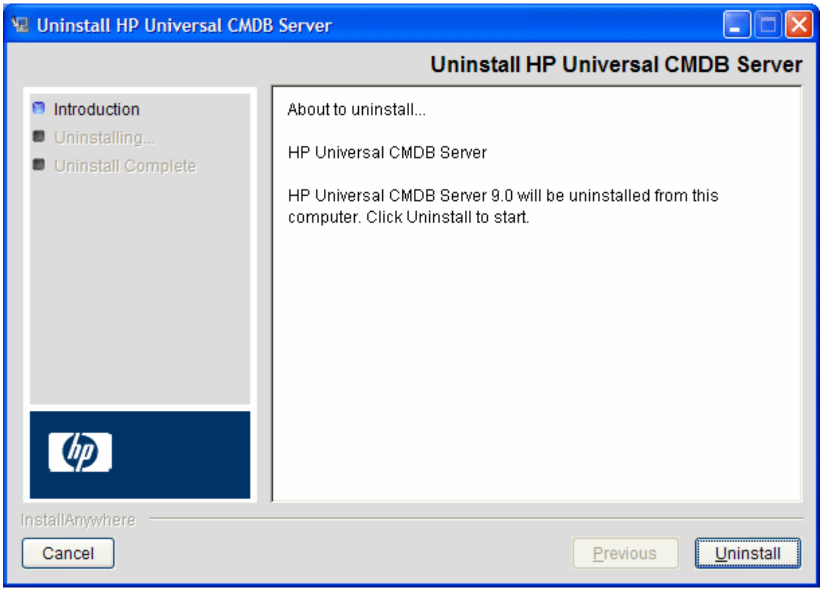
To configure the UCMDB Mail server:

1. In **Infrastructure Settings**, select the **Mail Settings** Category.
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 UCMDB

The following procedure explains how to uninstall HP Universal CMDB.

1 From the Start menu, choose **Programs** > **HP** > **UCMDB** > **Uninstall UCMDB**. The Uninstall HP Universal CMDB Server dialog box opens.



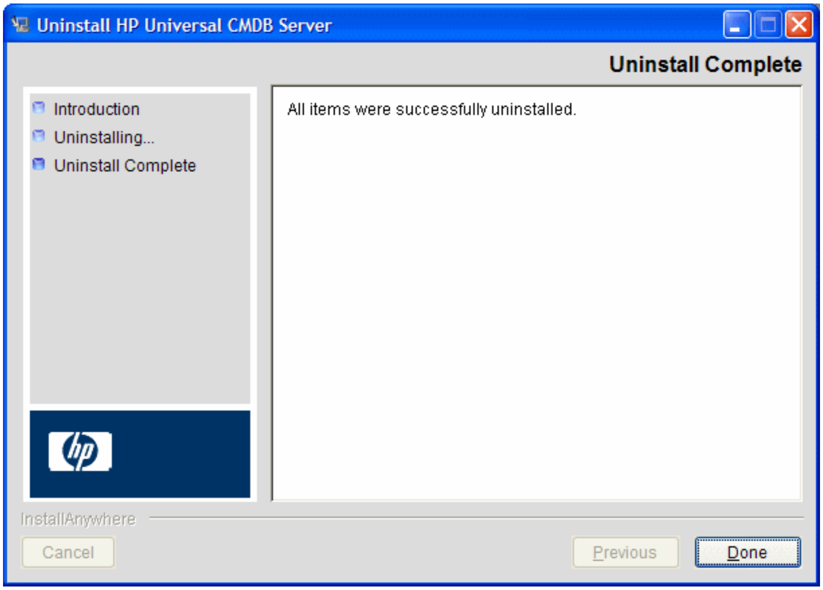
About to uninstall...

HP Universal CMDB Server

HP Universal CMDB Server 9.0 will be uninstalled from this computer. Click Uninstall to start.

2 Click **Uninstall**.

When uninstall is complete, a message is displayed:



All items were successfully uninstalled.

7

HP Universal CMDB Installation on a Linux Platform

This chapter includes:

Concepts

- Installation Prerequisites on page 73

Tasks

- Install HP Universal CMDB on page 74
- Configure the UCMDB Mail Server on page 82
- Uninstall UCMDB on page 83

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 Chapter 1, "Introduction to HP Universal CMDB."
- 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 Chapter 3, "Licensing Models for HP Universal CMDB."
- For details on troubleshooting login, see Chapter 28, "Available Troubleshooting Resources."
- 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 Chapter 8, "UCMDB Server Configuration."
  - 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

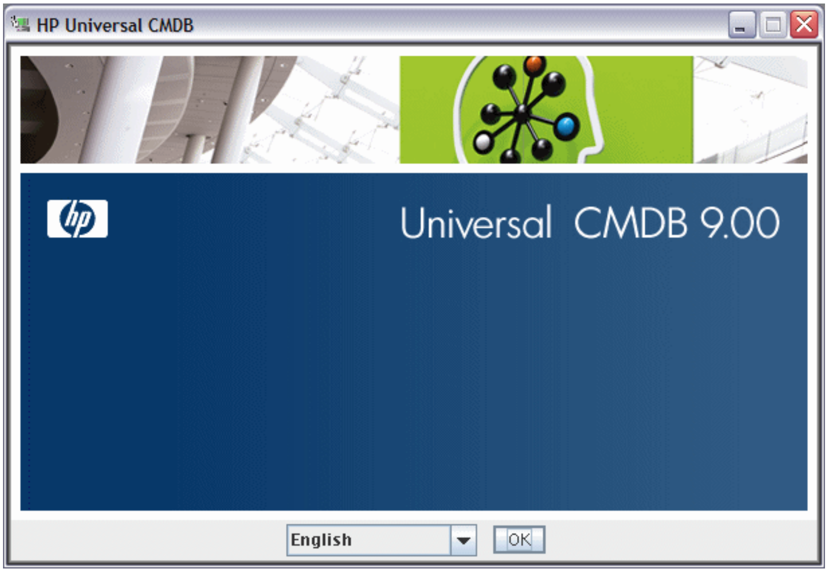
The following procedure explains how to install HP Universal CMDB.

1. The HP Universal CMDB 9.00 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_90.bin**.

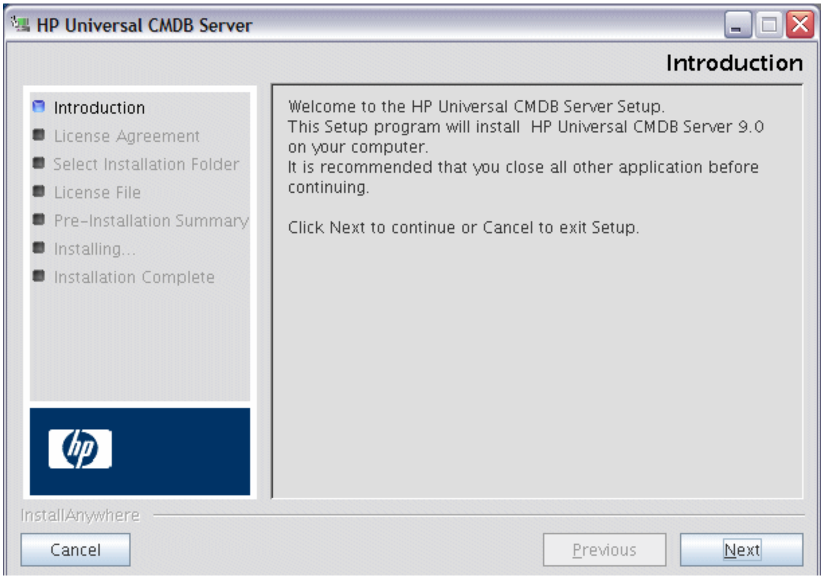
3 **sh <path-to-installer>/HPUCMDB_Server_90.bin** to open the splash screen.

The splash screen opens:



4 Choose the locale language and click **OK**.

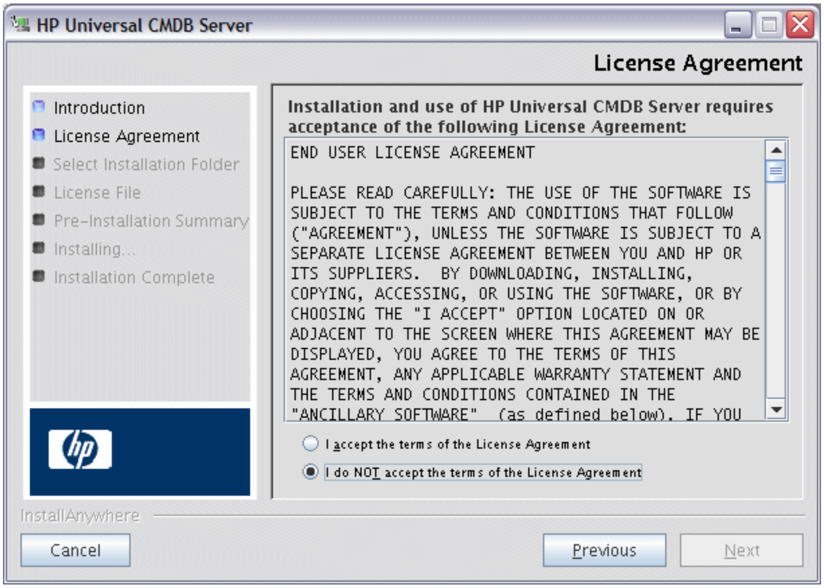
The **Introduction** dialog box opens.



Welcome to the HP Universal CMDB Server Setup.
This Setup program will install HP Universal CMDB Server 9.0 on your computer.
It is recommended that you close all other application before continuing.

Click Next to continue or Cancel to exit Setup.

5 Click **Next** to open the **License Agreement** dialog box.



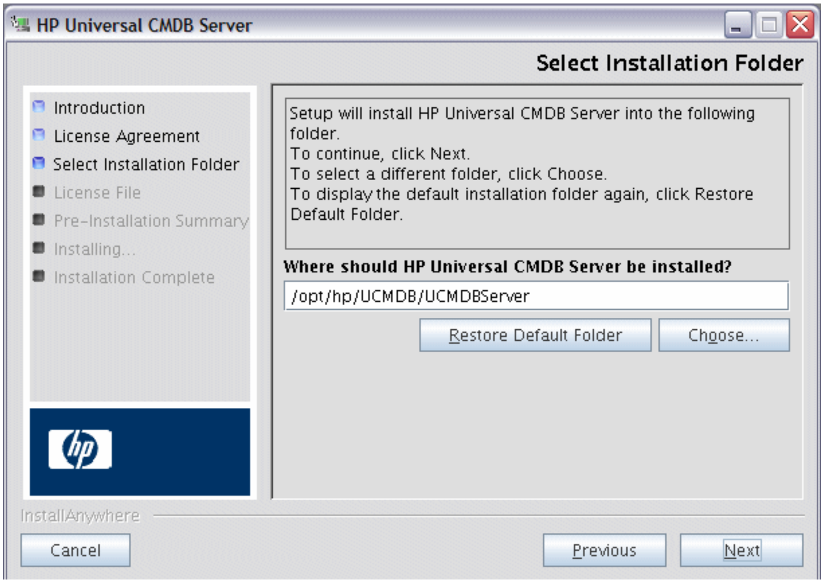
Installation and use of HP Universal CMDB Server requires acceptance of the following License Agreement:

```
END USER LICENSE AGREEMENT

PLEASE READ CAREFULLY: THE USE OF THE SOFTWARE IS
SUBJECT TO THE TERMS AND CONDITIONS THAT FOLLOW
("AGREEMENT"), UNLESS THE SOFTWARE IS SUBJECT TO A
SEPARATE LICENSE AGREEMENT BETWEEN YOU AND HP OR
ITS SUPPLIERS.  BY DOWNLOADING, INSTALLING,
COPYING, ACCESSING, OR USING THE SOFTWARE, OR BY
CHOOSING THE "I ACCEPT" OPTION LOCATED ON OR
ADJACENT TO THE SCREEN WHERE THIS AGREEMENT MAY BE
DISPLAYED, YOU AGREE TO THE TERMS OF THIS
AGREEMENT, ANY APPLICABLE WARRANTY STATEMENT AND
THE TERMS AND CONDITIONS CONTAINED IN THE
"ANCILLARY SOFTWARE"  (as defined below). IF YOU
```

○ I accept the terms of the License Agreement
● I do NOT accept the terms of the License Agreement

Accept the terms of the license and click **Next** to open the **Select Installation Folder** dialog box.



Setup will install HP Universal CMDB Server into the following folder.
To continue, click Next.
To select a different folder, click Choose.
To display the default installation folder again, click Restore Default Folder.

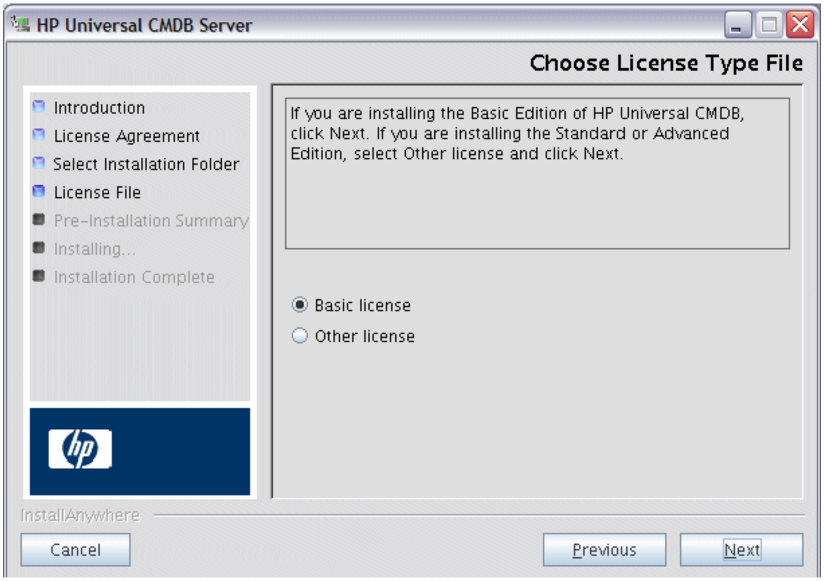
Where should HP Universal CMDB Server be installed?

/opt/hp/UCMDB/UCMDBServer

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**.

6 Click **Next** to open the Choose License Type File dialog box.



If you are installing the Basic Edition of HP Universal CMDB, click Next. If you are installing the Standard or Advanced Edition, select Other license and click Next.

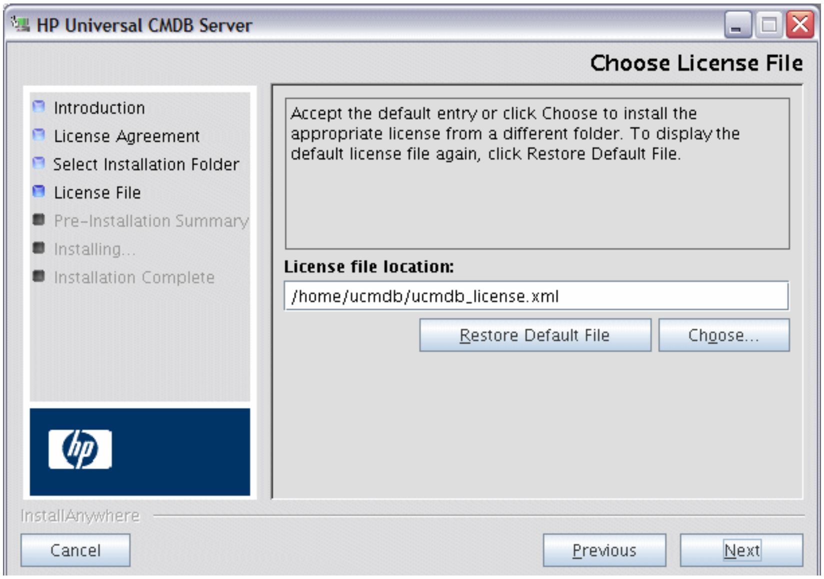
● Basic license

○ Other license

To install the Foundation license, accept the default entry. To install the Integrations or DDM Advanced license, select **UCMDB Integrations or DDM Advanced license**. For details on licensing, see Chapter 3, “Licensing Models for HP Universal CMDB.”

If you select **UCMDB Foundation license**, skip to step 7.

If you select **UCMDB Integrations or DDM Advanced license**, click **Next** to open the Choose License File dialog box.



HP Universal CMDB Server

Choose License File

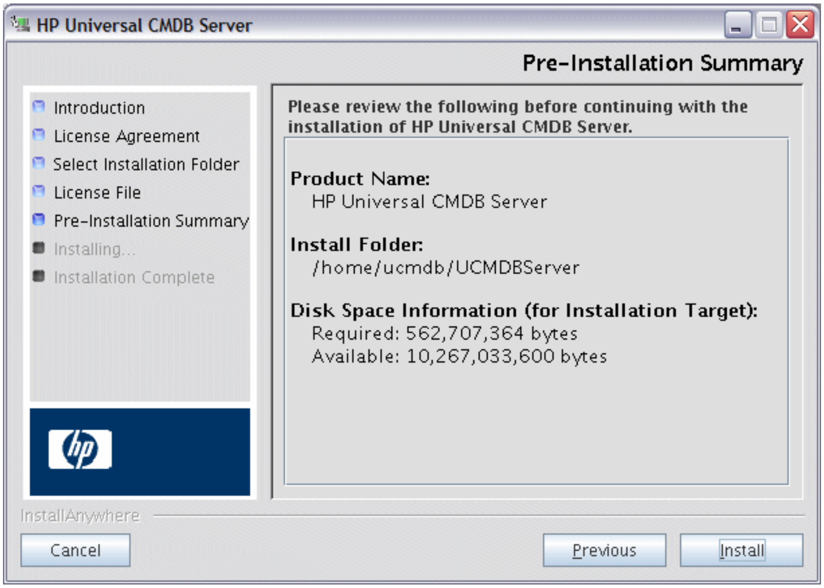
Accept the default entry or click Choose to install the appropriate license from a different folder. To display the default license file again, click Restore Default File.

License file location:

/home/ucmdb/ucmdb_license.xml

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**).

7 Click **Next** to open the Pre-Installation Summary dialog box that lists the installation options you have selected. If you are satisfied with the summary, click **Install**.



HP Universal CMDB Server

Pre-Installation Summary

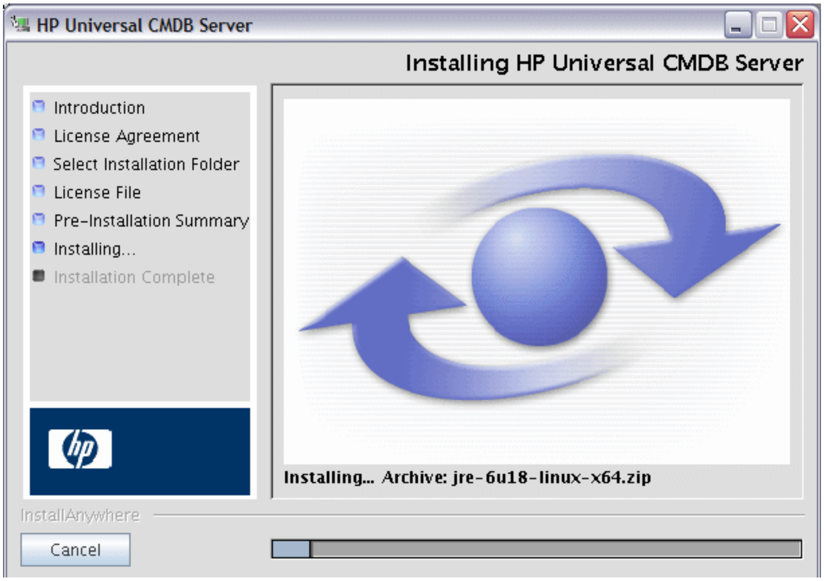
Please review the following before continuing with the installation of HP Universal CMDB Server.

Product Name:
HP Universal CMDB Server

Install Folder:
/home/ucmdb/UCMDBServer

Disk Space Information (for Installation Target):
Required: 562,707,364 bytes
Available: 10,267,033,600 bytes

8 A message is displayed indicating that the installation is currently being performed.

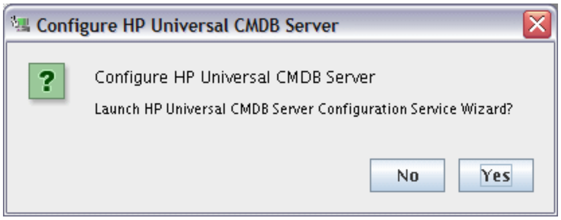


HP Universal CMDB Server

Installing HP Universal CMDB Server

Installing... Archive: jre-6u18-linux-x64.zip

9 After the installation has completed the dialog prompts you to launch the **UCMDB Server Configuration Wizard** (to set up the database or schema).



Configure HP Universal CMDB Server

Configure HP Universal CMDB Server

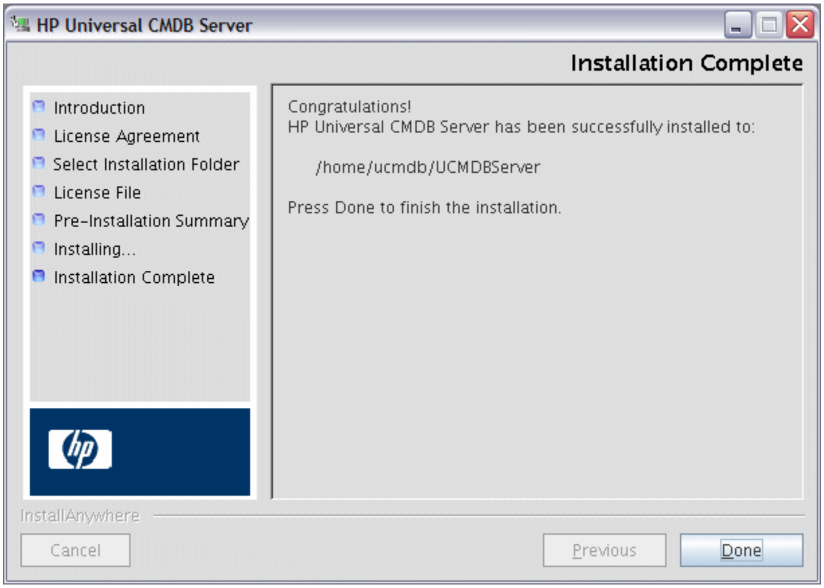
Launch HP Universal CMDB Server Configuration Service Wizard?

10 Click **Yes** to continue with the configuration and open the Wizard dialog box.

If you prefer, you can set up the database or schema later by running the script **configure.sh** located in **bin** subfolder of the installation folder.

11 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 85.

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



Congratulations!
HP Universal CMDB Server has been successfully installed to:

/home/ucmdb/UCMDBServer

Press Done to finish the installation.

Configure the UCMDB Mail Server

To configure the UCMDB Mail server:

1 In **Infrastructure Settings**, select the **Mail Settings** Category.

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**.

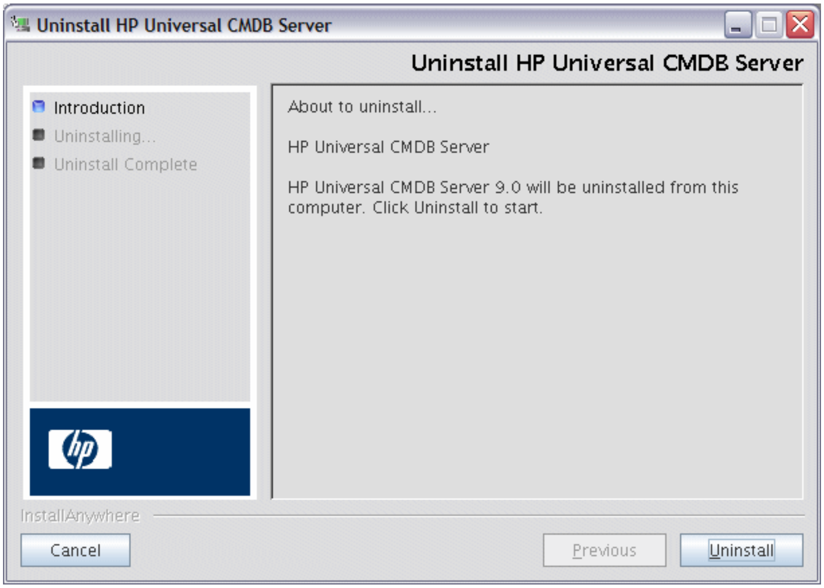
5 Edit the setting for **Email sender** with the name to appear in reports that HP Universal CMDB sends.

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 UCMDB

The following provides a procedure for uninstalling UCMDB.

1 Execute the **Uninstall_UCMDBServer** script from the **UninstallerData** subfolder of the Installation folder.



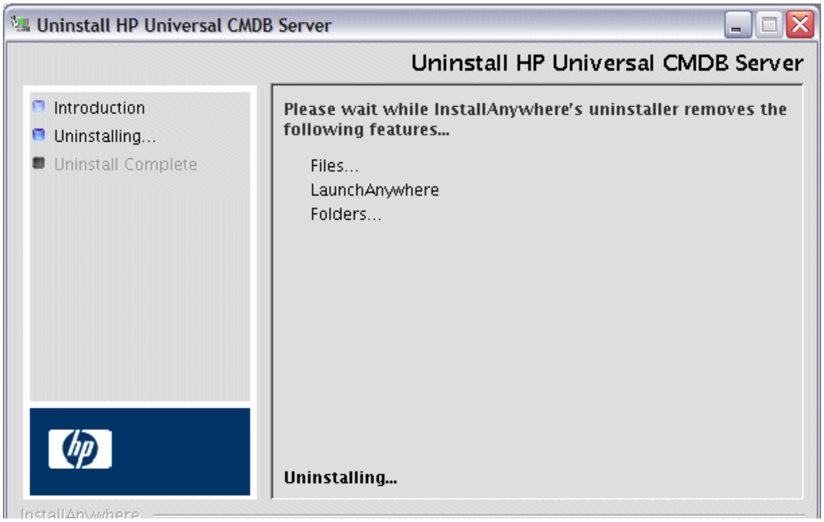
Uninstall HP Universal CMDB Server

About to uninstall...

HP Universal CMDB Server

HP Universal CMDB Server 9.0 will be uninstalled from this computer. Click Uninstall to start.

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



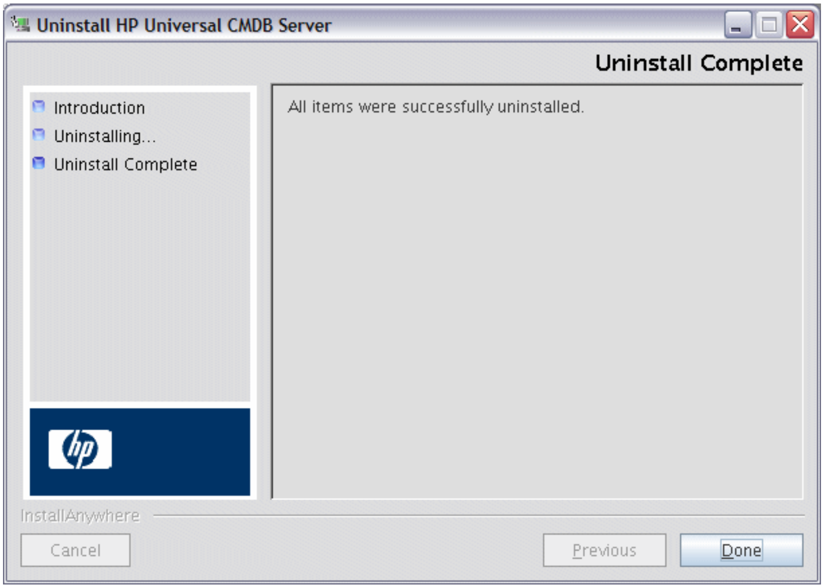
Uninstall HP Universal CMDB Server
Uninstall HP Universal CMDB Server
Introduction
Uninstalling...
Uninstall Complete
InstallAnywhere

Please wait while InstallAnywhere's uninstaller removes the following features...

Files...
LaunchAnywhere
Folders...

Uninstalling...

3 Click **Done** to complete the uninstall process.



All items were successfully uninstalled.

8

UCMDB Server Configuration

This chapter includes:

Concepts

- ➤ Choosing the Database or Schema on page 85
- ➤ Required Information for Setting Database Parameters on page 87
- ➤ Allocating Memory to Processes on page 89

Tasks

- ➤ Access the UCMDB Server Configuration Wizard on page 89
- ➤ Create a Microsoft SQL Server Database on page 90
- ➤ Create an Oracle Schema on page 94
- ➤ Connect to an Existing Microsoft SQL Server Database on page 96
- ➤ Connect to an Existing Oracle Schema on page 96
- ➤ Restart the Server on page 96

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 Chapter 6, "HP Universal CMDB Installation on a Windows Platform" or Chapter 7, "HP Universal CMDB Installation on a Linux Platform."

Note: It is highly recommended that you thoroughly read the introduction to this guide before commencing installation. For details, see Chapter 1, "Introduction to HP Universal CMDB."

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 use the database contents you have from using 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 both 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's TCP/IP port. HP Universal CMDB automatically displays the default port, **1433**.
- **Database 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 Chapter 10, "Changing the HP Universal CMDB Service User." 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 password.** The name and password of the existing user schema, or the name that you will give 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 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.

Allocating Memory to Processes

The amount of memory allocated to a process is calculated by:

- The settings in the **C:\hp\UCMDB\UCMDBServer\j2f\conf\deployment.xml** file.
- The amount of physical memory available on the server at the time the UCMDB Server Configuration Wizard is running.

  If you add more memory to the server later, you should rerun the Wizard so that HP Universal CMDB can take advantage of the added memory.

Tasks

Access the UCMDB Server Configuration Wizard

If you did not set up the database or schema during installation, you can set it up using one of the following methods:

- Access the UCMDB Server Configuration Wizard from the Windows Start menu by selecting **Start** > **Programs** > **HP UCMDB** > **Start UCMDB Server Configuration Wizard**.
- Double-click the following file: <**HP Universal CMDB root directory**>**\UCMDBServer\j2f\tools\ConfigServer\ucmdb-config-server-wizard.bat**.

Create a Microsoft SQL Server Database

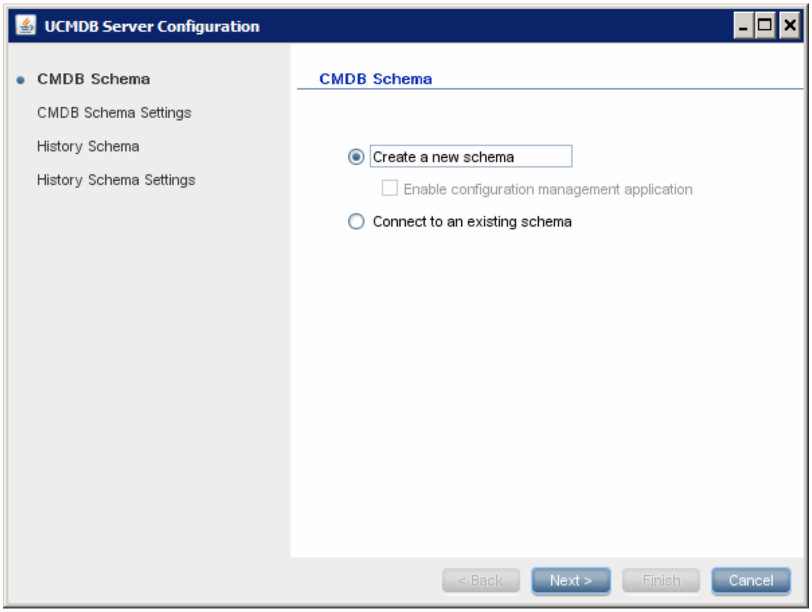
This section explains how to set up the Microsoft SQL Server database. There are two parts to this stage of the installation: setting up the CMDB schema and setting up the CMDB History schema.

Note: In UCMDB version 9.00 the Foundations and CMDB databases are combined. For upgrade information see "Upgrading HP Universal CMDB to Version 9.00" on page 121.

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 89.



CMDB Schema

● Create a new schema

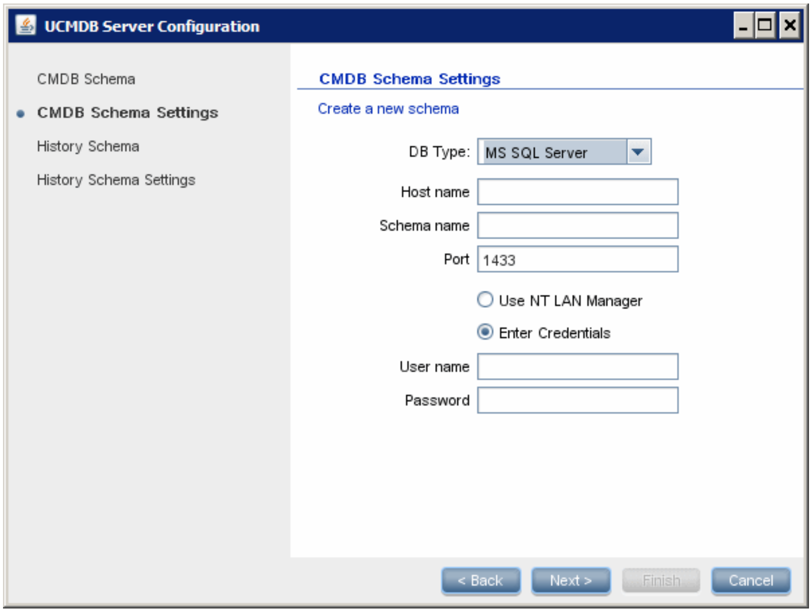
□ Enable configuration management application

○ Connect to an existing schema

Select **Create a new schema.**

2 Click **Next** to open the CMDB Schema Settings dialog box.

3 In the DB Type box, select **MS SQL Server**.



CMDB Schema Settings

Create a new schema

DB Type: MS SQL Server

Host name

Schema name

Port 1433

○ Use NT LAN Manager

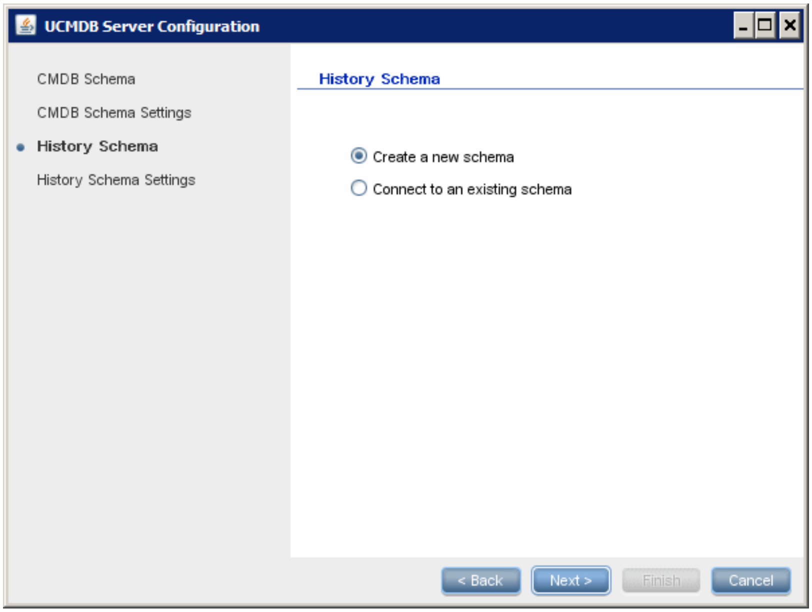
● Enter Credentials

User name

Password

- ➤ Enter the host name, schema name, and port through which the database is accessed.
- ➤ 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.
- ➤ Enter the name and password of the user with permissions to access the database.

4 Click **Next** to open the History Schema dialog box.

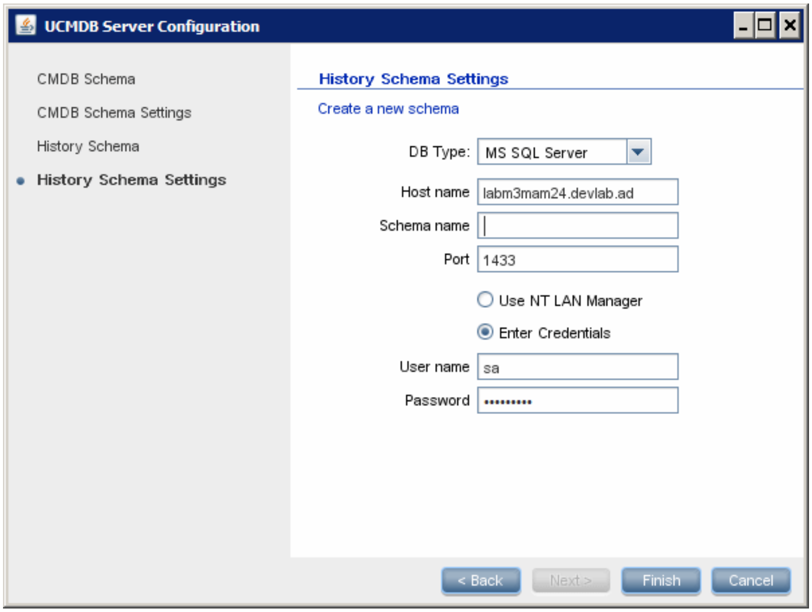


History Schema

● Create a new schema

○ Connect to an existing schema

5 Click **Next** to display the History Schema Settings dialog box.



History Schema Settings

Create a new schema

DB Type: MS SQL Server

Host name labm3mam24.devlab.ad

Schema name

Port 1433

○ Use NT LAN Manager

● Enter Credentials

User name sa

Password •••••••••

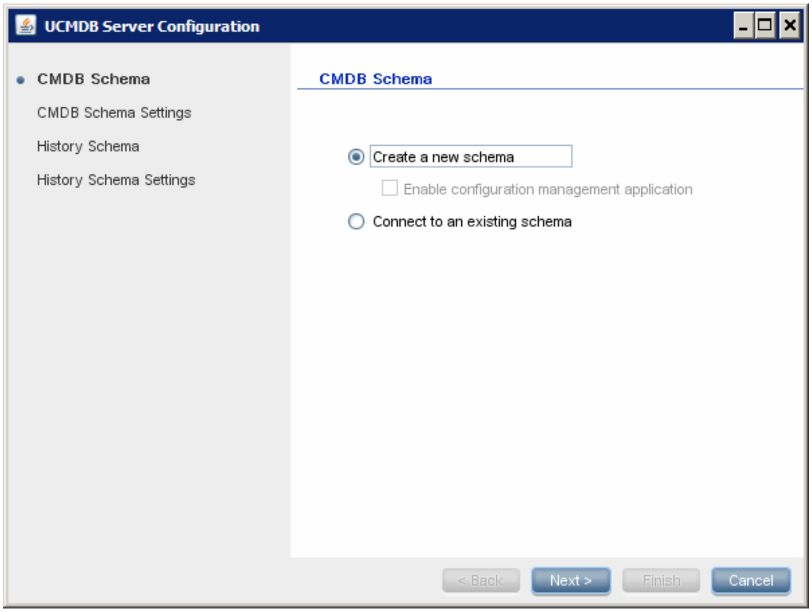
Enter the schema name and click **Finish**.

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 Database Settings dialog box.



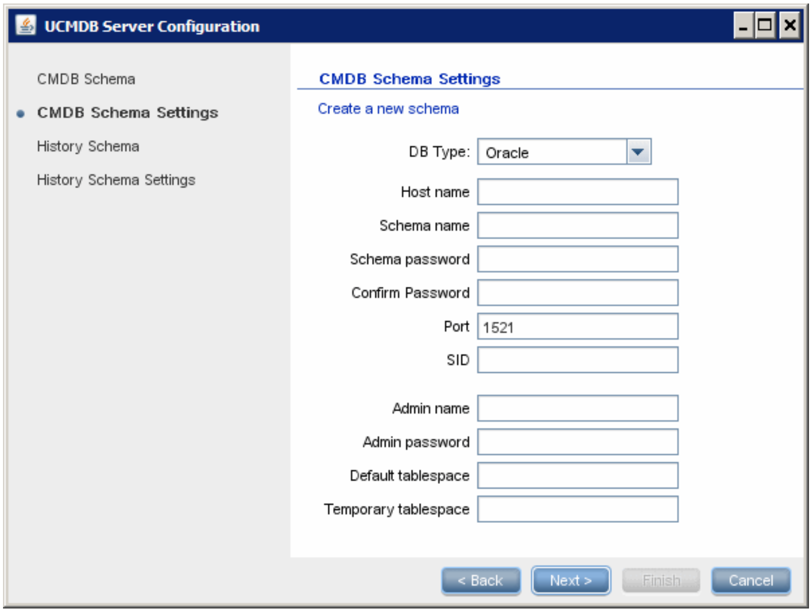
● Create a new schema

□ Enable configuration management application

○ Connect to an existing schema

2 Click **Next** to open the CMDB Schema Settings dialog box.

3 In the DB Type box, select **Oracle**.



UCMDB Server Configuration

CMDB Schema Settings

Create a new schema

DB Type: Oracle

Port 1521

- Enter the host name, schema name and password, and confirm the password. The schema name should be unique.
- Accept the port through which the database is accessed or change the port number. Enter the SID.
- Enter the details of the schema:
  - **Admin name** and **password.** Enter the name and password of the admin user with permissions to access the database.
  - **Default tablespace.** Enter the default tablespace name.
  - **Temporary tablespace.** If your database administrator created a non-default temporary tablespace, enter that name; otherwise, enter **temp**.

4 Enter the details for the CMDB History schema.

5 Click **Finish**.

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 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 90, select **Connect to an existing schema** and click **Next**.
- In step 4 on page 93, 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 to the CMDB History schema.

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

- In step 1 on page 94, select **Connect to an existing schema** and click **Next**.
- In the History Schema dialog box, select **Connect to an existing schema** and click **Next**.

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 Server Service

This chapter includes:

Tasks

- Change the HP Universal CMDB Server Service User on page 97
- Start and Stop the HP Universal CMDB Server Service on page 99

Tasks

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:

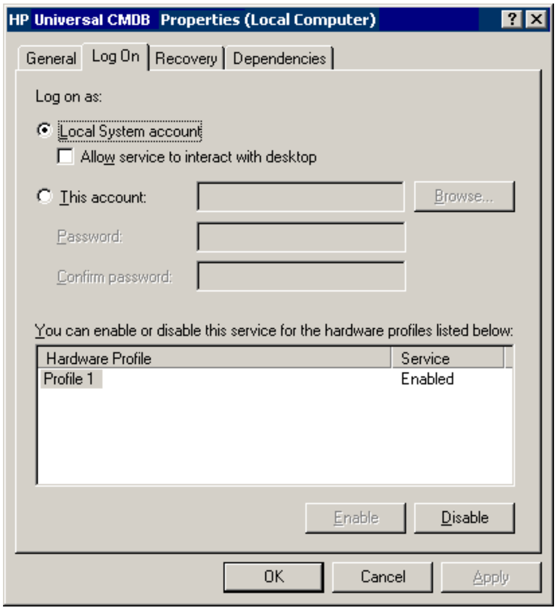
- sufficient database permissions (as defined by the database administrator)
- sufficient network permissions
- administrator permissions on the local server

To change the service user.

1 Disable HP Universal CMDB through the Start menu (**Start** > **Programs** > **HP UCMDB** > **Stop UCMDB Server**) or by stopping the HP Universal CMDB Server service. For details, see “Start and Stop the HP Universal CMDB Server Service” on page 99.

2 In Microsoft's **Services** window, double-click **UCMDB Server**. The **UCMDB Server Properties (Local Computer)** dialog box opens.

3 Click the **Log On** tab.



Log on as:

● Local System account

□ Allow service to interact with desktop

○ This account:

Password:

Confirm password:

You can enable or disable this service for the hardware profiles listed below:

Hardware Profile	Service
Profile 1	Enabled

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** > **Programs** > **HP UCMDB** > **Start UCMDB Server**) or by starting the HP Universal CMDB Server service. For details, see "Start and Stop the HP Universal CMDB Server Service" on page 99.

Start and Stop the HP Universal CMDB Server Service

Access the Microsoft **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 UCMDB through the Start menu, see "Start and Stop the Server on the Windows Platform" on page 315.

Part III

Data Flow Probe Installation

10

UCMDB Data Flow Probe Installation

This chapter includes:

Tasks

- ➤ Install the UCMDB Data Flow Probe on page 103
- ➤ Upgrade the Probe on page 113
- ➤ Run Probe Manager and Probe Gateway on Separate Machines on page 113
- ➤ Configure the Probe Manager and Probe Gateway Components on page 114

Tasks

Install the UCMDB Data Flow Probe

Note: It is highly recommended to thoroughly read “Introduction to HP Universal CMDB” on page 21 before commencing installation. For more information on Data Flow Management read “Introduction to Data Flow Management” in the *Data Flow Management Guide*.

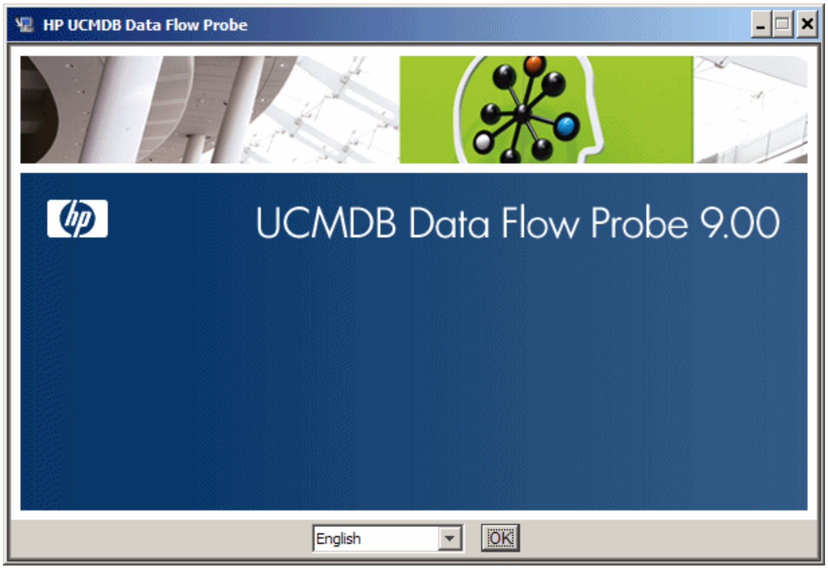
The following procedure explains how to install the Data Flow Probe on a Windows platform.

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.

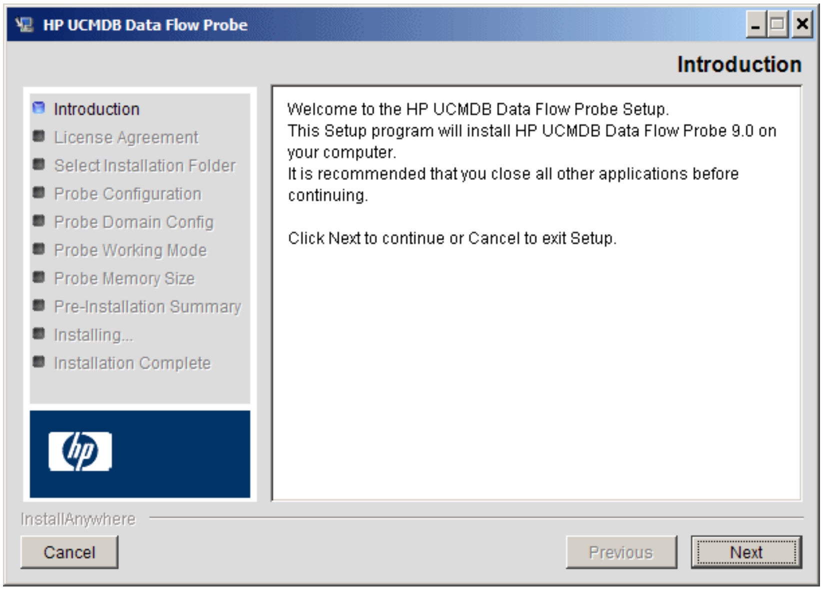
Note: For details on licensing, see “Licensing Models for HP Universal CMDB” on page 39.

To install the UCMDB Data Flow Probe:

1. Insert the **HP Universal CMDB 9.00 Setup Windows** DVD into the drive from which to install. If you are installing from a network drive, connect to it.
2. Double-click the <**DVD root folder**>\ **UCMDB90\HPUCMDB_DataFlowProbe_90.exe** file. A progress bar is displayed. Once the initial process is complete, the splash screen opens.



3 Choose the locale language and click **OK** to open the Introduction dialog box.



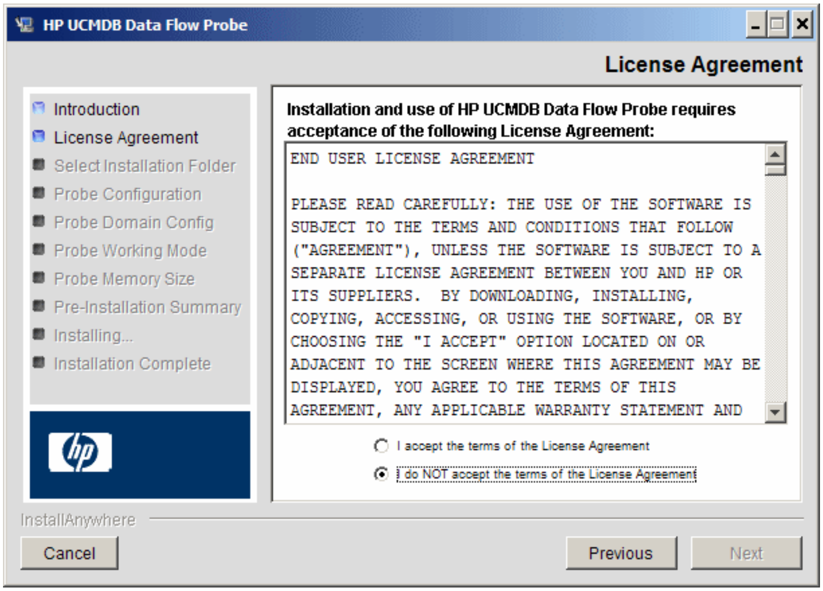
HP UCMDB Data Flow Probe

Introduction

Welcome to the HP UCMDB Data Flow Probe Setup.
This Setup program will install HP UCMDB Data Flow Probe 9.0 on your computer.
It is recommended that you close all other applications before continuing.

Click Next to continue or Cancel to exit Setup.

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



HP UCMDB Data Flow Probe

License Agreement

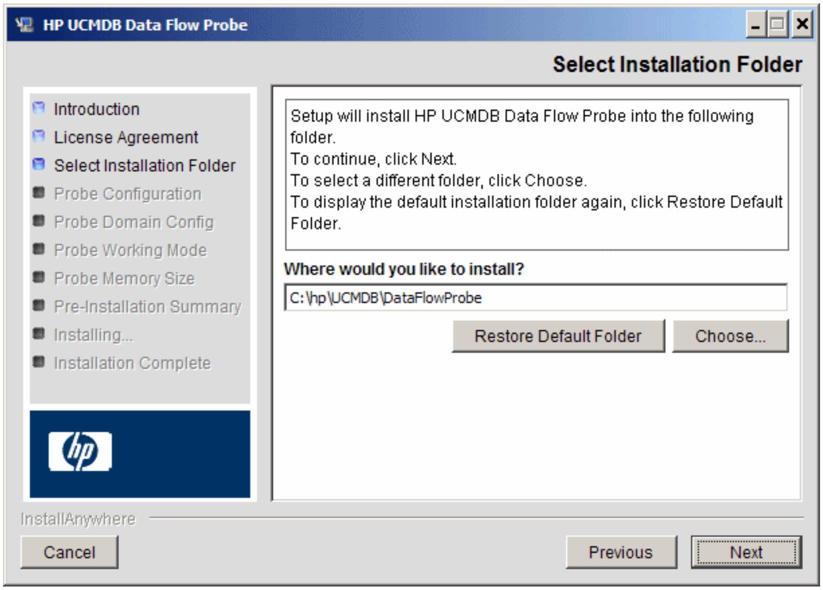
Installation and use of HP UCMDB Data Flow Probe requires acceptance of the following License Agreement:

```
END USER LICENSE AGREEMENT

PLEASE READ CAREFULLY: THE USE OF THE SOFTWARE IS
SUBJECT TO THE TERMS AND CONDITIONS THAT FOLLOW
("AGREEMENT"), UNLESS THE SOFTWARE IS SUBJECT TO A
SEPARATE LICENSE AGREEMENT BETWEEN YOU AND HP OR
ITS SUPPLIERS.  BY DOWNLOADING, INSTALLING,
COPYING, ACCESSING, OR USING THE SOFTWARE, OR BY
CHOOSING THE "I ACCEPT" OPTION LOCATED ON OR
ADJACENT TO THE SCREEN WHERE THIS AGREEMENT MAY BE
DISPLAYED, YOU AGREE TO THE TERMS OF THIS
AGREEMENT, ANY APPLICABLE WARRANTY STATEMENT AND
```

○ I accept the terms of the License Agreement
● I do NOT accept the terms of the License Agreement

5 Accept the terms of the agreement and click **Next** to open the Select Installation Folder dialog box.



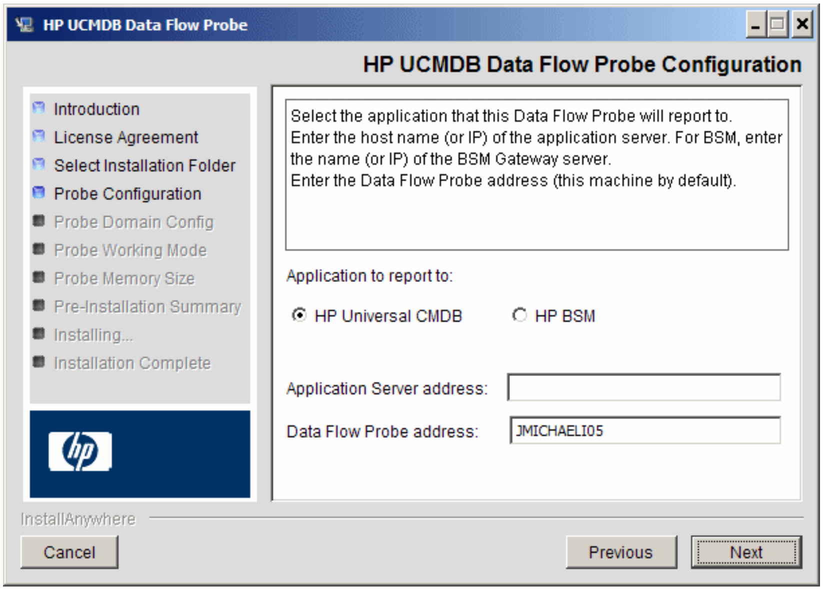
Setup will install HP UCMDB Data Flow Probe into the following folder.
To continue, click Next.
To select a different folder, click Choose.
To display the default installation folder again, click Restore Default Folder.

Where would you like to install?
C:\hp\UCMDB\DataFlowProbe

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: 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.



Select the application that this Data Flow Probe will report to.
Enter the host name (or IP) of the application server. For BSM, enter the name (or IP) of the BSM Gateway server.
Enter the Data Flow Probe address (this machine by default).

Application to report to:

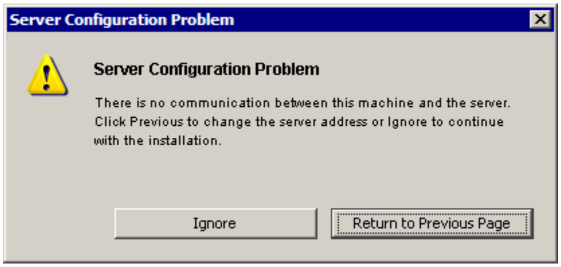
● HP Universal CMDB ○ HP BSM

Application Server address:

Data Flow Probe address: JMICHAELI05

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

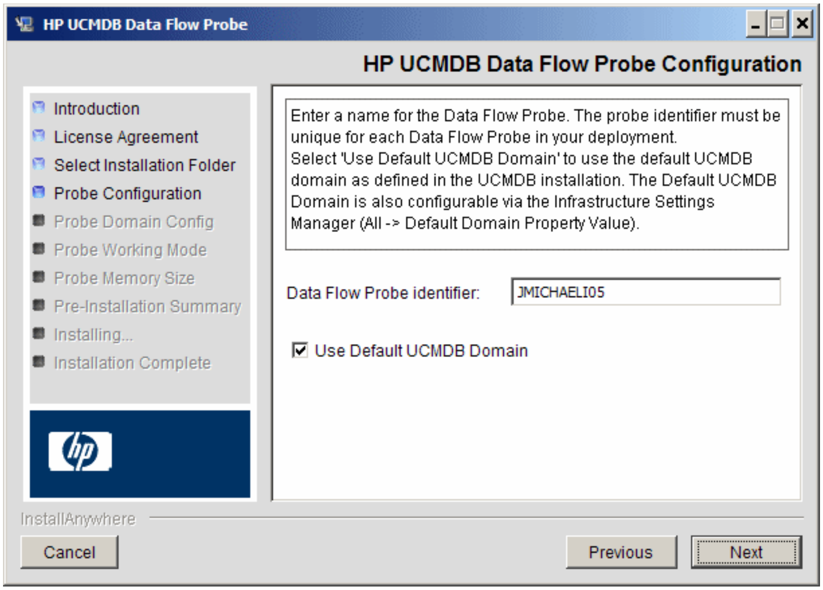
8 If you do not enter the address of the application server, a message is displayed. You can choose to continue to install the Probe without entering the address, or to return to the previous page and add the address.



Server Configuration Problem

There is no communication between this machine and the server. Click Previous to change the server address or Ignore to continue with the installation.

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



HP UCMDB Data Flow Probe Configuration

Enter a name for the Data Flow Probe. The probe identifier must be unique for each Data Flow Probe in your deployment.
Select 'Use Default UCMDB Domain' to use the default UCMDB domain as defined in the UCMDB installation. The Default UCMDB Domain is also configurable via the Infrastructure Settings Manager (All -> Default Domain Property Value).

Data Flow Probe identifier: JMICHAELI05

☑ Use Default UCMDB Domain

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

Important:

- The UCMDB Probe identifier 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 to the Probe Gateway and all its Managers. This name appears in UCMDB as a single Probe node.

- 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 the Infrastructure Settings Manager, available after installing HP Universal CMDB (**CMDB Class Model Settings** > **Default Domain Property Value**).

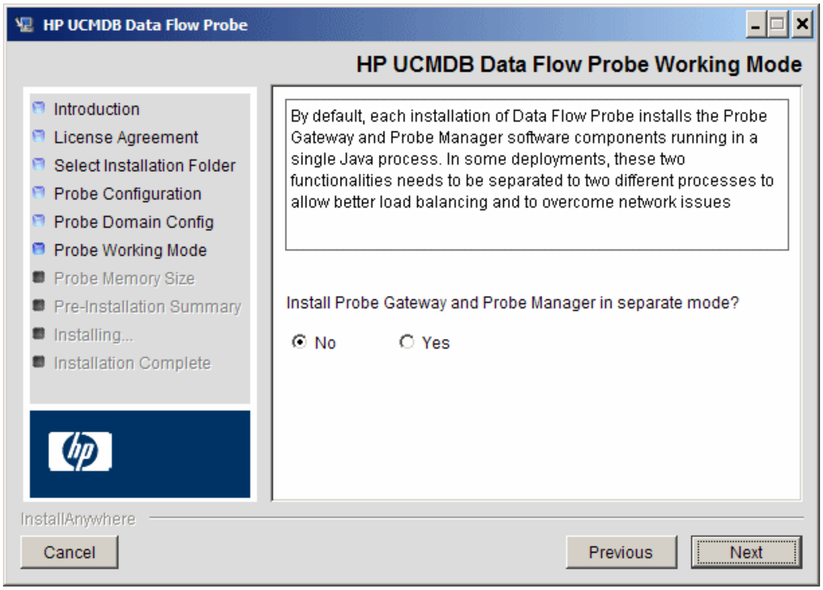
10 Click **Next.** If you cleared the **Use Default CMDB Domain** box in the HP UCMDB Data Flow Probe Configuration dialog box, the HP UCMDB Data Flow Probe Configuration Domain Configuration dialog box appears.

- **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.



By default, each installation of Data Flow Probe installs the Probe Gateway and Probe Manager software components running in a single Java process. In some deployments, these two functionalities needs to be separated to two different processes to allow better load balancing and to overcome network issues

Install Probe Gateway and Probe Manager in separate mode?

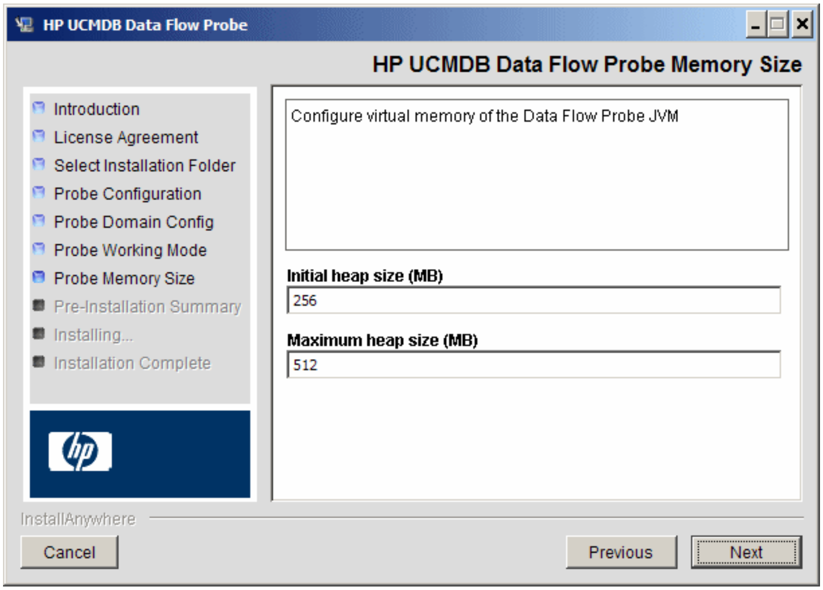
● No ○ Yes

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 113.

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



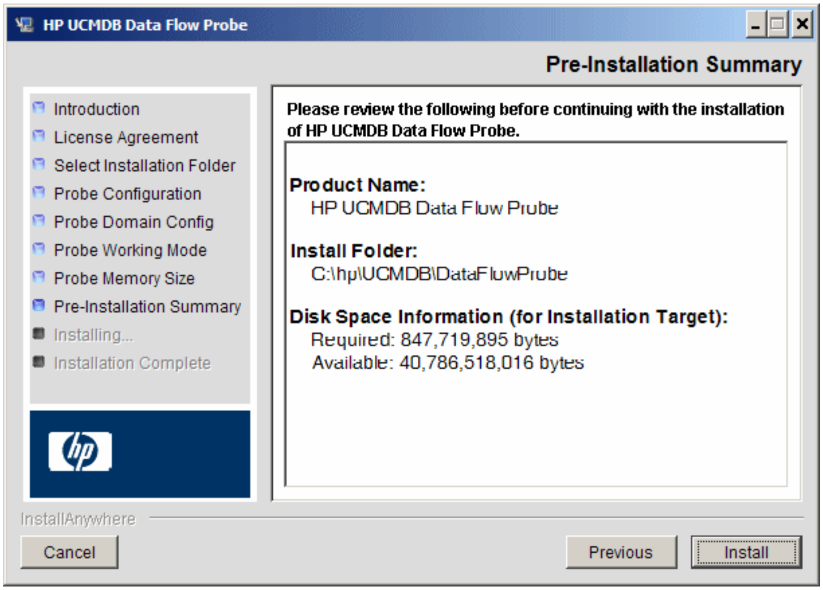
Configure virtual memory of the Data Flow Probe JVM

Initial heap size (MB): 256

Maximum heap size (MB): 512

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

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



Please review the following before continuing with the installation of HP UCMDB Data Flow Probe.

Product Name:
HP UCMDB Data Flow Probe

Install Folder:
C:\hp\UCMDB\DataFlowProbe

Disk Space Information (for Installation Target):
Required: 847,719,895 bytes
Available: 40,786,518,016 bytes

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: **<UCMDB Installation Directory>\DataFlowProbe \HP_UCMDB_Data_Flow_Probe_InstallLog.log.**

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

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 *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 116.

Upgrade the Probe

This task describes how to upgrade the Data Flow Probe.

1 Uninstall the Old Probe

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

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.

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 UCMDB Data Flow Probe” on page 103.

   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 to the Probe Gateway and all its Managers. You name the Probe during installation in the **Data Flow Probe Identifier** box in the **HP UCMDB Data Flow Probe Configuration** dialog box. For details, see step 9 on page 108.

   This name appears in UCMDB as a single Probe node. Failure to give the same name may prevent jobs from running.

2. Choose **Yes** in step 11 on page 110.
3. Perform the configuration in “Configure the Probe Manager and Probe Gateway Components” on page 114.

Configure the Probe Manager and Probe Gateway Components

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

This section includes the following topics:

- "Set Up the Probe Gateway Machine" on page 114
- "Set Up the Probe Manager Machine" on page 114
- "Start the Services" on page 115

1 Set Up the Probe Gateway Machine

Open the following file:

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

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

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

b Open the following file:
C:\hp\UCMDB\DataFlowProbe\conf\DiscoveryProbe.properties

c 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: **Start** > **Programs** > **UCMBDB** > **Start Data Flow Probe Manager.**

b On the Probe Gateway machine start the Gateway: **Start** > **Programs** > **UCMBDB** > **Start Data Flow Probe Gateway**.

Data Flow Probe Installation Requirements

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

Platform	**OS Version and Edition**	**Supported**	**Recommended**
32-bit x86/x64	Windows 2008 Standard/Enterprise editions, SP2 and R2	**Yes**	**Yes**
32-bit x86/x64	Windows 2003 Standard/Enterprise editions SP2 and R2 SP2	**Yes**	
Any	Windows 7 Professional/Enterprise	**No**	
Any	Windows 2000	**No**	

Virtual Environments

Virtual Environment	**Guest OS Version and Edition**	**Supported**	**Recommended**

VMware ESX 3.x	Windows 2003 Standard/Enterprise editions SP2 and R2 SP2 Windows 2008 Standard/Enterprise SP2 and R2 Windows 7 Professional/Enterprise	**Yes**	
VMware ESX 4.0	Windows 2003 Standard/Enterprise editions SP2 and R2 SP2 Windows 2008 Standard/Enterprise SP2 and R2 Windows 7 Professional/Enterprise	**Yes**	**Yes**
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**	

Part IV

Upgrading HP Universal CMDB from Version 8.0x to 9.0x

11

Upgrading HP Universal CMDB to Version 9.00

This chapter includes:

Concepts

- Upgrade Prerequisites on page 121
- Upgrade Summary on page 123
- Input Parameters, Class Model, and Log Files on page 123

Tasks

- Uninstall UCMDB 8.0x on page 125
- Upgrade to UCMDB 9.00 on page 125
- Post Upgrade Procedures on page 134

Reference

- Ordered Summary of Upgrade Steps on page 134

Concepts

Upgrade Prerequisites

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

- The UCMDB 9.00 upgrade process upgrades UCMDB from 8.x to 9.00 versions. This is an offline process during which all resources and data is being transformed from 8.x data model to the new BDM (BTO Data Model) version 1.1.
- To upgrade from version 7.x to 9.00, first upgrade to the latest 8.0x version and install the latest content pack. For details refer to the version 8.0x documentation.
- 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."
- Hardware and OS requirements are listed in the UCMDB "HP Universal CMDB Support Matrix" on page 31.
- Allocate enough space to your space table to enable temporary duplication of the CMDB schema.
- Backup the CMDB, history, and foundation databases. In UCMDB 9.00 the Foundations and CMDB schemas are combined. Backup all three schemas individually to ensure the correct binding during the 9.00 upgrade.

Note: As an added precaution, run your current UCMDB version against the backup schemas to make sure they are not corrupted.

- Run the database consistency tool to clean the CMDB schema from the following corrupted data:
  - Links where end objects are missing
  - CIs with missing information in some of the tables along the data model hierarchy

Upgrade Summary

This section lists the steps necessary for the upgrade process:

1. Backup the databases and uninstall prior versions of UCMDB.
2. Delete the entire installation folder.
3. Stop the Data Flow Probe.
4. Reboot the UCMDB Server prior to running the 9.00 installation.
5. Install UCMDB 9.00.
6. Run the upgrade tool.
7. Reboot the UCMDB Server.
8. Reinstall any Reverse Proxy
9. Reinstall LWSSO
10. Reinstall SSL configurations.

Input Parameters, Class Model, and Log Files

This section includes the following topics:

- "Upgrade Input Parameters" on page 123
- "Modifying the Class Model Changes Files" on page 124
- "Log File Overview" on page 124

Upgrade Input Parameters

In addition to your schemas and taking into account your type of upgrade (**Full** or **Resource Only**), the upgrade process uses the following:

- Files describing the class model transformation being performed during the upgrade. These are all the files with **_changes.xml** under the **conf/upgrade** directory.
- The out of the box class model of **8.04+CP6**. This version enables the upgrade process to add missing class model entities before the upgrade.

- Out of the box data model of **9.0+CP6**. This version enables the upgrade process to add missing class model entities post upgrade and makes sure the upgraded class model is CMS and Business Service Management compliant.

Modifying the Class Model Changes Files

Class model changes files should not be modified after the completion of the **Validate Class Model** step. This refers to the out-of-the-box files, the automatic conflict resolution (see "Validate Class Model" on page 142) file and any file manually placed under **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.

Log File Overview

During the upgrade the following logs files are used:

- **upgrade.detailed.log** – This is the main log file for the upgrade. 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.
- **upgrade.short.log** – A summary of the detailed log. All lines in this file appear in the **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 class 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 previous class model, class model upgrade, validation with target class model). Typically the combined size of these file logs (.log file and all roll-over files) can reach to 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 the upgrade success.

- **mam.packaging.log** – This log is relevant only for the "Redeploy Basic Packages" on page 185, this file includes all of that step information.

Tasks

Uninstall UCMDB 8.0x

This section is necessary if you intend to install your UCMDB version 9.00 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 9.00 and you can skip to the next step "Upgrade to UCMDB 9.00" on page 125.

To remove the UCMDB 8.0x server:

1 Click the **Start** > **Programs** > **HP UCMDB** > **Stop HP Universal Server.** A console window appears to let you know that the server has now been stopped.

2 Click the **Start** > **Programs** > **HP UCMDB** > **Uninstall HP Universal Server.**

3 Remove the entire **..\hp\UCMDB** folder. For details, see "Uninstall UCMDB" on page 71.

Upgrade to UCMDB 9.00

The upgrade process consists of installing UCMDB 9.00 and then upgrading the data.

1 Stop all Data Flow Probes. The upgrade process uninstalls the old Probes and installs the new Probes.

2 Install UCMDB 9.00 but do not set up the database or schema.

For the procedure for installing UCMDB 9.00, see "Install UCMDB" on page 61.

Caution: Following completion of the installation, do not continue with the UCMDB Server Configuration Wizard (to set up the database or schema). Click **No** and complete the installation. Instead, perform the following step.

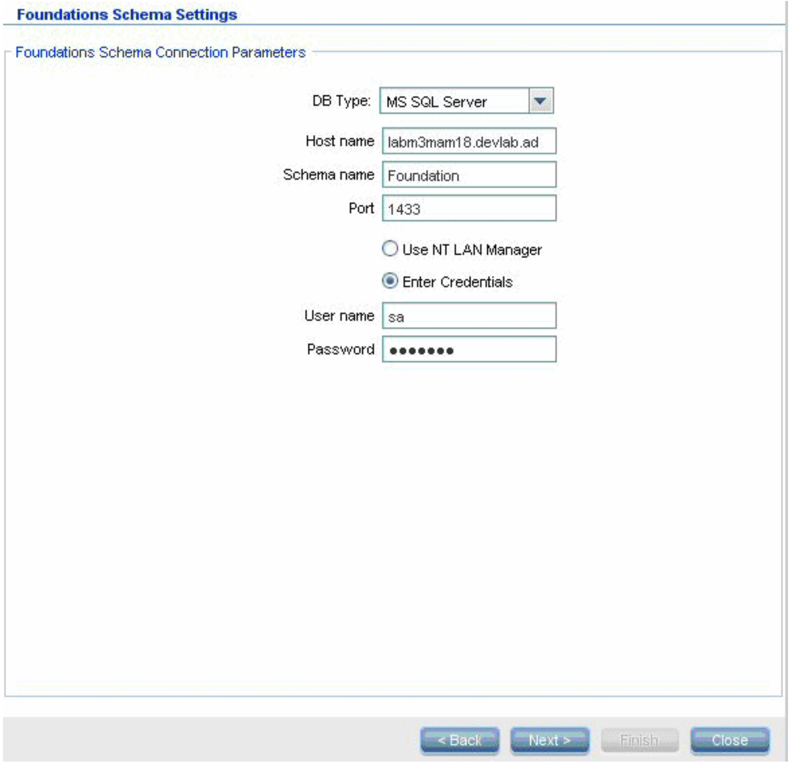
---

3 Locate then launch the **upgrade.bat** file:
C:\hp\UCMDB\UCMDBServer\tools\upgrade.bat

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

5 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 87.



Foundations Schema Settings

Foundations Schema Connection Parameters

DB Type: MS SQL Server

Host name: labm3mam18.devlab.ad

Schema name: Foundation

Port: 1433

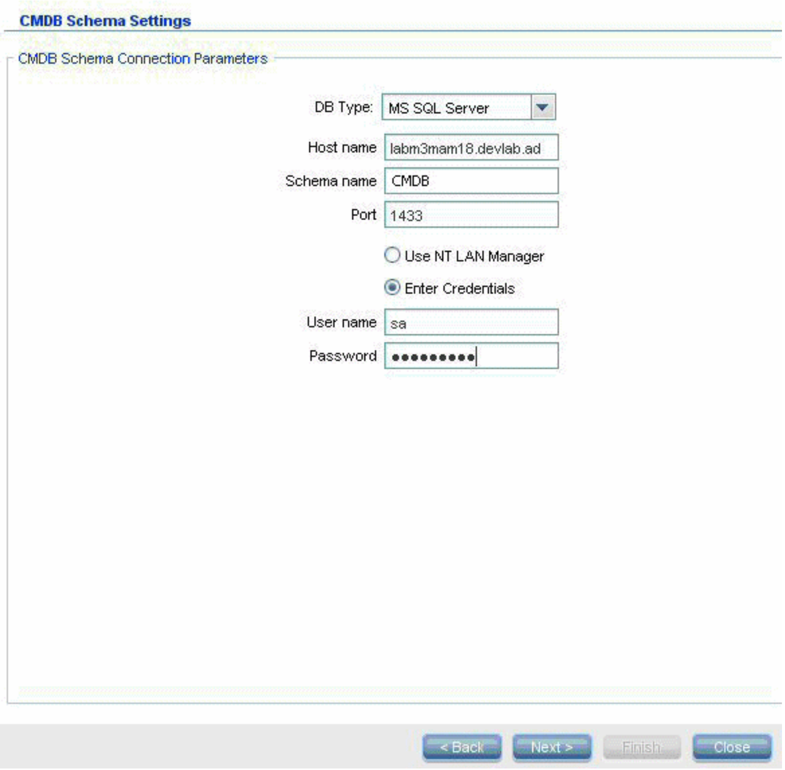
○ Use NT LAN Manager

● Enter Credentials

User name: sa

Password: •••••••

6 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.



CMDB Schema Settings

CMDB Schema Connection Parameters

DB Type: MS SQL Server

Host name labm3mam18.devlab.ad

Schema name CMDB

Port 1433

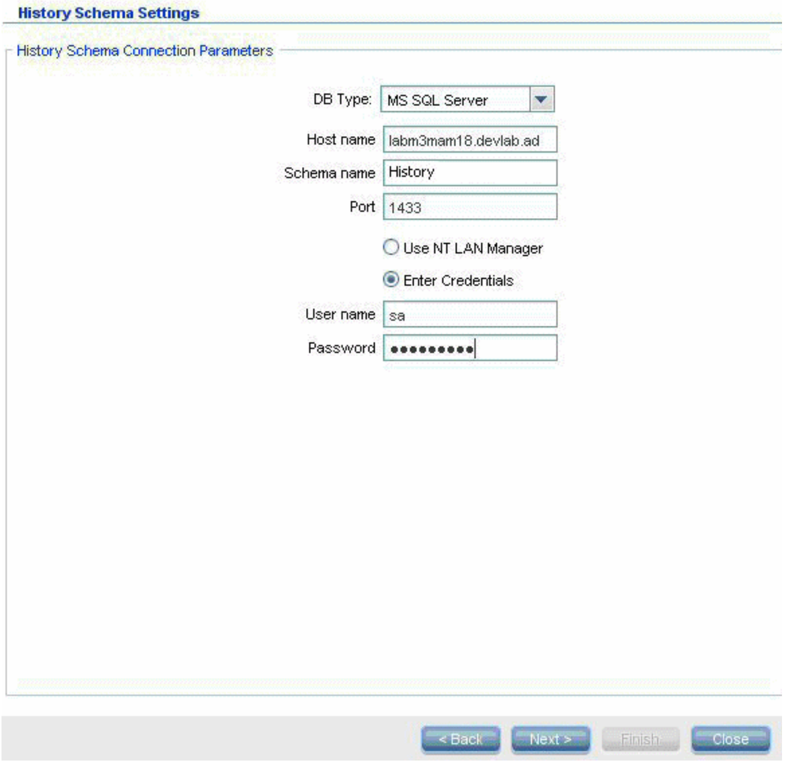
○ Use NT LAN Manager

● Enter Credentials

User name sa

Password ●●●●●●●●●●

7 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

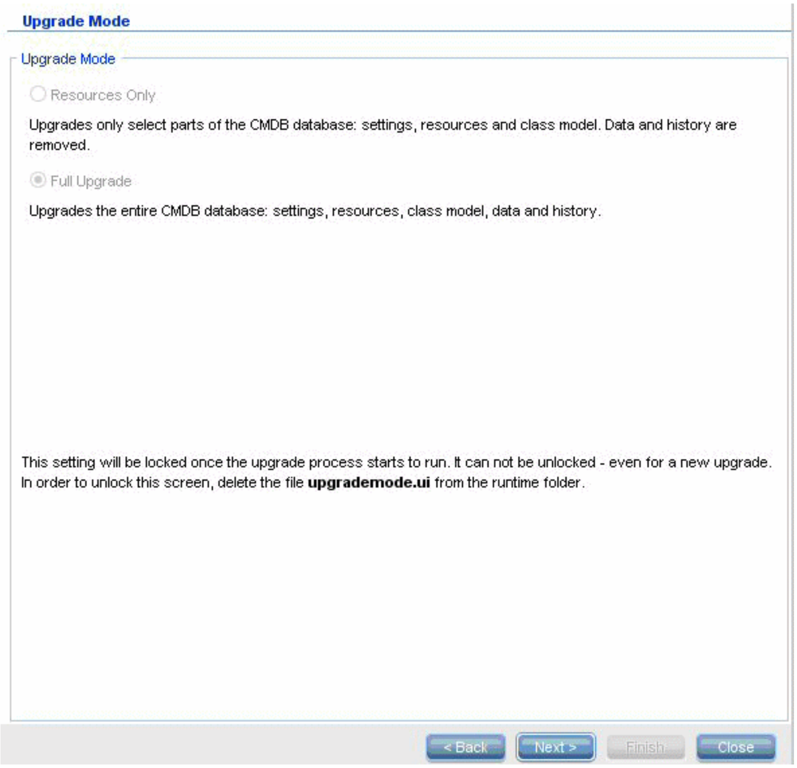
User name: sa

Password: •••••••••

8 Click **Next** and select the Upgrade Mode:

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

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



Upgrade Mode

Upgrade Mode

○ Resources Only

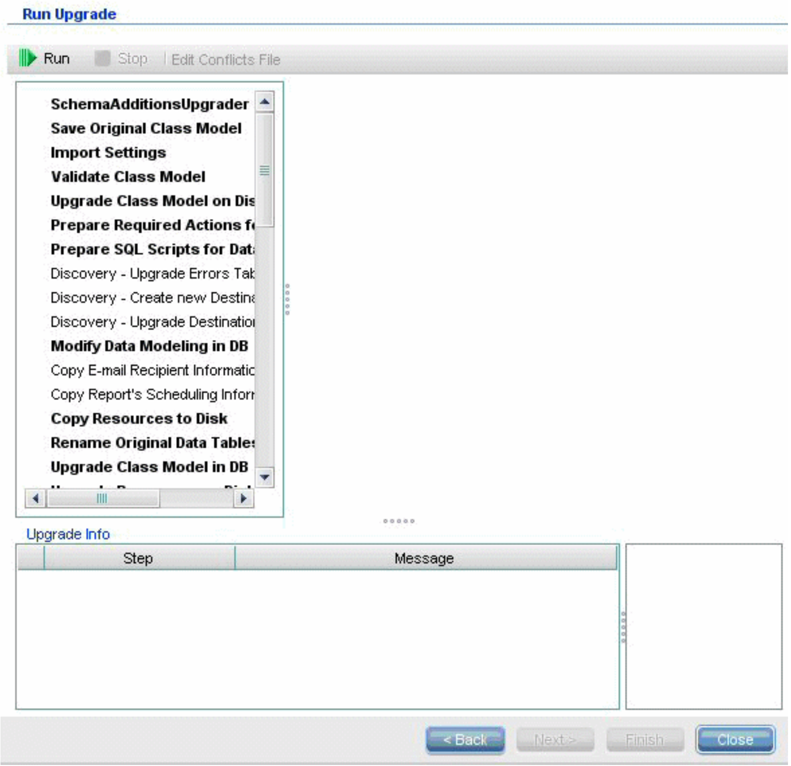
Upgrades only select parts of the CMDB database: settings, resources and class model. Data and history are removed.

● 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.

9 The Run Upgrade screen lists the upgrade steps. To select specific upgrade steps, highlight them, and select **Run Selected**. The selected steps appear in bold. Click **Run** to begin the Upgrade.



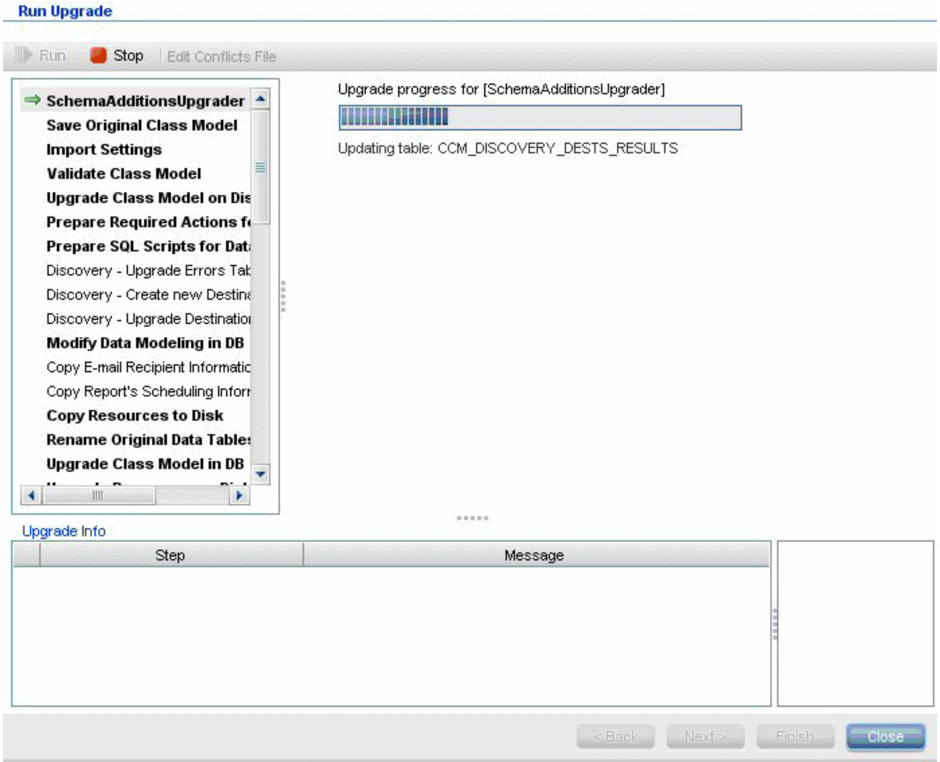
Run Upgrade

- **SchemaAdditionsUpgrader**
- **Save Original Class Model**
- **Import Settings**
- **Validate Class Model**
- **Upgrade Class Model on Dis**
- **Prepare Required Actions fo**
- **Prepare SQL Scripts for Dat**
- Discovery - Upgrade Errors Tab
- Discovery - Create new Destina
- Discovery - Upgrade Destinatio
- **Modify Data Modeling in DB**
- Copy E-mail Recipient Informatic
- Copy Report's Scheduling Inforr
- **Copy Resources to Disk**
- **Rename Original Data Tables**
- **Upgrade Class Model in DB**

Upgrade Info

	Step	Message

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

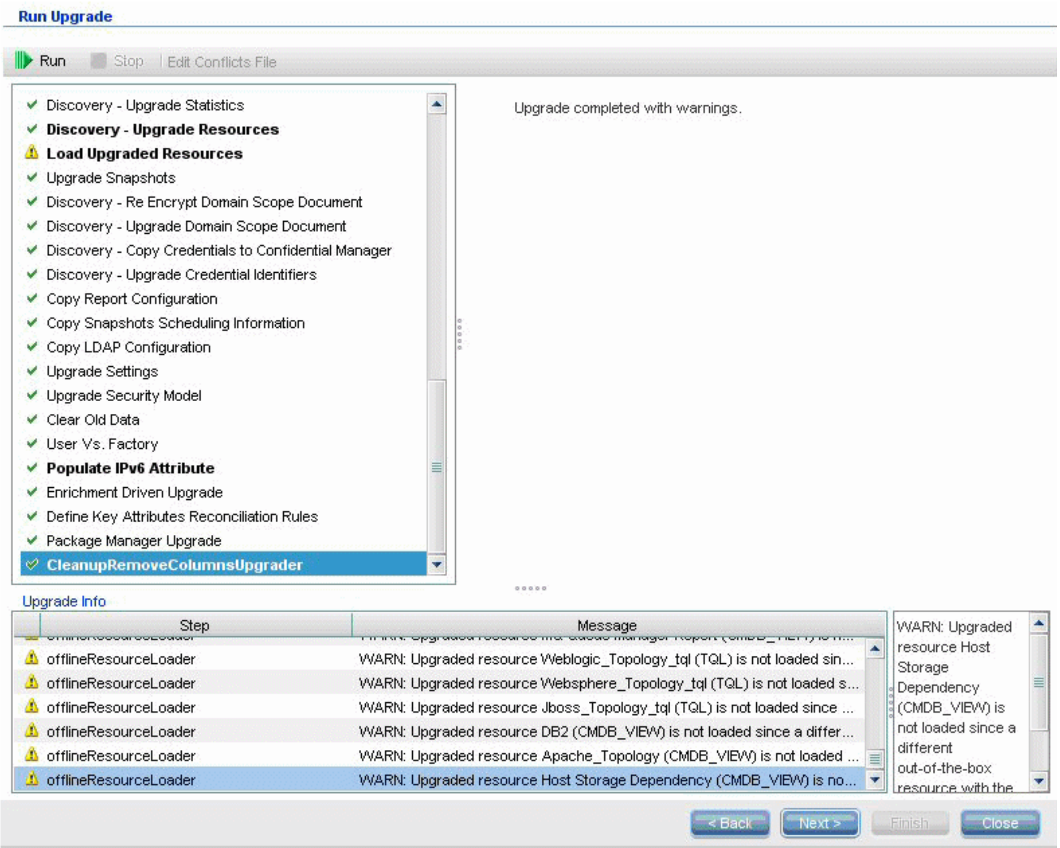


- SchemaAdditionsUpgrader
- Save Original Class Model
- Import Settings
- Validate Class Model
- Upgrade Class Model on Dis
- Prepare Required Actions fo
- Prepare SQL Scripts for Dat
- Discovery - Upgrade Errors Tab
- Discovery - Create new Destin
- Discovery - Upgrade Destinatio
- Modify Data Modeling in DB
- Copy E-mail Recipient Informatio
- Copy Report's Scheduling Infor
- Copy Resources to Disk
- Rename Original Data Tables
- Upgrade Class Model in DB

Upgrade progress for [SchemaAdditionsUpgrader]

Updating table: CCM_DISCOVERY_DESTS_RESULTS

11 The Upgrade can 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 see this information, highlight the row where the **upgrade step** appears: relevant information appears to the right.



- ✓ Discovery - Upgrade Statistics
- ✓ **Discovery - Upgrade Resources**
- ⚠ **Load Upgraded Resources**
- ✓ Upgrade Snapshots
- ✓ Discovery - Re Encrypt Domain Scope Document
- ✓ Discovery - Upgrade Domain Scope Document
- ✓ Discovery - Copy Credentials to Confidential Manager
- ✓ Discovery - Upgrade Credential Identifiers
- ✓ Copy Report Configuration
- ✓ Copy Snapshots Scheduling Information
- ✓ Copy LDAP Configuration
- ✓ Upgrade Settings
- ✓ Upgrade Security Model
- ✓ Clear Old Data
- ✓ User Vs. Factory
- ✓ **Populate IPv6 Attribute**
- ✓ Enrichment Driven Upgrade
- ✓ Define Key Attributes Reconciliation Rules
- ✓ Package Manager Upgrade
- ✓ **CleanupRemoveColumnsUpgrader**

Upgrade completed with warnings.

Upgrade Info

	Step	Message
⚠	offlineResourceLoader	WARN: Upgraded resource Weblogic_Topology_tql (TQL) is not loaded sin...
⚠	offlineResourceLoader	WARN: Upgraded resource Websphere_Topology_tql (TQL) is not loaded s...
⚠	offlineResourceLoader	WARN: Upgraded resource Jboss_Topology_tql (TQL) is not loaded since ...
⚠	offlineResourceLoader	WARN: Upgraded resource DB2 (CMDB_VIEW) is not loaded since a differ...
⚠	offlineResourceLoader	WARN: Upgraded resource Apache_Topology (CMDB_VIEW) is not loaded ...
⚠	offlineResourceLoader	WARN: Upgraded resource Host Storage Dependency (CMDB_VIEW) is no...

WARN: Upgraded resource Host Storage Dependency (CMDB_VIEW) is not loaded since a different out-of-the-box resource with the

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, after the upgrade, reconfigure the reverse proxy. For configuration details, see "Using a Reverse Proxy" on page 245.

SSL

After upgrade SSL should be reconfigured. For configuration details, see "Enabling Secure Sockets Layer (SSL) Communication" on page 237.

JMX Console

The default administrator's user and password have been changed to **sysadmin**.

Delete Foundation Schema

The Foundation schema is no longer used after the upgrade and can be deleted.

Ordered Summary of Upgrade Steps

The upgrade process is a multi-step process comprising an ordered list of steps. Each step performs a specific task. This section describes the steps that comprise the complete upgrade process and includes the following subjects:

- "Description of Upgrade Steps" on page 135
- "Links to Upgrade Steps" on page 135

Description of Upgrade Steps

For each step in the upgrade procedure, the following is described:

- The function 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 which 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 issue(s)?
- Relevant log information – 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 logs: **\runtime\log\upgrade.detailed.log** (possibly duplicated to **\runtime\log\upgrade.short.log**). For log information see "Log File Overview" on page 124.

Links to Upgrade Steps

The following links list the upgrade steps (and relevant sub-steps) in order. To re-run a specific step right-click on the step from the Upgrade Wizard in the **Steps** pane and select **Re-run**.

1. "Schema Additions" on page 139
2. "Save Original Class Model" on page 140
3. "Import Settings" on page 140
   - "To override the aging mechanism" on page 141

- ➤ "To restart the aging mechanism" on page 141

4 "Validate Class Model" on page 142

5 "Upgrade Class Model on Disk" on page 146

6 "Prepare Required Actions for Data Upgrade" on page 148

- ➤ "Initial analysis" on page 149
- ➤ "General information" on page 149
- ➤ "Class rules types" on page 149
- ➤ "Attribute rule types" on page 149
- ➤ "General class or rule analysis" on page 150
- ➤ "Copy condition analysis" on page 151
- ➤ "General attribute analysis" on page 152
- ➤ "Copy attribute from class analysis" on page 152
- ➤ "Copy attribute from attribute analysis" on page 153
- ➤ "Mapped transformation inside copy attribute" on page 153
- ➤ "Added attribute (new or not renamed) analysis" on page 153
- ➤ "Modified attribute (renamed) analysis" on page 153
- ➤ "Common attribute analysis" on page 154
- ➤ "Types" on page 154
- ➤ "Default values" on page 155
- ➤ "Size limits" on page 155
- ➤ "Miscellaneous" on page 155

7 "Post analysis" on page 156

- ➤ "Rules Flattening" on page 156
- ➤ "Abstract classes elimination stage" on page 158
- ➤ "Trivial rules stage" on page 158

8 "Prepare SQL Scripts for Data Upgrade" on page 159

9 "Discovery – Upgrade Errors Table" on page 160

10. "Discovery – Create New Destination IPs Table" on page 161
11. "Discovery – Upgrade Destinations Table" on page 162
12. "Modify Data Modeling in DB" on page 163
13. "Copy E-mail Recipient Information" on page 163
14. "Copy Report's Scheduling Information" on page 164
15. "Copy Resources to Disk" on page 165
16. "Rename Original Data Tables" on page 167
17. "Upgrade Class Model in DB" on page 167
18. "Upgrade Resources on Disk" on page 168
    - "General Log Messages" on page 169
    - "Pattern Upgrade" on page 169
    - "Single Pattern Reference" on page 170
    - "Enrichment Upgrade" on page 171
    - "Gold Master Report Upgrade" on page 171
    - "View Upgrade" on page 172
    - "Report Upgrade" on page 173
19. "Upgrade Data" on page 173
20. "Create Temporary Removed CIs Table" on page 174
21. "Populate Root Table" on page 174
22. "Upgrade List Attribute Table" on page 175
23. "Delete Legacy Configuration Tables" on page 175
24. "Upgrade History DB" on page 176
25. "Handle non Consistent Data" on page 180
26. "Recalculate Non-Random Generated IDs" on page 181
27. "Populate Global ID" on page 182
28. "Discovery – Upgrade Configuration" on page 183
29. "Federation – Remove old Configuration" on page 184

30 "Redeploy Basic Packages" on page 185

31 "Validate Upgraded Class Model" on page 186

32 "Discovery – Upgrade Statistics" on page 186

33 "Discovery – Upgrade Resources" on page 187

34 "Load Upgraded Resources" on page 188

35 "Upgrade Snapshots" on page 190

36 "Discovery – Re-Encrypt Domain Scope Document" on page 190

37 "Discovery – Upgrade Domain Scope Document" on page 192

38 "Copy Credentials to Confidential Manager" on page 192

39 "Discovery - Upgrade Credential Identifiers" on page 193

40 "Copy Report Configuration" on page 194

41 "Copy Snapshots Scheduling Information" on page 194

42 "Copy LDAP Configuration" on page 195

43 "Upgrade Settings" on page 195

44 "Upgrade Security Model" on page 196

45 "Clear Old Data" on page 197

46 "User vs. Factory" on page 197

47 "Populate IPv6 Attribute" on page 199

48 "Enrichment Driven Upgrade" on page 200

49 "Define Key Attributes Reconciliation Rules" on page 200

50 "Package Manager Upgrade" on page 201

51 "Resource Only Upgrade – the Different Steps" on page 202

52 "Truncate Data Tables" on page 204

Schema Additions

Functionality

This step adds the new required tables and columns to the CMDB.

Is Critical

Yes

Can be re-run

Yes

Implication of Failure

The complete success of this step is critical for the CMDB to function correctly.

Functionality

Saves the complete class model, prior to the upgrade, to disk under **/runtime/original-class-model.xml**.

Is Critical

Yes

Can be re-run

Yes

Implication of Failure

Probable reasons for failure are:

- Permission issues (not enough permission)
- Database connectivity issues (the database cannot be connected)
- Locking (tables cannot be modified)

Relevant Log information

- "Updating table: ..." – When updating a specific table in the database.

- “Initializing default customer registration” – when updating the global “customer” information.

Save Original Class Model

Functionality

Saves the complete class model, prior to the upgrade, to disk under **/runtime/original-class-model.xml**.

Is critical

Yes

Can be re run

Yes

Implication of Failure

Failure in this step means that the existing user class model could not be read from the CMDB. It is likely that the cause is a corrupt class model definition. The only solution for this kind of failure is to manually edit the class model definition in the database before trying to re-run the step.

Another reason for failure may be that the CMDB has no permissions to write to the **\runtime** folder. **Read**/**Write**/**Create** folders permissions are needed for the entire installation folder (although most Writes are done only to the **\runtime** folder).

Relevant Log information

Failures in the **cmdb.classmodel.log** or **error.log** that might indicate which entity in the class model failed to load. For more information see "Log File Overview" on page 124.

Import Settings

Functionality

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

Is critical

Yes

Can be re-run

Yes

Implication of Failure

Failure in this step means that your settings will not be properly migrated and that the CMDB factory default values will be used instead. If the aging mechanism is left on large portions of the CMDB data model might be removed when the CMDB first starts up.

The probable cause of failure in this step is an incorrectly configured (or non-existent) foundations database. The best solution for this is to properly configure the foundations database using the upgrade wizard. If the database has been damaged or a new database is desired, it's possible to create an empty foundations database using the CMDB 8.0x database wizard.

To override the aging mechanism

edit the **\conf\settings.override.properties** and add the line **model.aging.is.aging.enabled=false** and **restart** the **Upgrade Wizard**.

To restart the aging mechanism

When you are ready to return the aging to its previous state, edit the **\conf\settings.override.properties** and remove the line **model.aging.is.aging.enabled=false** and **restart** the **CMDB**.

Relevant Log information

- "Fetch old settings" – when retrieving the settings from the old foundations database.
- "Set new settings" – when writing the settings to the new management database.
- "Aging mechanism has been disabled" – when the aging mechanism has been disabled. It is recommended that the aging mechanism remains disabled until a full massive discovery has been run at least once.

Validate Class Model

Functionality

Ensures your old class model, read from **/runtime/original-class-model.xml** is aligned with the expected out of the box class model so it can be accessible for the class model transformations that are part of the upgrade process. Validate Class Model uses the old 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 your disk under: **/runtime/original-fixed-class-model.xml**.

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

Is critical

Yes

Can be re-run

Yes

Implication of Failure

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 being allocated to a new out-of-the-box class or attribute. If this happens a new additional transformation file is automatically generated and saved to disk under **/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 by choosing different names for example.

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 in order to correctly reload these changes.

Relevant Log information

- Missing entity or unsupported additional entity in the user class model will produce a warning to the log file. The warning contains the type of the entity, name and location in the class model hierarchy, and the action that was 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, an error is produced with the name if 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, and at this point in the upgrade we don't have all the information to decide in the matter.
- "Class removal is not allowed in Class <name>. Class was added": The user class model is missing a factory class, so the class is forced back into the user class model. This can happen as a result of class removal by the user or as a result of failure in CP6 deployment.
- "Class Qualifier addition of type <name> is not allowed. The qualifier was removed in Class <name>": Certain types of class qualifiers are not allowed to be added by the user. If the user added one of them, this message will appear and the class qualifier will be removed from the class.
- "Class Qualifier removal of type <name> is not allowed in Class <name>. The qualifier was added": We expect to find in each factory class certain factory class qualifiers, if those qualifiers are missing, we force them back to the class.

- "Attribute removal is not allowed. Attribute <name> in Class <name>. The Attribute was added": The user class model is missing a factory attribute in a factory class, so the attribute is forced back into the class. This can happen as a result of attribute removal by the user or as a result of failure in CP6 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 created by the user in a factory class. We do not allow the user to add specific types of attribute qualifiers on new attributes. The attribute qualifier was 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>": We do not allow the user to add specific types of attribute qualifiers on factory attributes. The attribute qualifier was 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 the user in a factory class. The user also added override on the new attribute in a sub-class. We do not allow the user to add specific types of attribute qualifiers on new attributes or its overrides. The attribute qualifier was 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>": We do not allow the user to add specific types of attribute qualifiers on factory attributes or its overrides. The attribute qualifier was removed from the attribute override in the user class model.
- "Attribute Qualifier removal <name> is not allowed. Attribute <name> in Class <name>": The user removed attribute qualifier that came with the out of the box class model. We do not allow removing specific type of attribute qualifiers from factory attributes.
- "Attribute Qualifier removal <name> in override is not allowed. Attribute <name> in Class <name>": The user removed attribute qualifier in attribute override that came with the out of the box class model. We do not allow removing specific type of attribute qualifiers from factory attribute override.

- "Valid Link <name> removal is not allowed": Valid link was removed by the user or failed to deploy from CP6. The valid link was forced back into the user class model.
- "Calculated Link <name> removal is not allowed. Class <name>": Calculated link was removed by the user or failed to deploy from CP6. The calculated link was forced back into the user class model.
- "TypeDef <name> removal is not allowed": Factory TypeDef (Enum or List) is missing in the user class model, and it is forced back in. The TypeDef could be missing as a result of removal by the user or as a result of failure in CP6 deployment.
- "Enum entry removal is not allowed. Enum <name> with Enum entry key <key> and Enum entry value <value>": An Enum entry is missing in a TypeDef of type Enum, the entry is forced back into the Enum. The Enum entry could have been deleted by the user or failed to deploy from CP6.
- "List entry removal is not allowed. List <name> with List entry value <value>": A List entry is missing in a TypeDef of type List, the entry is forced back into the List. The List entry could have been deleted by the user or failed to deploy from CP6.
- "Enum entry addition can cause conflicts. Enum <name> with Enum entry key <key> and Enum entry value <value>": User added an entry to a TypeDef of type Enum. At this point in the upgrade we do not have enough information to determine if the added entry will cause the upgrade to the fail.
- "List entry addition can cause conflicts. List <name> with List entry value <value>": User added an entry to a TypeDef of type List. At this point in the upgrade we do not have enough information to determine if the added entry will cause the upgrade to the fail.
- In case of attribute type change, an error is produced with the name if the attribute and its class.
- Hierarchy change also produces a warning, with the name of the class that changed its parent class.
- Problem with the user class model will produce: “User class model is not valid for upgrade"

- Problem with class model transformations will produce: “Upgrade configuration files are not valid”

Upgrade Class Model on Disk

Functionality

Uses the class model generated in the previous step (see "Validate Class Model" on page 142): **/runtime/original-fixed-class-model.xml** together with the predefined transformation files to generate the upgraded class model and saves it to disk under **/runtime/upgraded-class-model.xml.**

Is critical

Yes

Can be re-run

Yes

Implication of Failure

If this step fails it means that the class model cannot currently be upgraded properly. A possible solution is to edit the problematic classes in the 8.0x UCMDB instance and re-run the upgrade. Another possible solution is to edit the class model changes files as described in the "Validate Class Model" on page 142 step. If such editing is done, it is important to **re-run** the **Validate class model** step before continuing with the upgrade.

Relevant Log Information

General messages (all top level class model entities):

- “Adding non-modified <entity type> <entity name>” – the entity was not modified between the user and the target class model and can also appear in the form “Adding un-upgraded…”
- “Adding <entity type> <name>” – An upgraded entity will be added to the target class model.
- “Skipping <entity type> <name> - Dropped in upgrade” – the entity is to be explicitly removed in the upgrade.
- Can also appear in the form “Not adding…”

- "Skipping <entity type> <name> - exists in new basic CM" – The entity exists in the basic class model and it's definition there will be used.
- "Adding new <entity type> <name>" – A new entity, specified to be added during the upgrade, will be added to the target class model.
- "Skipping adding new <entity type> <name> - exists in new basic CM" – A new entity, specified to be added during the upgrade, will not be 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 will be 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 was already added as part of a calculated link. See previous log messages to know what actually occurred with that class.
- "skipping adding new class <name> extends <parent name> which does not exist" – The class will not be added since 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 / link) cannot be found in the target class model.
- "Duplicate CITs found: <names>" – due to an error these CI types have been added twice to the target class model. This error is unrecoverable without editing the upgrade class model changes files and rerunning the "validate" and "class model upgrade" steps again.
- "Adding <old name> -> <new name> to rename map." – the rename map is used to identify old classes names to new classes 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 might indicate a problem in the class model upgrade. This message does not, in itself, stops the upgrade process.

Valid links validation:

- "Start removing invalid links." – Valid links are to be checked and invalid ones (no end 1 / end 2 / link class) will be removed.
- "Link <entity> <name> does not exist in target class model - Removing valid link <name>". – The valid link entity (end 1 / end 2 / 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 might cause some resources (TQLs, Views…) to fail the upgrade.
- "Done removing invalid links." – When this sub-step is complete.

For a user's class with key attributes different than its parent the complete set of key attributes is being restored. Each key attribute which was removed from its out of the box ancestors and was added will produce the following log info message:

- "Added ID qualifier to attribute <attribute name> in class <class name>"

Prepare Required Actions for Data Upgrade

Functionality

Uses the **/runtime/ original-class-model.xml**, the **/runtime/upgraded-class-model.xml** and the class model transformations to deduce the actions required to perform the data transformation. Saves the analysis result to disk under **/runtime/data-upgrade-actions.xml**. This step skips CI types listed in **upgrade/DataModelUpgradeConfig.xml** (**app-infra.jar**) that causes the data upgrade to omit non-upgradable data.

Is critical

Yes

Can be re-run

Yes

Implication of Failure

Failure in this step means that the upgrade could not 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.

Relevant Log information

Initial analysis

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 transformation 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 rules 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 on an existing attribute that is being renamed.
- **Removed** – The rule defines that this attribute should not exist in the target DI.
- Default rule / Default action: defined on a specific CIT. This means that 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 in the source CIT level. Attributes from 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. As such, no DIs can exist for it. It is added to a reference list "added CITs" in the xml.
- "Class <name> added to removed CITs." – The CIT is marked to be removed along with all of its DIs.
- "Change has empty class name." – Warning that the requested transformation is invalid and no action will be taken. Cause: invalid transformation definition.
- "Target CIT name is <name>", "Source CIT name is <name> (from <origin>)" – DIs of the source CIT will be copied to the target CIT.
- "Target CIT <name> does not exist in target class model, skipping rule!." – 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 bad class model upgrade.
- "Source CIT <name> does not exist in source class model, skipping rule!." - 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, bad class model upgrade or the user class model (after fixes) not conforming to the 8.0x class model.

- "Source CIT <name> does not exist in source class model, skipping rule, adding to added CITs!." – Warning that the rules do not match the actual class model. The source CIT cannot be found, so the target CIT is to handled as if it's a new CIT (no data upgrade). Cause: invalid transformation definition, bad class model upgrade or the user class model (after fixes) not conforming to the 8.0x class model.
- "Source CIT is empty." / "Target CIT is empty." – Warning that the transformation rule is invalid. The rule will be 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 on which DIs should be copied, but that source CIT does not exist in the user class model. Warns that the condition will be ignored. Cause: invalid transformation definition or the user class model (after fixes) not conforming 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 on which DIs should be copied, but that attribute in the source CIT does not exist in the user class model. Warns that the copy instruction will be ignored. Cause: invalid transformation definition or the user class model (after fixes) not conforming to the 8.0x class model.
- "Copy condition attribute: <name>, Type: <type>, Operator: <operator>." / "Copy condition value: <value>."– The condition that A DI would be copied (not discarded) using this rule is that the value of the attribute maintains the indicated condition (e.g. "ipport not-equal to 3").
- "Attribute condition.attribute name is empty." – The attribute name is empty. Warns that the copy condition is invalid and will not be used (all DIs would be copied). Cause: invalid transformation definition.
- "Copy condition value is empty." – The copy condition value is empty. Warns that the copy condition is invalid and will not be used (all DIs would be copied). Cause: invalid transformation definition.

General attribute analysis

- "Entering copy attribute analysis" – Analysis for attributes is about to start.
- "Rule type for attribute <old name> -> <new name> is <rule type>." - Analysis for this rule is about to start. Note: type "MERGED" and "MOVED" are not applicable for attribute rules.
- "Rule type changed from <original type> to ADDED - no old name or oldName == Name." – While 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 (difference between the user class model and the expected 8.0x class model).
- "No target class <name> in new class model." – Warns that the target class cannot be found in the target class model and this attribute rule will be skipped. Cause: bad class model upgrade.
- "No target attribute <name> in target class <class name> in new class model." – Warns that the target attribute in the target class cannot be found in the target class model and this attribute rule will be skipped. Cause: bad class model upgrade.
- "Attribute <name> in class <class name> in new class model is declared STATIC_ATTRIBUTE. Skipping rule." – Static attributes live on the CIT, not 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 is 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 specified one.

Copy attribute from attribute analysis

- “Copy attribute from attribute” – This attribute value is determined by another attribute.
- “Old attribute name: <name>.” – Applicable to “added” attribute - the source attribute is the indicated one.
- “Source attribute name (from enum): <name>.” / “Source attribute name (from OldName): <name>.” – Applicable to “modified” attribute – the source for this rule either is constant (“from enum”) or another attribute (“from OldName”).

Mapped transformation inside copy attribute

- “Entering map transformation analysis.” – The source should be transformed using a source -> target map (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, this transformation will 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 will not be 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 will not be used. Cause: invalid transformation definition.

Common attribute analysis

- "Completing and adding." – Entering the common analysis stage for this attribute rule.
- "Attribute was not properly completed." – The common analysis stage failed, the attribute rule will not be used. This must be preceded by one of the following:
- "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 bad 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 bad class model upgrade.
- "Cannot determine target type <name>." – The target attribute type is invalid. Cause: bad class model upgrade.
- "Source CIT name is empty." – the source CIT is empty. Cause: invalid rule, bad class model upgrade or previous error in data actions analysis.
- "Source attribute name is empty." / "Source attribute is null."– the source CIT is empty. Cause: invalid rule, bad class model upgrade or previous error in data actions 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 specified one.
- "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 will be used if the original DI property was empty.
- "Source default value is <value>." – If the DI original property was equal to the old default value, it will be transformed to 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 chars).
- "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 was specified.

Miscellaneous

- "Attribute did not pass validation. " – final validation failed, the attribute rule will not be used. Actual cause 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 remained 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) remained 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 some other rule.
- “Value transformation source is empty.” / “Value transformation target is empty.” – the value map transformation is invalid.

Relevant Log information

Post analysis

Rules Flattening

The rules defined in the class model changes have been converted to actions. This stage will now copy rules from parent classes to children classes to create a complete non-trivial rule-set disconnected from the class hierarchy

- “Flatten rules stage” – stage starts.
- “Building class to direct children map.” – starting to build a complete class to children dictionary.
- “Class <child name> is a child of <parent name>.”
- “Class appeared twice.” – warns that a class was found twice. Most likely that 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 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.” – warns that the rule cannot be added to the map because another instance of it already exists under a different target/source class. The rule will be ignored for children 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 will handle 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 will be used to copy 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 will be checked from the bottom (the specified CIT) up (to root) in order to collect the correct set of rules. The bottom-most rule that generate a value for a target attribute is the one used.
- "Visiting source class <name>." – the specified source class is to be checked.
- "Found rule from source class <source> to <target>." – about 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>." – about to start 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 doesn't have any value generator rule.
- "Rule is not in ignore list - adding to target attribute rules." – the specified rule will be used to generate values for the target attribute.
- "Attribute did not pass validation." – attribute rule did not pass validation. See previous section about possible validation messages and causes.
- "Rule is in ignore list - not added." – attribute was marked as "do not copy", so it can't be used.
- "Going over ignore list: <attributes>." – If an attribute was removed, it will appear 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 on 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's constrained by the 'current' copy condition.

Abstract classes elimination stage

Abstract CITs do not have DIs (or tables under the new DB model). Rules that have been created for these CITs (flattening process, errors, mismatch between user 8.0x class model and expected) will now be deleted:

- "Remove abstract classes stage" – stage starts.
- "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 are 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 will be 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’s not duplicated to 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’s 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 exists) will be used as a source for the default rule. If the second message does not appear, then no rule will be used and the attribute value will remain 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

Functionality

Analyzes the **/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 **/runtime/data-upgrade-script.sql**.

Is critical

Yes

Can be re-run

Yes

Implication 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.

Relevant Log information

- "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 this 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 will not take place and all CIs of the source CIT type would be 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

Functionality

Upgrades discovery errors data (stored in **CCM_DISCOVERY_ERRORS** table in the CMDB) **-** replaces error messages by error codes with parameters (discovery runtime information).

Is critical

No

Can be re-run

Yes

Implication of Failure

Information regarding discovery errors will be lost. Skipping this step will require you to truncate the **CCM_DISCOVERY_ ERRORS** table in the CMDB and re-activate all discovery jobs after the server is back up.

Relevant Log Information

- "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

Functionality

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

No

Can be re-run

Yes

Implication of Failure

Information regarding discovery destinations will be 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.

Relevant Log Information

- "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

Functionality

Renames CI types in **CCM_DISCOVERY_DESTS** table in the CMDB (discovery runtime information).

Is critical

No

Can be re-run

Yes

Implication of Failure

Information regarding discovery destinations will be 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.

Relevant Log Information

- "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. It might 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

Functionality

Modify CMDB structure to the new 9.00 structure.

Is critical

Yes

Can be re-run

No

Implication of Failure

Failure means that the DB 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 and History schemas from backup, delete the **\runtime** folder and run the upgrade tool from the beginning.

Relevant Log information

None

Copy E-mail Recipient Information

Functionality

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

No

Can be re-run

Yes, if class model upgrade hasn't run yet.

Implication of Failure

Scheduled reports are not sent. Users must add recipients through the Recipients Manager or through the upgraded scheduled jobs themselves.

Relevant Log information

- Get an indication of the existing number of recipients: "Number of EmailRecipients in the CMDB is x"
- If the upgrade fails: "Failed to handle Recipient"
- If it succeeds: "RecipientUpgrader is complete"

Copy Report's Scheduling Information

Functionality

Copies scheduled reports configuration from foundation database to new management table in the CMDB.

Is Critical

No

Can be re-run

Yes

Implication of Failure

Your scheduled reports will not be upgraded and you will need to redefine them.

Relevant Log information

- For success: "Upgrade of scheduled report finished successfully"
- For overall failure: "failed to upgrade scheduled reports"

- For failure on specific job: “failed to upgrade scheduled report of job name <job name>”

Copy Resources to Disk

Functionality

Extract queries, views, reports, enrichments and correlations from the database and store them to disk. The Resources are stored under **/runtime/1/<resource type>/<sub folder>/**. Where resource type 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 – gold master 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.

Sub folder 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** directory, 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 put into the **classmode**l subfolder.

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

Yes

Can be re-run

Yes

Implication of Failure

Resources cannot be upgraded, since none exist on the disk for upgrade. Do not try to continue without completing this step.

Relevant Log information

Retrieve resources from DB messages:

- "got <number> < resource-type> from database": Specify how many resources were retrieved from the DB for each type of resource. This message is followed by the list of resource names.
- "did not succees 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 DB 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.

Rename Original Data Tables

Functionality

Rename your old data tables, adding the **TEMP_** prefix to the names of all CDM tables.

Is Critical

Yes

Can be re-run

No

Implication of Failure

The upgrade process should be run again from the beginning after fixing the problem. Restore the DB schemas, delete the “runtime” folder, and start the upgrade from the beginning.

Relevant Log information

None

Upgrade Class Model in DB

Functionality

Truncate class model tables in the CMDB, removing old class model definitions, uses the **/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

Yes

Can be re-run

Yes

Implication of Failure

Failure implies that the new class model was not loaded into the DB. The upgrade cannot continue without the new class model.

Relevant Log information

None

Upgrade Resources on Disk

Functionality

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 won't be loaded to the upgraded UCMDB. Similarly, queries using attributes which are being removed during the upgrade, as a property condition, will also be removed. Aside from the class model transformations applied over these resources, the following changes are being 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

Yes

Can be re-run

Yes

Implication of Failure

Failure in the entire step will result 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.

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 does not exist in UCMDB 9.0. All those resources will be 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 will be removed, the next message will inform 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 "\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 will 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 will specify the parts of the pattern that were upgraded.
- "About to write patterns to disk after structure upgrade (<number-of-patterns>):{<list-of-pattern-names>}.": These patterns can be found under "\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 "\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 "\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 "\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 was upgraded and is located under "\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 "\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 "\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 "\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 "\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 will be "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 "\runtime\upgrade\<customer-id>\cmdbview\classmodel" or "\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 would not be upgraded and will be in one of the folders "\runtime\upgrade\<customer-id>\cmdbview\unupgradeable" or "\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 "\runtime\upgrade\<customer-id>\cmdbview\classmodel".
- "Could not upgrade view <name>".": The views can be found under "\runtime\upgrade\<customer-id>\ cmdbview \ unupgradeable".
- "About to copy unchanged BacViews.": The views can be found under "\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 was not found on the disk for the current report. If the pattern was not moved to version 9.0 (after upgrade or as is) it will be under "\runtime\upgrade\<customer-id>\patterns\ unupgradeable\", and this message will be produced. The report can be found under "\runtime\upgrade\<customer-id>\reports\structure".
- "Report <name> was upgraded to view <name>.": Finished upgrading report. The report can be found under "\runtime\upgrade\<customer-id>\cmdbview\structure". The class model upgrade will be 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 "\runtime\upgrade\<customer-id>\reports\ unupgradeable\".

Upgrade Data

Functionality

Executes SQL statements from **/runtime/data-upgrade-script.sql**, it reads data from the old data tables, 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 the upgrade finishes, this space is released.

Is Critical

Yes

Can be re-run

No

Implication of Failure

Data in DB is not upgraded.

Relevant Log information

None.

Create Temporary Removed CIs Table

Functionality

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

Yes

Can be re-run

Yes

Implication of Failure

Failure means that the “Upgrade List Attribute Table” and “Handle non-Consistent Data” steps cannot be executed.

Relevant Log information

None.

Populate Root Table

Functionality

Copies upgraded relevant attribute values from leaf data tables to the root table (CDM ROOT).

Is Critical

Yes

Can be re-run

No

Implication 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.

Relevant Log information

None.

Upgrade List Attribute Table

Functionality

Upgrade attributes of type list which are stored in a separate table.

Is Critical

Yes

Can be re-run

No

Implication of Failure

All attributes of type **list** will have wrong values.

Relevant Log information

None.

Delete Legacy Configuration Tables

Functionality

Removes tables no longer needed in CMDB.

Is Critical

No

Can be re-run

Yes

Implication of Failure

The tables that are meant to be deleted will stay in the CMDB schema, but would not disrupt the normal behavior of the UCMDB. It is possible to manually remove these tables.

Relevant Log information

None.

Upgrade History DB

Functionality

Upgrade history database. History database may hold huge amount of data, during this step we keep reference to the last upgraded data so in case of failure the upgrade will continue from the point it was stopped.

Is Critical

Yes

Can be re-run

Yes

Implication of Failure

This step can be re-run multiple times and can recover from failure using designated recovery files, located under **runtime/upgrade** folder. Each file contains the status of a sub step; together it holds 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 will result in losing your historical data and will require creating new history schema via the configuration wizard.

Relevant Log Information

General Log Messages

Failure will produce the following message:

- ”History DB upgrader failed, but is not failing upgrade process…”

and the progress reports will produce one of the following messages:

- “INFO - <step name> is upgrading chunk <current chunk number> out of <total number of chunks>”
- "No upgrade is needed. Upgrade was finished in the previous upgrade": This is not the first time the History DB 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 DB.

- "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 DB, 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 DB 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 DB.
- "Summary of all collect data from History DB": The following log messages will contains 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 DB, 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 DB, because its 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": Those classes has attribute that can potentially be merged. The next stage will verify it.
- "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 DB.
- "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 DB.
- "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 DB.
- "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 DB.

"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 DB.

"Executing SQL statement on snapshots between event id <number> and "ExecuteBatch for snapshot is done in seconds"

Handle non Consistent Data

Functionality

Perform the following:

- Remove links whose one of their end objects was removed during the upgrade.

- Perform recursive delete if necessary.

- Recalculate value for attribute defined as calculated-attribute for all objects and links.

Is Critical

No

Can be re-run

Yes

Implication of Failure

The data will be 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.

Relevant Log Information

In the upgrade short log the following information can be found:

- ➤ The number of removed objects and links during the upgrade - “Found x objects/links that were removed during upgrade”.
- ➤ The number of dangling links that are being removed - "Found x dangling links".
- ➤ The number of objects that are being removed due to recursive-delete - "Found x recursive-delete objects”.
- ➤ Row for each type of object/link for attribute-recalculation is being performed - "Updating calculated attributes for type CLASS_NAME (x instances, y bulks)".

Recalculate Non-Random Generated IDs

Functionality

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

Yes

Can be re-run

Yes

Relevant Log information

None

Populate Global ID

Functionality

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

No

Can be re-run

Yes

Implication of Failure

Might cause the CIs not to have a global id. This can be 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’ll 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’ll need to make it a global id generator and then make it a non global id generator.

Relevant Log information

None.

Discovery – Upgrade Configuration

Functionality

Re calculates IDs for discovery configuration CIs.

Is Critical

Yes

Can be re-run

No

Implication of Failure

Discovery might not function at all. Skipping this step will require you to perform the following:

Disable the Three Upgraders

1. Export user packages from old cmdb.
2. Upgrade all packages manually via the packages upgrade tool.
3. Before the upgrade process, remove the following instances of discovery configuration CIs from CMDB:

- ‘domain’.
- ‘discoveryjob’.
- ‘discoverymodule’.
- ‘cmdbclass’.
- ‘discoverypattern’.
- ‘discoverywizard’.
- ‘discoveryprobegateway’.
- ‘discoveryprobemanager’.
- ‘discoveryresource’.
- ‘discoverytql’.
- ‘triggers’.

- ‘management’.

4 After the upgrade process, import the upgraded packages.

Relevant Log Information

- “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

Functionality

Removes old federation configuration data (new configuration is being deployed).

Is Critical

Yes

Can be re-run

Yes

Implication of Failure

Might cause the federation/replication not to work.

Workaround – the **Model Services -> deleteByClassType** JMX can be used to remove all instances of **fcmdb_configuration** CIT.

Relevant Log information

Log messages can be found in the log file **cmdb.model.audit.short.log** and **cmdb.model.audit.detailed.appender**.

Redeploy Basic Packages

Functionality

Deploys the CMDB factory packages. Class model updates in this step are restricted to additions only in order for the factory packages not to remove user-added attributes.

Is Critical

No

Can be re-run

Yes

Implication 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.

Relevant Log information

Log information can be found in the log file mam.packaging.log.

Validate Upgraded Class Model

Functionality

Validates that upgraded class model is BDM and CMS compliant by comparing it with an out class 9.0 class model. Missing class model entities are being added.

The class model existing in the database before this step (upgraded + packages) is written to **/runtime/upgraded-after-packages-class-model.xml**. The updated class model is written to **/runtime/ upgraded-fixed-after-packages-class-model.xml**.

If the class model was changed during this step, it is updated back to the database.

Is Critical

No

Can be re-run

Yes

Implication of Failure

Failure in this stage will 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 Business Service Management and CMS compliant.

Relevant Log information

See relevant Log information for the "Validate Class Model" on page 142 step.

Discovery – Upgrade Statistics

Functionality

Renames CI types in the **CCM_DISCOVERY_STATS** table in the CMDB (discovery history information).

Is Critical

No

Can be re-run

Yes

Implication of Failure

Statistic information of previous discovery executions will be lost. Skipping this step would require the user to truncate **CCM_DISCOVERY_STATS** table in the CMDB.

Relevant Log Information

- "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 will appear in red.

Discovery – Upgrade Resources

Functionality

Upgrades discovery resources – patterns, jobs, and modules (discovery configuration data).

Is Critical

Yes

Can be re-run

Yes

Implication of Failure

Same as the step for "Discovery – Upgrade Configuration" on page 183.

Relevant Log Information

- "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. On most cases such errors will come after another log message with more details.

Load Upgraded Resources

Functionality

Loads the upgraded resources created in the previous step "Discovery – Upgrade Resources" on page 187 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

Yes

Can be re-run

Yes

Implication of Failure

The upgraded resources will not be loaded in to the database. The factory resources are already in the database, as a result of the step "Redeploy Basic Packages" on page 185. Only the user resources will be missing from the database.

Relevant Log information

- "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 has been deployed to the DB, cannot be retrieved. The factory resources cannot take precedence over the user resources, so all the user resources will be loaded into the DB, and will run over 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 will be loaded into the DB.
- "Resource <name> could not be loaded becuase of missing dependencies: <list-of-names>.": The resource cannot be loaded into the DB since other resources that it needs does not exists in the DB. 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 going to lose the changes he/she made.
- "Failed to add <type> <name>": The resource of the specific type was not loaded.

Upgrade Snapshots

Functionality

Upgrade snapshot data is stored in the CMDB.

Is Critical

No

Can be re-run

Yes

Relevant Log information

None.

Discovery – Re-Encrypt Domain Scope Document

Functionality

Re-encrypts the Domain Scope Document from DES encryption (used in 8.0x) to AES encryption.

Is Critical

No

Can be re-run

Yes

Implication of Failure

Discovery might not function at all. Skipping this step will require that you do the following:

1. Export the Domain Scope Document from the old CMDB.
2. After the upgrade process, import the Domain Scope Document. For details, see "Export and Import the domainScopeDocument (DSD) File in Encrypted Format" on page 265.

Relevant Log Information

- "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 Domain Scope Document is empty and therefore this step is redundant and won't do anything.
- "The DSD already encrypted by AES - doing nothing…" – Indicates that Domain Scope document is already encrypted by AES – step is redundant and won't do anything.
- "The DSD is encrypted by 3DES..." – indicates that Domain Scope Document is encrypted by 3DES – therefore it will be re-encrypted by AES.
- "Failed to decrypt DSD by 3DES" – indicates that the encryption process of Domain Scope Document failed – this step failed to re-encrypt Domain Scope Document by AES – need to import Domain Scope Document to the UCMDB system after the upgrade process.
- "Failed to encrypt DSD by AES" – step failed, need to import the Domain Scope Document to the UCMDB system after the upgrade process.
- "Got empty DSD after AES encryption" – step failed, need to import the Domain Scope Document to UCMDB system after the upgrade process.
- "Got empty DSD after 3DES decryption" – step failed, need to import the Domain Scope Document to UCMDB system after the upgrade process.

- "Failed to decrypt the DSD by AES and 3DES" – step failed; need to import the Domain Scope Document to UCMDB system after the upgrade process.

Discovery – Upgrade Domain Scope Document

Functionality

Renames CI types and attributes in the domain scope document.

Is Critical

No

Can be re-run

Yes

Implication of Failure

Same as for the step "Discovery – Re-Encrypt Domain Scope Document" on page 190.

Relevant Log Information

- "Upgrade process of DomainScopeDocument data has been started"
- "DomainScopeDocument data has been successfully upgraded"
- "Failed to upgrade DomainScopeDocument data"

Copy Credentials to Confidential Manager

Functionality

Extracts credentials information out of the domain scope document into the confidential manager . Credentials information in the Domain Scope Document are replaced by Confidential Manager identifiers. For details, see "Confidential Manager" on page 295.

Is Critical

No

Can be re-run

Yes

Implication of Failure

Same as for the step "Discovery – Re-Encrypt Domain Scope Document" on page 190.

Relevant Log Information

- “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

Functionality

Upgrade **credential_id** attribute over the CIs in the CMDB to match the confidential manager identifiers.

Is Critical

No

Can be re-run

Yes

Implication of Failure

Credential attribute of existing CIs contains wrong data. Skipping this step would require you to run massive discovery to reconstruct the data.

Relevant Log Information

- “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

Functionality

Copies reports configuration from foundation to new management database.

Is Critical

No

Can be re-run

Yes

Implication of Failure

Favorite filters from 8.0x will not be upgraded and their scheduling will not be available.

Relevant Log information

"failed to upgrade report: <report name>

Copy Snapshots Scheduling Information

Functionality

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

No

Can be re-run

Yes

Implication of Failure

Scheduled snapshots will not be upgraded and user will have to redefine them.

Relevant Log information

Failed to handle **schedulerJob [<schedulerJob.toString()>]**

Copy LDAP Configuration

Functionality

Copies LDAP configuration from foundation to new management database.

Is Critical

No

Can be re-run

Yes

Implication of Failure

LDAP mapping between LDAP group and uCMDB role will not be upgraded. User will have to redefine it under LDAP Manager.

Relevant Log information

- "LDAPUpgrader failed"

Upgrade Settings

Functionality

Rename CI types in selected settings.

Is Critical

No

Can be re-run

Yes

Implication 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 was defined, you may need to redefine the frontend URL. Reverse proxy settings will not be affected.

Relevant Log information

- "SettingsClassModelUpgrader failed" or a specific one with the prefix "failed to upgrade"

Upgrade Security Model

Functionality

Upgrades permissions according to the new ACL Model.

- Is Critical

No

Can be re-run

Yes

Implication of Failure

Some permissions will be aligned with new ACL model but some will not. Administrator will need to go inside Security Manager and verify that all permissions are as required and if not set accordingly.

Relevant Log information

- "Role [<role name>] failed to get permissions due to the following error:…

Clear Old Data

Functionality

Removes old data tables (“TEMP” tables).

Is Critical

No

Can be re-run

Yes

Implication of Failure

The UCMDB will work 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**.

Relevant Log information

None.

User vs. Factory

Functionality

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

No

Can be re-run

Yes

Implication of Failure

All class model entities will be mark as factory entities. Certain operations on the class model are closed for user over factory entities.

Relevant Log information

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 can suggest a previous problem in the deployment of Content Pack 6.00 or in the upgrade process. The probable steps are:

  - “Validate Class Model”, "Validate Class Model" on page 142
  - “Upgrade Class Model on Disk”, "Upgrade Class Model on Disk" on page 146
  - “Upgrade Class Model in DB”, "Upgrade Class Model in DB" on page 167
  - “Redeploy Basic Packages”, "Redeploy Basic Packages" on page 185
  - “Validate Upgraded Class Model”, "Validate Upgraded Class Model" on page 186.

- "!!! 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

Functionality

Copies the IP value from the "name" attribute to the new "IpAddressValue" attribute in the "IpAddress" class in IPv6 normalized form.

Is Critical

Yes

Can be re-run

Yes

Implication 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).

Relevant Log information

Relevant log messages can be found in the log file **cmdb.reconciliation.log**.

Enrichment Driven Upgrade

Functionality

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

No

Can be re-run

Yes

Define Key Attributes Reconciliation Rules

Functionality

Adds a reconciliation rule of type 'key-attributes' to any user's CI type with key attributes.

Is Critical

No

Can be re-run

Yes

Implication of Failure

A user defined CIT that was identified by key attributes in 8.00 will use its parent reconciliation rule.

The key attribute identification rule can be added later on from a package/reconciliation JMX.

Relevant Log information

None.

Package Manager Upgrade

Functionality

Updates packaging information stored in the UCMDB server model.

The configuration file of the Package Manager Upgrade is stored in **upgrade\PackageManagerUpgrader\config.xml** (**cmdb.jar**). The configuration lists obsolete sub-systems and the sub-systems rename rules.

Package Manager Upgrades performs steps as follows:

1. Unpackage resources of obsolete subsystems
2. Rename old subsystem names to the new ones
3. Update the names of the class model resources used by Package Manager
   - **a** Change class names in class definitions
   - **b** Change class names in the definitions of valid links
   - **c** Change class names in the triplets of the calculate link definitions
4. Unpackage non-existing resources.

Is Critical

No

Can be re-run

Yes

Implication 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.

Relevant Log information

None.

Resource Only Upgrade – the Different Steps

Resource Only upgrade uses only part of the steps mentioned. The steps are:

1. Save Original Class Model,
2. Import Settings, "Import Settings" on page 140
3. Validate Class Model, "Validate Class Model" on page 142
4. Upgrade Class Model on Disk, "Upgrade Class Model on Disk" on page 146
5. Prepare Required Actions for Data Upgrade, "Prepare Required Actions for Data Upgrade" on page 148
6. Prepare SQL Scripts for Data Upgrade, "Prepare SQL Scripts for Data Upgrade" on page 159
7. Modify Data Modeling in DB, "Modify Data Modeling in DB" on page 163
8. Copy E-mail Recipient Information, "Copy E-mail Recipient Information" on page 163
9. Copy Resources to Disk, "Copy Resources to Disk" on page 165
10. Copy Report's Scheduling Information, "Copy Report’s Scheduling Information" on page 164
11. Truncate Data Tables – New step for Resource only upgrade (see details below)
12. Rename Original Data Tables, "Rename Original Data Tables" on page 167
13. Upgrade Class Model in DB, "Upgrade Class Model in DB" on page 167
14. Upgrade Resources on Disk, "Upgrade Resources on Disk" on page 168
15. Upgrade Data, "Upgrade Data" on page 173
16. Populate Root Table, "Populate Root Table" on page 174
17. Upgrade List Attribute Table, "Upgrade List Attribute Table" on page 175
18. Delete Legacy Configuration Tables, "Delete Legacy Configuration Tables" on page 175

19 Recalculate non Random Generated IDs, "Recalculate Non-Random Generated IDs" on page 181

20 Populate Global ID, "Populate Global ID" on page 182

21 Discovery - Upgrade Configuration, "Discovery – Upgrade Configuration" on page 183

22 Redeploy Basic Packages, "Redeploy Basic Packages" on page 185

23 Validate Upgraded Class Model, "Validate Upgraded Class Model" on page 186

24 Discovery - Upgrade Resources, "Discovery – Upgrade Resources" on page 187

25 Load Upgraded Resources, "Load Upgraded Resources" on page 188

26 Discovery - Re Encrypt Domain Scope Document, "Discovery – Re-Encrypt Domain Scope Document" on page 190

27 Discovery - Upgrade Domain Scope Document, "Discovery – Upgrade Domain Scope Document" on page 192

28 Discovery - Copy Credentials to Confidential Manager, "Copy Credentials to Confidential Manager" on page 192

29 Discovery - Upgrade Credential Identifiers, "Discovery - Upgrade Credential Identifiers" on page 193

30 Copy Report Configuration, "Copy Report Configuration" on page 194

31 Copy Snapshots Scheduling Information, "Copy Snapshots Scheduling Information" on page 194

32 Copy LDAP Configuration, "Copy LDAP Configuration" on page 195

33 Upgrade Settings, "Upgrade Settings" on page 195

34 Upgrade Security Model, "Upgrade Security Model" on page 196

35 Clear Old Data, "Clear Old Data" on page 197

36 User Vs. Factory, "User vs. Factory" on page 197

37 Define Key Attributes Reconciliation Rules, "Define Key Attributes Reconciliation Rules" on page 200

38 Package Manager Upgrade, "Package Manager Upgrade" on page 201

Truncate Data Tables

Functionality

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

Yes

Can be re-run

Yes

Implication of Failure

Non-upgraded data will stay in the CMDB and History schemas. Since part of the data would not be upgraded in the next steps, the system behavior after the upgrade will finish is unpredictable .

Relevant Log information

- "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 unrelevant data from root table: <SQL-statement>": The statement that removes all irrelevant data from the root table.

Troubleshooting and Limitations

This section describes troubleshooting and limitations for upgrading from UCMDB 8.0x to UCMDB 9.00.

Validate Data Model Conflict

Validate Data model uses the old Data model, the predefined transformations and the out of the box Data models as input, generates a modified Data model, after the addition of missing Data model entities, to disk under "**\runtime\old-class-model.xml**."

If a conflict is detected, as is the case when a new class or attribute name defined by the user is being allocated to a new out of the box class or attribute, a new additional transformation file is generated and saved to disk under "**\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. Running the upgrade again, will include these new transformations and enable the upgrade to proceed.

Resources Were Not Loaded to the Upgraded UCMDB

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 as a property condition are also removed during the upgrade. Except for the Data model transformations applied over these resources, the following changes are being made:

- Views are redefined to match the new view definition.
- Topology reports are redefined as views. In UCMDB 9.00 reports and views are seen as different visualization of the same data.
- Queries are now saved in a new, more readable XML format.

12

Upgrading Packages from Version 8.04 to 9.00

This chapter includes:

Concepts

- Package Migration Utility – Overview on page 208

Tasks

- Migrate a Custom Package on page 209

Troubleshooting and Limitations on page 211

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 8.04 to version 9.00.

Custom packages created before upgrading the system to version 9.00 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 9.00 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 9.00.

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**

   - Solaris: **C:/hp/UCMDB/UCMDBServer/2f/packupgrade/bin/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 9.00 system.

Troubleshooting and Limitations

- The Package Migration Utility has been verified only for packages compatible with UCMDB 8.04.
- 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

13

HP Universal CMDB High Availability

This chapter includes:

Concepts

- Best Practices for the HP Universal CMDB High Availability Solution on page 215

Tasks

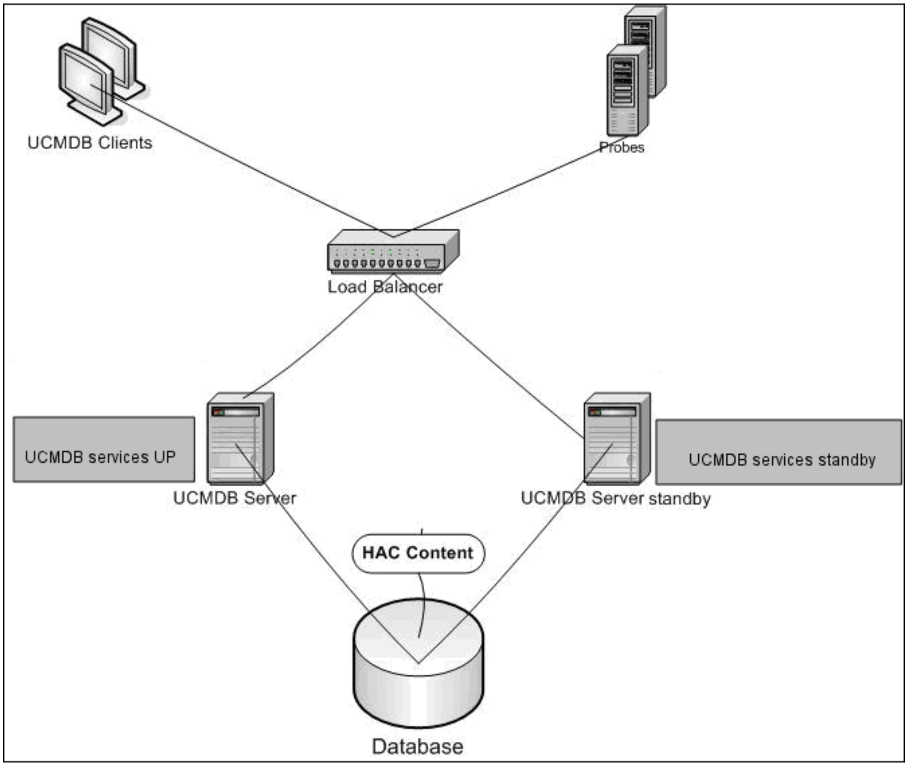
- Install HP Universal CMDB in High Availability Mode on page 217
- Configure Network High Availability on page 220
- Configure Full Site on page 221

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 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 only active on the active server.
- Load balancer with:
  - Configured per cluster.
  - Keep alive to **http://<UCMDB-Server:port>/ping?clusterId=<clusterId>**.
  - Session stickiness.

    - Round robin policy for the servers.
- Each server is connected to two separate networks:
    - Front-end (for load balancer access)
    - Back-end (for database and High Availability Controller communication)

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.

This section includes the following topics:

- "Install the Server" on page 217
- "Complete Server Startup" on page 218
- "Configure the Server" on page 219
- "Configure the Load Balancer" on page 219
- "Configure the Probe" on page 219

1 Install the Server

a Run the server installation on two or more machines without running the configuration wizard (select **No** at the wizard prompt).

Note: The machines used for the primary and backup 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 all servers you have installed.

- ➤ To run the wizard from a Windows platform, select **Start** > **HP Universal CMDB** > **Start UCMDB server configuration wizard**.

The first time the wizard runs, select the **Create new DB** option. The other times, select the **Connect to** option.

2 Complete Server Startup

a Start the first server. Wait until the startup process is completed.

b Install the servers. The typical configuration is two servers: one active and the other backup.

c Run the configuration wizard on one of the installed servers. Select **Create new schema**.

d Run the configuration wizard on the other servers. Select **Connect to existing schema** and provide the details of the schema you created for the first server.

e Run the first server. Open the Server Management Tool, located at: **\UCMDBServer\tools\server_management.bat**. For the server name, enter **localhost** or the name of the server. Enter the user name and password of system user (default is sysadmin/sysadmin). The connection from the tool to the HP Universal CMDB server is done via HTTPS. If there is a problem with the connection, make sure that **SSL** mode is configured (**Enable HTTPS connections** should be set to **true**). In the Server Management Tool, select the **Clusters** tab. Click the asterisk button to create a new cluster. On the right side of the opened window, add the machine names of all the servers you installed. Set one of them to be active.

Note: After saving, a dialog asks you if you want to switch all existing customers to the active server. Select **Yes**.

f Run all the other servers.

3 Configure the Server

a Access Infrastructure Settings Manager: **Admininstration** > **Infrastructure Settings Manager**.

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 the infrastructure settings.
- There should be a round robin policy for the servers.
- Session stickiness should be maintained.
- 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 non-active server returns HTTP response 503 (service unavailable).

Note: It is important for the load balancer to provide the cluster ID in the keep alive request, because a server can belong to several clusters, being active in one and passive in another.

5 Configure the Probe

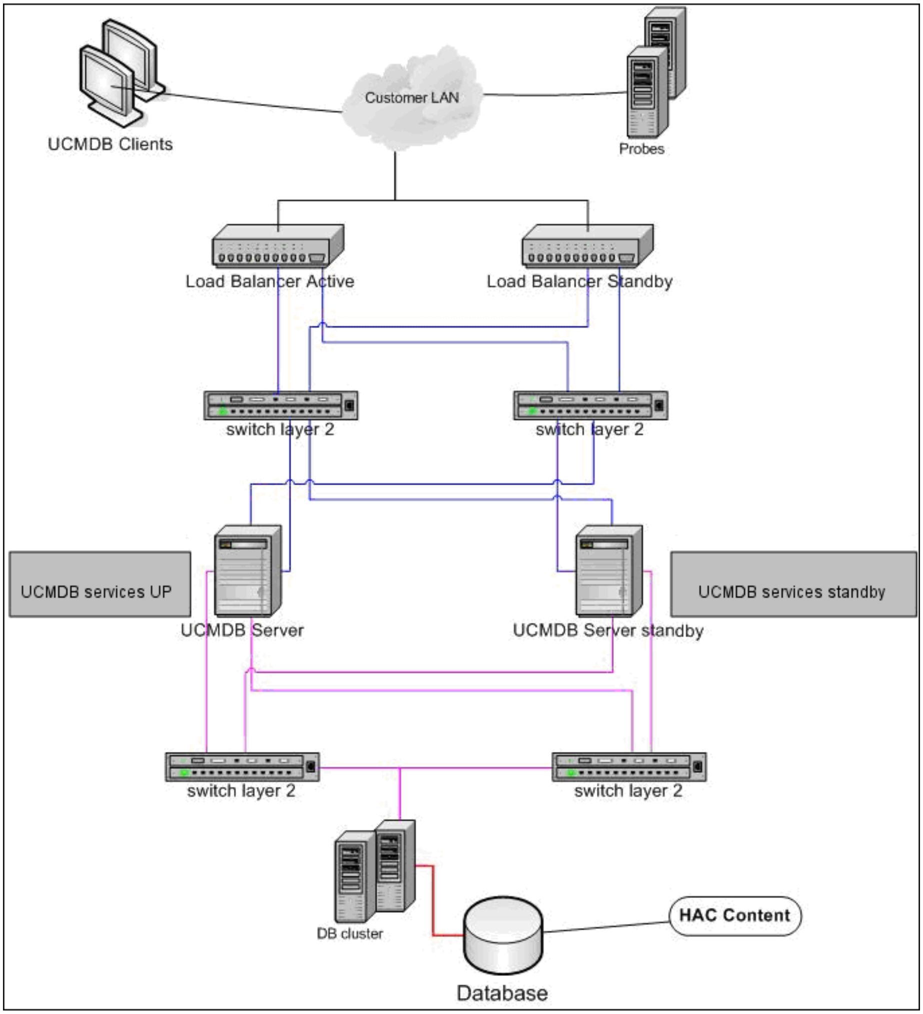
a Run the Probe installation on the Probe machine with the load balancer virtual IP address as the HP Universal CMDB server name.

b Start the Probe.

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.

14

HP Universal CMDB Large Capacity Planning

This chapter includes:

Concepts

- Large Capacity Planning Overview on page 224
- Managed Hosts and Host-Related CIs on page 225

Tasks

- UCMDB Server Configuration on page 226
- Oracle Database Configuration on page 226

Reference

- System Test Setup on page 227
- System Test Results on page 228

Concepts

Large Capacity Planning Overview

Using the default configuration, HP Universal CMDB can work with a deployment of up to 12.5 million objects and links. To work with a larger deployment, you must implement the following configuration:

- Use an Oracle database to store the CIs and links in the CMDB.
- Increase the CMDB heap to 8 GB. For details, see "UCMDB Server Configuration" on page 226.
- Set up the Oracle Database SGA as follows: 4 GB supported, 8 GB recommended. For details, see "Oracle Database Configuration" on page 226.

The following table displays the maximum supported number of CIs and links for a UCMDB deployment:

Database/Operating System	Windows	Linux
MS SQL Server	12.5 million CIs and links	12.5 million CIs and links
Oracle	25 million CIs and links (Configuration required as described in this section)	12.5 million CIs and links

Based on this table, if you estimate that your system will exceed 12.5 million CIs and links in the future, you should install the UCMDB Server on a Windows 64-bit platform and configure it to use the Oracle database.

For more details on:

- The changes you must make to the system configuration to support this capacity, see "UCMDB Server Configuration" on page 226.

- How you can improve performance, see "Oracle Database Configuration" on page 226.
- The setup used for capacity testing, see "System Test Setup" on page 227.
- Performance results of the system test run on UCMDB 9.00, see "System Test Results" on page 228.

Managed Hosts and Host-Related CIs

When planning capacity, among other issues, you should consider the ratio of managed hosts in your CMDB to host-related CIs. Host-related CIs include all CIs of types which are subclasses of Application Resource, Host Resource, or Software Element.

The following table lists the number of host-related CIs you can discover for each managed host in your environment. This number depends on the size of your deployment and the number of managed hosts: The more managed hosts you maintain in the CMDB, the fewer host-related CIs you can discover for each managed host.

For example, in an Enterprise deployment if you are running 56,000 managed hosts, you can discover 160 host-related CIs for each managed host. If you are running only 18,000 managed hosts, you can discover 500 resource CIs for each managed host.

Deployment	Number of Managed Hosts/Host-Related CIs
Enterprise	56000/160 – 18000/500
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 25 million CIs and links, you should update the following parameters on the UCMDB Server:

- **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
  ```

Oracle Database Configuration

When working on a system containing 25 million objects and links, you can improve performance by increasing the Oracle SGA size to 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 25 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	24 GB	Win2008R2 64-bit
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	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
  - Perspective
  - Different number of hierarchies in the TQL results (1-5)

    - Compound
    - Sub-graph
    - JoinF
- **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: For most TQLs the 90% percentile is below 1 second of calculation time.

Part VI

Hardening HP Universal CMDB

15

Introduction to Hardening

This chapter includes:

Concepts

➤ Hardening Overview on page 231

➤ Hardening Preparations on page 233

Tasks

➤ Deploy HP Universal CMDB in a Secure Architecture on page 234

➤ Change User Name or Password for the JMX Console on page 235

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 guidelines relate to both single machine and distributed deployments of 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 Chapter 17, "Using a Reverse Proxy."

If you must use another type of secure architecture with HP Universal CMDB, 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 Chapter 19, "Hardening the Data Flow Probe."

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 Chapter 16, "Enabling Secure Sockets Layer (SSL) Communication" 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 237.

➤ **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 245.

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 UCMDB Data Flow Probe with Mutual Authentication” on page 272.

Change User Name or Password for the JMX Console

The JMX console uses system users, that is, cross-customer users in a multi-tenant 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 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 JMX MBEAN View 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 user name or password through the Server Management tool:

- For **Windows**, run the following file: **C:\hp\UCMDB\UCMDBServer\tools\server_management.bat**.

16

Enabling Secure Sockets Layer (SSL) Communication

This chapter includes:

Tasks

- Enable SSL on the Server Machine With a Self-Signed Certificate on page 237
- Enable SSL on the Server Machine With a Certificate from a Certification Authority on page 239
- Enable SSL on the Client Machines on page 241
- Enable SSL on the Client SDK on page 242
- Change the Server Keystore Passwords on page 242
- Enable or Disable HTTP/HTTPS Ports on page 244

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 the Jetty 6.1 as the default Web server.

The HP Universal CMDB keystore (JKS type) should be placed in the **C:\hp\UCMDB\UCMDBServer\conf\security** folder.

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 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 <ucmdbServer Root
Dir>\conf\security\server.keystore
```

  The console dialog box opens.

- Enter the keystore password. If the password has changed, run the **changeKeystorePassword** JMX method, in 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 <ucmdbServer Root
Dir>\conf\security\server.keystore -storepass <your password> -file hpcert
```

3 Place the Certificate in the Client's Trusted Store

After generating the 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 the **server.keystore**.

4 Disable HTTP Port 8080

For details, see "Enable or Disable HTTP/HTTPS Ports" on page 244.

Tip: 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 244.

Tip: 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 the **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 trust store.

The following example demonstrates how to import the self-signed **hpcert** certificate into the Windows trust store to be used by Internet Explorer.

To import a certificate into the Windows trust store:

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 trust store 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)>
```

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.

Tip: 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 JMX MBEAN View page.

c Locate and execute the **changeKeystorePassword** operation.

This field must not be empty and 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 <ucmdbServer Root
Dir>\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 <ucmdbServer Root Dir>\conf\security\server.keystore
```

c Change the key password (if the store is not empty):

```
keytool -keypasswd -alias <alias> -keypass <currentPass> -new <newPass> -
keystore <ucmdbServer Root Dir>\conf\security\server.keystore
```

Note: The store password must match the individual key password, so you must change the store password with the property mentioned above and then change the password to each key to match that password.

5 Start the UCMDB Server

6 Repeat the procedure for the Server truststore

Enable or Disable HTTP/HTTPS Ports

1. Log on to HP Universal CMDB.
2. Access Infrastructure Settings (**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 the **Server Management Util** from functioning.

17

Using a Reverse Proxy

This chapter includes:

Concepts

- Reverse Proxy Overview on page 246
- Security Aspects of Using a Reverse Proxy Server on page 247

Tasks

- Configure a Reverse Proxy Using Infrastructure Settings on page 248
- Configure a Reverse Proxy Using the JMX Console on page 249

Reference

- Apache 2.0.x – Example Configuration on page 250

Concepts

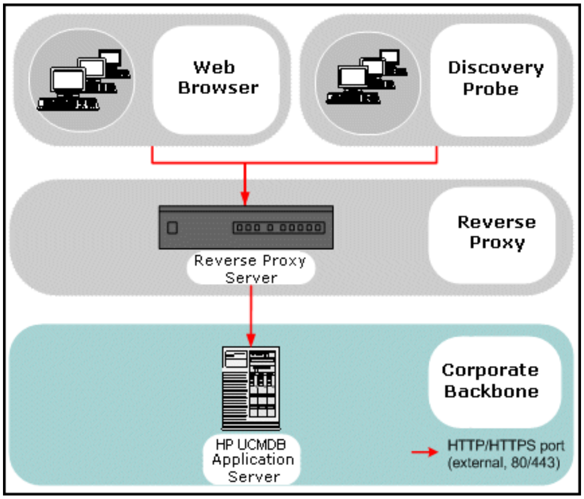
Reverse Proxy Overview

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.

HP Universal CMDB supports a reverse proxy in DMZ architecture. The reverse proxy is an HTTP mediator between the Data Flow Management (DFM) 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 250.

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 enable a reverse proxy configuration:

To enable a reverse proxy configuration:

1. Access Infrastructure Settings (**Administration** > **Infrastructure settings**).
2. In the Categories pane, select the **General Settings** option.
3. Change the **Frontend URL** setting. Enter the address, for example, **https://my_proxy_server:443/**.
4. Change the **Is Frontend URL from settings enabled?** to **true**.

Important: Once you have made this change, you cannot access the HP Universal CMDB server directly through a client. However, you can change the reverse proxy configuration using the JMX console on the server machine. For details, see "Configure a Reverse Proxy Using the JMX Console" on page 249.

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.

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 disable/enable this setting, use the **enableUseFrontendURLBySettings** or **disableUseFrontendURLBySettings** methods.

6 To see the value of this setting, use the **showFrontendURLInSettings** method.

Reference

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 **MAM_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:

```
ProxyRequests off
<Proxy *>
Order deny,allow
Deny from all
Allow from all
</Proxy>
ProxyPass /mam http://MAM_server/mam
ProxyPassReverse /mam http://MAM_server/mam
ProxyPass /mam_images http://MAM_server/mam_images
ProxyPassReverse /mam_images http://MAM_server/mam_images
ProxyPass /mam-collectors http://MAM_server/mam-collectors
ProxyPassReverse /mam-collectors http://MAM_server/mam-collectors
ProxyPass /ucmdb http://MAM_server/ucmdb
ProxyPassReverse /ucmdb http://MAM_server/ucmdb
ProxyPass /site http://MAM_server/site
ProxyPassReverse /site http://MAM_server/site
ProxyPass /ucmdb-ui http://MAM_server/ucmdb-ui
ProxyPassReverse /ucmdb-ui http://MAM_server/ucmdb-ui
```

4 Save your changes.

18

Hardening Data Flow Management

This chapter includes:

Concepts

- Hardening Data Flow Management Overview on page 254
- Credentials Encryption With Confidential Manager on page 256

Tasks

- Manage the Storage of Credentials on page 257
- Generate or Update the Encryption Key on page 259
- Export and Import the domainScopeDocument (DSD) File in Encrypted Format on page 265

Concepts

Hardening Data Flow Management Overview

Discovery credentials entered in the Data Flow Probe Setup window are saved in UCMDB DB, and managed by the Confidential Manager. On the Probe side, the credentials are saved in an encrypted file termed a domain scope document (DSD). This DSD contains discovery domain data. Each discovery domain entry in the document contains the network scope for the domain's Probes and the credentials the Probes may use when communicating with remote machines.

Note: Security features related to HP Universal CMDB user management—for example, authentication and authorization—are not discussed here.

This section includes the following topics:

- "Basic Security Assumptions" on page 254
- "Credentials Encryption Management" on page 255
- "HTTPS\SSL Configuration" on page 256

Basic Security Assumptions

Note the following security assumptions:

- You have secured the HP Universal CMDB Server and Probe file systems for authorized access only.
- You have secured the UCMDB Server JMX console to enable access to UCMDB system administrators only, preferably through localhost access only.

Credentials Encryption Management

Note the following guidelines for managing credential encryption:

- The **domainScopeDocument** (DSD) file is encrypted using standard, symmetric encryption. The DSD file is encrypted during transfer and at its location (the key is stored on the server database and the Probe file system). The encryption uses an AES algorithm with a default key of 192 bytes (but you can decide the length of the encryption/decryption key and other security parameters). For details on changing the key size, see "Update an Encryption Key" on page 261.
- A default, symmetric key is distributed with the UCMDB installation. As all default keys are identical, you should replace this key with a locally-generated key.
- The DSD file is exportable and importable in encrypted file form. To import a file you should supply the matching key used for the encryption of the file. Perform the import and export operations through the server's JMX console (the Discovery Manager service). For details, see "Export and Import the domainScopeDocument (DSD) File in Encrypted Format" on page 265.
- You can exchange the key while the system is up to keep the consistency of the system without losing any data. This is managed through the server's JMX console. For details, see "Generate or Update the Encryption Key" on page 259.
- When a key is updated, you can automatically distribute the new key to the Probes. This option is easier to deploy but is considered less secure. The new key is encrypted using the old key. To achieve better security, you can change the key manually. For details, see "Generate a New Encryption Key" on page 260.
- The key for DSD encryption is itself encrypted using DPAPI and is stored on the Probe and UCMDB server file systems (in encrypted format–and not in clear text). DPAPI relies on the Windows user password in the encryption process. Therefore, to ensure that the Probe can read the key, the Probe should always run under the same Windows user that was used during the Probe's installation (it is possible to change the user password). (DPAPI is a standard method to protect confidential data—such as certificates and private keys—on Windows.)

HTTPS\SSL Configuration

You can configure communication between the HP Universal CMDBServer and the Data Flow Probe to use HTTPS\SSL. This enables better DSD security during transit.

Note: As a result of using SSL, other aspects (for example, discovery tasks and gathered results) of the HP Universal CMDB product may become more secure.

Credentials Encryption With Confidential Manager

Note the following guidelines for managing credential encryption:

- The **domainScopeDocument** (DSD) file on the UCMDB Server contains credentials IDs only. Credentials details are stored on Confidential Manager. For details, see Chapter 21, “Confidential Manager.”
- The DSD file on the Data Flow Probe contains full credentials information. This copy is encrypted using standard symmetric encryption.

When the UCMDB Server updates the Probe with a new copy of the DSD, the following process occurs:

1. A new copy of DSD is created. This copy contains full credentials information that has been loaded from Confidential Manager.
2. The DSD copy is encrypted using standard symmetric encryption and transferred to the Data Flow Probe.

The encryption uses an AES algorithm with a default key of 192 bytes. However, you can decide the length of the encryption and decryption keys and other security parameters. For details on changing the key size, see “Update an Encryption Key” on page 261.

- A default, symmetric key is distributed with the UCMDB installation. As all default keys are identical, you should replace this key with a locally generated key.
- The DSD file is exportable and importable in encrypted file format. To import a file you should supply the matching key used for the encryption of the file. Perform the import and export operations through the Server's JMX console (the Discovery Manager service). For details, see “Export and Import the domainScopeDocument (DSD) File in Encrypted Format” on page 265.

Tasks

Manage the Storage of Credentials

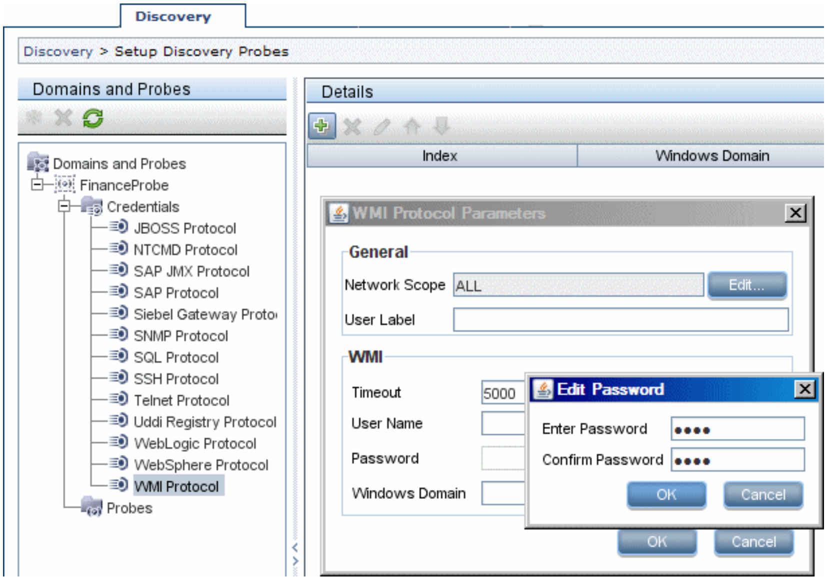
This section explains how to manage the DSD file.

This section includes the following tasks:

- “View Credentials Information (Data Direction: Server to HP Universal CMDB)” on page 258
- “Update Credentials (Data Direction: HP Universal CMDB to Server)” on page 258

1 View Credentials Information (Data Direction: Server to HP Universal CMDB)

Passwords are not sent from the Server to the application. That is, HP Universal CMDB displays asterisks (*) in the password field, regardless of content:



Network Scope: ALL

User Label:

Timeout: 5000

User Name:

Password:

Windows Domain:

Enter Password: ●●●●

Confirm Password: ●●●●

2 Update Credentials (Data Direction: HP Universal CMDB to Server)

- 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.

- The password field is limited to 40 characters. The length of the password is not limited in other ways since it is saved only in a file.

- You can use special characters and non-English characters as passwords.

Generate or Update the Encryption Key

You can generate or update an encryption key for probe encryption and the transport of credentials from server to Probe. In each case DFM creates a new encryption key based on parameters that you supply (key length, extra PBE cycles, JCE provider). You can also disable DPAPI encryption.

The result of running the **generateEncryptionKey** method is a new generated encryption key. This key is stored only in the **secured_storage.bin** file and its name and details are not known. If you reinstall an existing 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 to 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 section includes the following tasks:

- "Generate a New Encryption Key" on page 260
- "Update an Encryption Key" on page 261
- "Retrieve Encryption Key File Name" on page 262
- "Disable DPAPI Encryption" on page 263
- "Manually Change the Encryption Key When Probe Manager and Probe Gateway Installed on Separate Machines" on page 264
- "Define Several JCE Providers for the Server" on page 264

Generate a New Encryption Key

You can generate a new key to be used by the UCMDB Server and Data Flow Probe for encryption/decryption. DFM 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. 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=Discovery Manager** to open the JMX MBEAN View page.

3. Locate the **generateEncryptionKey** operation.

   - In the **customerId** parameter box, enter **1** (the default).
   - **keySize**. The length of the encryption key (the length can be 128, 192, or 256).
   - **usePBE**. **True**: use additional PBE hash cycles. **False**: do not use additional PBE hash cycles.
   - **jceVendor**. You can choose to use a non-default JCE provider. If the box is empty, the default provider is used.
   - **autoUpdateProbe**. **True**: The server distributes the new key to the Probes automatically. **False**: The new key should be placed on the Probes manually.

- **exportEncryptionKey**. **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\server\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 have changed 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**).

---

4 Click **Invoke** to generate the encryption key.

Update an Encryption Key

You use the **changeEncryptionKey** method to import an encryption key.

To update an encryption key through the JMX Console:

1 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=Discovery Manager** to open the JMX MBEAN View page.

3 Locate the **changeEncryptionKey()** operation.

- In the **customerId** parameter box, enter **1** (the default).
- **newKeyFileName**. Enter the name of the new key.

- **keySizeInBits**. The length of the encryption key (the length can be 128, 192, or 256).
- **usePBE**. **true**: use additional PBE hash cycles. **false**: do not use additional PBE hash cycles.
- **jceVendor**. You can choose to use a non-default JCE provider. If the box is empty, the default provider is used.
- **autoUpdateProbe**. Leave as **True** for the server to automatically distribute the changed key to the Probes.

  Select **False** to distribute the changed key 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 have changed 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**).

4 Click **Invoke** to generate and update the encryption key.

Retrieve Encryption Key File Name

When you change an encryption key on the server (by using the **changeEncryptionKey** method), you may not want the new key to be downloaded automatically to the Probes because of security concerns. You can download the encryption key file to a Probe manually.

To prevent automatic download, run the importEncryptionKey method:

1 Place the encryption key file in the **C:\hp\UCMDB\DataFlowProbe\runtime\probeManager\binaryData** directory.

2 Launch the Web browser and enter the Probe address, as follows: http://localhost:1977/.

You may have to log in with a user name and password.

3 Under the Probe domain, click **type=MainProbe** to open the MBean View page.

4 Locate the **importEncryptionKey** method.

5 Enter the name of the encryption key file that resides in the **C:\hp\UCMDB\DataFlowProbe\runtime\probeManager\binaryData** directory.

This file contains the key to be imported.

6 Click the **importEncryptionKey** button.

Disable DPAPI Encryption

The key is encrypted with DPAPI on the file system. You can disable this encryption.

To disable encryption with DPAPI:

1 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=Discovery Manager** to open the JMX MBEAN View page.

3 Locate the **setDPApiUsage()** operation and enter the following properties:

- ➤ In the **customerId** parameter box, enter **1** (the default).
- ➤ **useDPAPI**. **true**: use DPAPI. **false**: do not use DPAPI.

4 Click **Invoke** to disable the DPAPI encryption.

Manually Change the Encryption Key When Probe Manager and Probe Gateway Installed on Separate Machines

a On the Probe Manager machine, start the Probe Gateway service: **Start** > **Programs** > **HP UCMDB** > **Probe Gateway**.

b Import the key from the server, using the Probe Gateway JMX. For details, see "Generate a New Encryption Key" on page 260.

c After the encryption key is imported successfully, stop the Probe Gateway service.

Define Several JCE Providers for the Server

When generating an encryption key through the JMX Console, you can define several JCE providers with the **changeEncryptionKey** and **generateEncryptionKey** methods.

To change the default JCE provider:

1. Register the JCE provider jar files at 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 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.

Export and Import the domainScopeDocument (DSD) File in Encrypted Format

You can export and import DSD files in encrypted format. (You would probably import a DSD file during recovery following a system crash or during upgrade.)

- ➤ **When exporting the DSD file**, you must enter a password (of your choosing). The file is encrypted with this password. The encryption key used for storing the DSD file in the UCMDB database is no longer used.
- ➤ **When importing the DSD file**, you must use the same password that was defined when the DSD file was exported.

Important: If you exported the domainScopeDocument file from UCMDB version 8.02, to import the file to your present version, copy the password from the contents of the key.bin file located on the version 8.02 system.

To export or import a DSD file:

1. 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. Under UCMDB, click **UCMDB:service=Discovery Manager** to open the JMX MBEAN View page.
3. Locate the **ExportDomainScopeDocument** or **importDomainScopeDocument** operation and enter the existing file name and password.
4. Click **Invoke** to export or import the domainScopeDocument file.

   The location of the saved domainScopeDocument file is the **C:\hp\UCMDB\UCMDBServer\conf\server\discovery\<customer_dir>** directory.

19

Hardening the Data Flow Probe

This chapter includes:

Tasks

- Set the MySQL Database Encrypted Password on page 268
- Set the JMX Console Encrypted Password on page 270
- Enable SSL Between UCMDB Server and UCMDB Data Flow Probe with Mutual Authentication on page 272
- Enable SSL on the Data Flow Probe with Basic Authentication on page 278
- Connect the Data Flow Probe by Reverse Proxy on page 278
- Control the Location of the domainScopeDocument File on page 280

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 **admin** and the password **admin** to log in.

---

b Locate the **Type=MainProbe** service and click the link to open the JMX MBEAN View 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

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).

Note: For Business Service Management: **Admin** > **ODB Administration** > **Data Flow Management** > **Resource Configuration** > **NetLinks** > **Configuration Files**

---

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 268.

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

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 **admin** and the password **admin** to log in.

---

b Locate the **Type=MainProbe** service and click the link to open the JMX MBEAN View 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 **getEncryptedDBPassword** 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

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

Test the result in a Web browser.

Enable SSL Between UCMDB Server and UCMDB Data Flow Probe with Mutual Authentication

Note: In version 9.00, this functionality is not supported. Instead, you should use basic authentication. For details, see “Enable SSL on the Data Flow Probe with Basic Authentication” on page 278.

You can set up authentication for both the Data Flow Probe and the UCMDB server with certificates. The certificate for each side is sent and authenticated before the connection is established.

Important: The following method of enabling SSL on the Data Flow Probe replaces the procedure for basic authentication, which is deprecated. For details on basic authentication, see “Enable SSL on the Data Flow Probe with Basic Authentication” on page 278.

This section includes the following topics:

- “Overview” on page 273
- “Keystores and Truststores” on page 273
- “Enable Mutual Certificate Authentication” on page 273
- “Encrypt a Password” on page 276
- “Create and Import a Keystore” on page 276
- “Enable Server Certificate Authentication Only” on page 278

Overview

UCMDB supports the following modes of communication between the UCMDB server and the Data Flow Probe:

- **Mutual Authentication**. This mode uses SSL and allows both server authentication by the Probe and client authentication by the server. For details, see "Enable Mutual Certificate Authentication" on page 273.
- **Server Authentication**. This mode uses SSL, and the Probe authenticates the UCMDB Server's certificate. For details, see "Enable Server Certificate Authentication Only" on page 278
- **Standard HTTP**. No SSL communication. This is the default mode, that is, the SSL port is disabled in UCMDB and the server communicates with the Data Flow Probe 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's certificate).

Enable Mutual Certificate Authentication

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 you do not have to perform the following procedure. To validate trust, try connecting to the Web server using SSL and check whether the certificate is already trusted.

During authentication, the UCMDB server sends its certificate to the Data Flow Probe client machine, and the Data Flow Probe sends its certificate to the UCMDB server.

Note: SSL is enabled by default. For details, see “Enabling Secure Sockets Layer (SSL) Communication” on page 237.

1 Enable Client Certificate Authentication on the UCMDB Server

a Access the **web.xml** file:

The **web.xml** file is located in the **WEB-INF** folder in the **mam-collectors.war** archive file, in the **C:\hp\UCMDB\UCMDBServer\j2f\AppServer\deploy\mam-jars\** folder.

b Uncomment the following section in the **web.xml** file:

```
<security-constraint>
       <web-resource-collection>
           <web-resource-name>AutoDiscovery_Servlets</web-resource-name>
                <description>Require users to authenticate</description>
                <url-pattern>/collectors/*</url-pattern>
                <url-pattern>/collectorsResults/*</url-pattern>
                <url-pattern>/collectorsUnSerializedResults/*</url-pattern>
                <url-pattern>/downloader/*</url-pattern>
       </web-resource-collection>
       <auth-constraint>
           <role-name>*</role-name>
       </auth-constraint>
   </security-constraint>
   <login-config>
       <auth-method>CLIENT-CERT</auth-method>
       <realm-name>AutoDiscovery</realm-name>
   </login-config>
  <security-role>
     <role-name>*</role-name>
  </security-role>
```

2 Enable SSL Communication for the Data Flow Probe

a Edit the **DiscoveryProbe.properties** file in the following folder: **C:\hp\UCMDB\DataFlowProbe\conf\**.

b Change the property **appilog.agent.probe.protocol** to **HTTPS**.

c Verify that the **serverPortHttps** value is the same as the HTTPS port used on the UCMDB Server (the default port is 8443):

➤ **DiscoveryProbe.properties:**

```
# Ports used for HTTP/s traffic
serverPort = 8080
serverPortHttps = 8443
```

3 Define the Keystore and Truststore Files for the Data Flow Probe

a Edit the **ssl.properties** file in the following folder: **C:\hp\UCMDB\DataFlowProbe\conf\security\**.

b Add the name of the keystore file to the **javax.net.ssl.keyStore** property.

Important: The Data Flow Probe Keystore defined in **C:\hp\UCMDB\DataFlowProbe\conf\security\ssl.properties** must contain one key entry only.

---

c Add the name of the truststore file to the **javax.net.ssl.trustStore** property.

d Define the encrypted password for the keystore in the **javax.net.ssl.keyStorePassword** property.

e Define the encrypted password for the truststore in the **javax.net.ssl.trustStorePassword** property.

Note: The keystore and truststore passwords are encrypted. For details, see “Encrypt a Password” on page 276.

Encrypt a Password

The DFM keystore and truststore encrypted passwords are stored in the **ssl.properties** file in the following folder: **C:\hp\UCMDB\DataFlowProbe\conf\security\**.

1. Run the Data Flow Probe (**Start** > **Programs** > **HP UCMDB** > **Start Data Flow Probe**).
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**.

   You may have to log in with a user name and password.
3. Locate the **Type=MainProbe** service and click the link to open the JMX MBEAN View page.
4. Locate the **getEncryptedKeyPassword** operation.
5. Enter your keystore or truststore password in the **Key Password** field and click **getEncryptedKeyPassword**.
6. Open the **ssl.properties** file in the following folder: **C:\hp\UCMDB\DataFlowProbe\conf\security\**.
7. Copy and paste the encrypted password (numbers separated by commas, for example, 1,2,3,4,5) into the relevant keystore or truststore line of the **ssl.properties** file.
8. Save the file.

Create and Import a Keystore

The following sections describe how to:

- create a new keystore for the Data Flow Probe
- export its certificate
- import the certificate into the UCMDB Server truststore

To create the Data Flow Probe's keystore:

1 Run the following command:

```
C:\hp\UCMDB\DataFlowProbe\bin\jre\bin\keytool -genkey -alias dfmkey -keyalg RSA -
keystore C:\hp\UCMDB\DataFlowProbe\conf\security\client.keystore
```

2 Enter information as required, for example, the password, keystore password, name and organization.

3 When asked, **Is CN=... C=... Correct?** type **yes** and press ENTER.

4 Press ENTER again to accept the keystore password as the key password.

5 Ensure that the following file has been created: **C:\hp\UCMDB\DataFlowProbe\conf\security\client.keystore**

To export the Data Flow Probe's certificate from the created keystore:

1 Run the following command:

```
C:\hp\UCMDB\DataFlowProbe\bin\jre\bin\keytool.exe -export -alias dfmkey -keystore
C:\hp\UCMDB\DataFlowProbe\conf\security\client.keystore -file
C:\hp\UCMDB\DataFlowProbe\conf\security\client.cer
```

2 Enter the keystore password that you created previously.

3 Ensure that the following file has been created: **C:\hp\UCMDB\DataFlowProbe\conf\security\client.cer**

To import the Data Flow Probe’s certificate into the UCMDB server’s truststore, to enable client authentication:

1 Run the following command:

```
C:\hp\UCMDB\DataFlowProbe\bin\jre\bin\keytool.exe -import -v -keystore
<SERVER_TRUSTSTORE_PATH> -file
C:\hp\UCMDB\DataFlowProbe\conf\security\client.cer -alias dfmkey
```

2 Enter the truststore password of the UCMDB server.

3 When asked, **Trust this certificate?** type **yes** and press ENTER.

4 Ensure the output is **Certificate was added to keystore**.

Enable Server Certificate Authentication Only

You can enable UCMDB Server authentication only, that is, the UCMDB server sends its certificate to the Data Flow Probe for authentication.

Use the procedure in the following steps: step 2 on page 274 and step 3 on page 275.

Enable SSL on the Data Flow Probe with Basic Authentication

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 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

Requests for... on the Reverse Proxy Server	Proxy Request to be Served by:
/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 "Manage the Storage of Credentials" on page 257.

2 Restart the Probe.

20

Lightweight Single Sign-On Authentication – General Reference

This chapter includes:

Concepts

- LWSSO Authentication Overview on page 282

Tasks

- Retrieve Current LW-SSO Configuration In Distributed Environment on page 283
- Enable Login to HP Universal CMDB with Lightweight Single Sign-On (LW-SSO) on page 284

Reference

- LW-SSO System Requirements on page 285
- LW-SSO Security Warnings on page 286

Troubleshooting and Limitations on page 288

Concepts

LWSSO Authentication Overview

Single Sign-On 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.

This section includes the following topics:

- "LW-SSO Token Expiration" on page 282
- "Recommended Configuration of the LW-SSO Token Expiration" on page 282
- "GMT Time" on page 282
- "Multi-domain Functionality" on page 283
- "Get SecurityToken for URL Functionality" on page 283

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 **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 a URL from other applications, the host application should configure the correct domain in the **lwsso** element of the configuration.

Tasks

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 JMX MBEAN View page.

3 Locate the **retrieveLWSSOConfiguration** operation.

4 Click **Invoke** to retrieve the configuration.

Enable Login to HP Universal CMDB with Lightweight Single Sign-On (LW-SSO)

HP Universal CMDB is configured with Lightweight Single Sign-On (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.

To enable Single Sign-On for HP Universal CMDB, use one of the following procedures:

Using JXM 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 JMX MBEAN View page.
3. Invoke the method **setLWSSOEnabled** with the parameter set to **True**.

Note: You also have to set the domain name of the machine on which UCMDB is installed and the init string using the methods **setLWSSODomain** and **setLWSSOInitString**.

4. **Optional**. Set additional LW-SSO configuration parameters, using the relevant methods. For details about additional parameters, see "LWSSO Authentication Overview" on page 282.
5. Invoke the method **reloadLWSSOConfiguration** to ensure that the configuration is loaded from the settings (the server does not need to be restarted).

6 To view the LW-SSO configuration as it is saved in the settings mechanism, invoke the **retrieveLWSSOConfigurationFromSettings** method.

7 To view the actual ,loaded LW-SSO configuration, invoke the **retrieveLWSSOConfiguration** method.

Using HP Universal CMDB Infrastructure Settings

1 Log on to HP Universal CMDB.

2 Access **Administration** > **Infrastructure Settings**.

3 Set the domain name and init string using the entries **LW-SSO domain** and **LW-SSO init string**.

4 Change the setting entry **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 "LWSSO Authentication Overview" on page 282.

6 Restart the server.

Reference

LW-SSO System Requirements

The requirements for LW-SSO configuration, per application, are as follows:

Application	Version	Comments
Java	1.5 and higher	N/A
HTTP Sevlets API	2.1 and higher	N/A
Internet Explorer	6.0 and higher	Browser should enable HTTP session cookie and HTTP 302 Redirect functionality

Application	Version	Comments
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	N/A
Acegi Authentications	Acegi 0.9.0 Acegi 1.0.4	N/A
Web Services Engines	Axis 1 - 1.4 Axis 2 - 1.2 JAX-WS-RI 2.1.1	N/A

LW-SSO Security Warnings

This section describes security warnings that are relevant to the LW-SSO configuration:

- **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.

- **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.

Note:

- 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.
- It is recommended to use at least twelve characters for the **initString** parameter.

- **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. This potential risk is relevant when an application sharing an initString either resides or is accessible in 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, such as the same user name being 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 onto AppB and enter a username. If the user enters a different username than was used to log onto AppA, the following unexpected behavior can arise: If the user subsequently accesses a third application (AppC) from AppA or AppB, then they will access it using the usernames that were used to log onto AppA or AppB respectively.

Troubleshooting and Limitations

This section describes troubleshooting and limitations for Lightweight Single Sign-On (LW-SSO) authentication.

- **Accessing the application.** The client must access the application with the Fully Qualified Domain Name (FQDN) in the login URL, for example: http://flood.mercury.global:8080/WebApp

  LW-SSO does not support URLs with an IP Address, or URLs without a domain.

- **LW-SSO framework integration.** Applications can leverage and use LW-SSO capabilities only if integrated within the LW-SSO framework in advance.

- **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.

- **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 on 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 referring 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 cookies 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 by default blocked 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 *.mydomian.com) to the "Intranet"/"Trusted" zone on your computer (on 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.**
  - When using a Java based application integrated with LW-SSO to access another Java based application also integrated with LW-SSO, do not use the SAML2 token. Using the SAML2 token in this case can lead to unexpected behavior. Use the LW-SSO token instead.

    The SAML2 token should be used only when one of the applications is not integrated with LW-SSO.
  - Logout functionality is not supported when the SAML2 token is used.

    Therefore, if the SAML2 token is used to access a second application, then a user who logs out of the first application will not be 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 of each other.
- **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.

- **Multi-domain logout functionality when using Internet Explorer 7.** Multi-domain logout functionality may fail when using Internet Explorer 7 and when the application is invoking more then 3 consecutive HTTP 302 redirect verbs in the logout procedure.

  In such a scenario, 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 that, if possible, you reduce the number of application redirect commands in the logout sequence.

LW-SSO Related Use Cases

Problem	Possible Cause	Possible Solution
LW-SSO cookie is not created after logging in.	A domain is not defined properly in the LW-SSO element of the configuration.	Make sure that the domain defined in the LW-SSO element of the configuration is equal to the application's domain.
	A domain that is passed as a parameter to the enableSSO function is not correct.	Make sure that the domain that is passed as a parameter to the **enableSSO** function is equal to the application's domain.
	You did not access the application with the Fully Qualified Domain Name (FQDN) in the login URL.	Make sure that you access the application with the Fully Qualified Domain Name (FQDN) in the login URL.
LW-SSO fails to create a cookie for AutoCookieCreation functionality.	A domain is not defined properly in the LW-SSO element of the configuration.	Make sure that the domain defined in the LW-SSO element of the configuration is equal to the application's domain.

Problem	**Possible Cause**	**Possible Solution**
The LW-SSO token is not validated.	The two applications have different initString parameters in the crypto element of the configuration (or other crypto parameters).	Use the same initString in both applications (in addition to all other crypto parameters in the LW-SSO creation element).
	Some applications have a GMT time difference greater than 15 minutes.	Make sure that all applications participating in a LW - SSO integration are set to the same GMT time, with a maximum difference of 15 minutes.

Problem	Possible Cause	Possible Solution
LW-SSO fails to validate the LW-SSO token in a multi domain environment.	In the configuration of one of the applications, a domain is not defined properly in the LW-SSO element.	The domain defined in the LW-SSO element of the application's configuration must be the same as the application's domain according to real domains in use.
	In the configuration of one of the applications, a domain is not defined correctly in the protectdDomains list.	Make sure that the domains in the protectedDomains list of all of the applications' configurations are defined correctly.
	The LW-SSO session cookie is blocked/denied when using the Internet Explorer 6.0 or 7.0 browsers.	Add all LW-SSO servers to the "Intranet"/"Trusted" zone in the Internet Explorer security zones on your computer (**Tools** > **Internet Options** > **Security** > **Local Intranet** > **Sites** > **Advanced**). This will allow all cookies to be accepted.
	Some applications have different initString parameters in the crypto element of the configuration (or other crypto parameters).	Use the same initString in all applications (in addition to all other crypto parameters in the LW-SSO creation element).
	Some applications have a GMT time difference greater than 15 minutes.	Make sure that all applications participating in a LW - SSO integration are set to the same GMT time with a maximum difference of 15 minutes.
	Multi domain link goes from the protected (HTTPS) to the Non protected (HTTP) resource.	When linking/crossing from one domain to another, make sure that the first link/cross request goes from one protected resource (HTTPS) to another protected resource (HTTPS).

SAML2 Related Use Cases

Problem	Possible Cause	Possible Solution
LW-SSO fails to issue a SAML2 Token.	A keystore configuration for SAML2 creation is not valid and most likely does not point to a valid keystore.	Make sure that the keystore configuration for SAML2 creation is valid and points to a valid keystore.
	A privateKeyAlias or privateKeyPassword configuration for SAML2 creation is not valid. They might not be pointing to a valid private key.	Make sure that the privateKeyAlias or privateKeyPassword configuration for SAML2 creation is valid and point to a valid private key.
LW-SSO fails to validate the SAML2 token.	A keystore configuration for SAML2 validation is not valid. It most likely does not point to a valid keystore.	Make sure that the keystore configuration for SAML2 validation is valid and points to a valid keystore.
	A certificate used for signing is not imported in the configured keystore with a required public key alias. Note that the public key alias may be configured in the SAML2 validation configuration or it can be passed in SAML2 token by the issuer.	Make sure that the certificate used for signing in is imported in the configured keystore with a required public key alias.
LW-SSO fails to receive all roles or groups.	The element's roleAttributeName or groupAttributeName defined in the SAML2 configuration is different then the one configured in the applications' configurations element.	Make sure that the elements roleAttributeName or groupAttributeName is defined equally in all of the applications' configurations as in the SAML2 configuration.

21

Confidential Manager

This chapter includes:

Concepts

- ➤ Confidential Manager Overview on page 296
- ➤ Security Considerations on page 296

Tasks

- ➤ Configure the HP Universal CMDB Server on page 297

Reference

- ➤ Definitions on page 299
- ➤ Encryption Properties on page 300

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 details guidelines for managing credential encryption on the Data Flow Probe, see “Credentials Encryption With Confidential Manager” on page 256.

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 300. 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 300.

   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 databse 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 297.

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

22

Disaster Recovery Setup

This chapter includes:

Concepts

➤ Disaster Recovery Overview on page 306

Tasks

➤ Prepare the Disaster Recovery Environment on page 307

➤ Prepare the HP Universal CMDB Failover Instance for Activation on page 310

➤ Perform Startup Cleanup Procedure on page 311

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 HP Universal CMDB 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 307
- "Configure System and Data Backup" on page 307

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 2000:

- support.microsoft.com/default.aspx?scid=http://support.microsoft.com/support/sql/content/2000papers/LogShippingFinal.asp
- www.microsoft.com/technet/prodtechnol/sql/2000/maintain/logship1.mspx

Microsoft SQL Server 2005:

- 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 (for details, see page 311) to remove any localization in the databases.

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 Server and Database Configuration utility

Run the Server and Database Configuration utility on each machine to reinitialize the needed tables in the database. To run the Server and Database Configuration utility, select **Start** > **Programs** > **HP UCMDB** > **Start UCMDB 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). Possible complete loss of configuration data will 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 servers

If you want 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

23

Starting and Stopping the Server

This chapter includes:

Tasks

- Start and Stop the Server on the Windows Platform on page 315

Tasks

Start and Stop the Server on the Windows Platform

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 99.

During the installation of HP Universal CMDB, a start menu is added to the settings of the machine on which you installed UCMDB.

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

- **Start UCMDB 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 85.
- **Start UCMDB Server.** Click to start the server service.
- **Stop UCMDB Server.** Click to stop the server service.

- **UCMDB Server Status.** Click to open a Web page with information about the server. For details, see “HP Universal CMDB Services” on page 53.
- **Uninstall UCMDB Server.** Click to uninstall the server.

24

Accessing HP Universal CMDB Through the IIS Web Server

This chapter includes:

Concepts

- Accessing HP Universal CMDB Through IIS Overview on page 317

Tasks

- Set Up IIS to Enable Access to UCMDB – Windows 2003 on page 318
- Set Up IIS to Enable Access to UCMDB – Windows 2008 on page 322
- Configure the Data Flow Probe on page 325

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 318

- "Supported Configurations" on page 318

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 9.00 or later

Supported Configurations

The following configurations are supported for this integration:

- Windows 2003/8 64-bit, HP Universal CMDB 9.00 or later and IIS 6 or 7.X on the **same** server.
- Windows 2003/8 64-bit, HP Universal CMDB 9.00 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**.

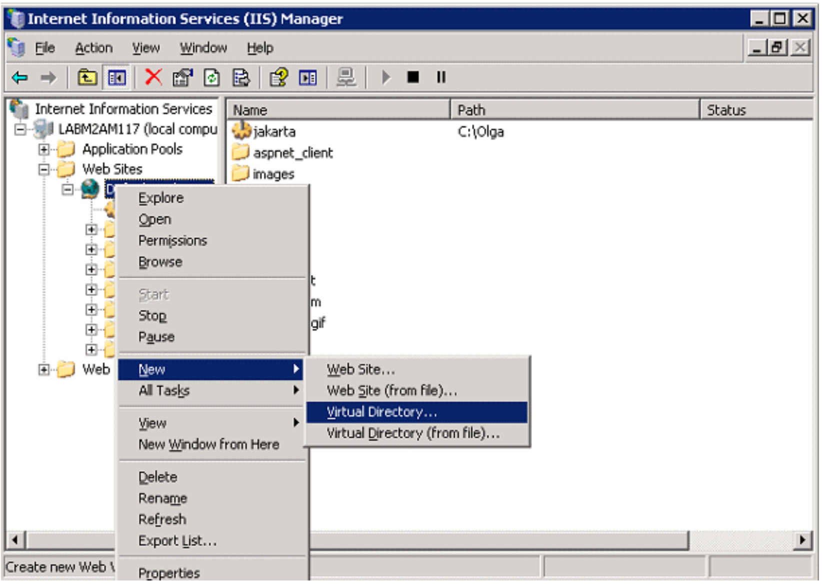
b the **worker_file** should contain the location of the **workers.properties.minimal** file, for example, **C:\hp\UCMDB\UCMDBServer\tools\iis_integration\workers.properties.minimal**.

c the **worker_mount_file** should contain the location of the **uriworkermap.properties** file, for example **C:\hp\UCMDB\UCMDBServer\tools\iis_integration\uriworkermap.properties**.

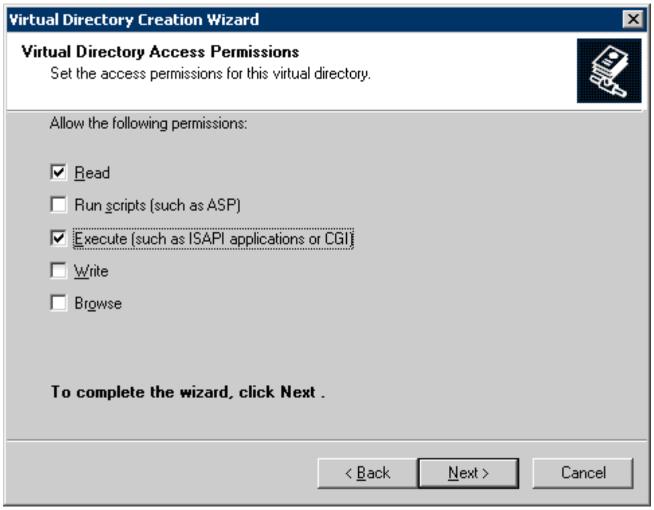
3 Change the string **worker.localAjp.host=localhost** to the UCMDB server hostname (if the HP Universal CMDB server does not reside on the same machine as IIS).

4 Open the IIS management console. Run **inetmgr** from the command line.

5 Add a new virtual directory to your IIS Web site for **Windows 2003/IIS6**:



6 The Virtual Directory Creation Wizard window appears. 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. Assign **Execute** access to the new virtual directory:



Virtual Directory Creation Wizard

Virtual Directory Access Permissions

Set the access permissions for this virtual directory.

Allow the following permissions:

☑ Read

□ Run scripts (such as ASP)

☑ Execute (such as ISAPI applications or CGI)

□ Write

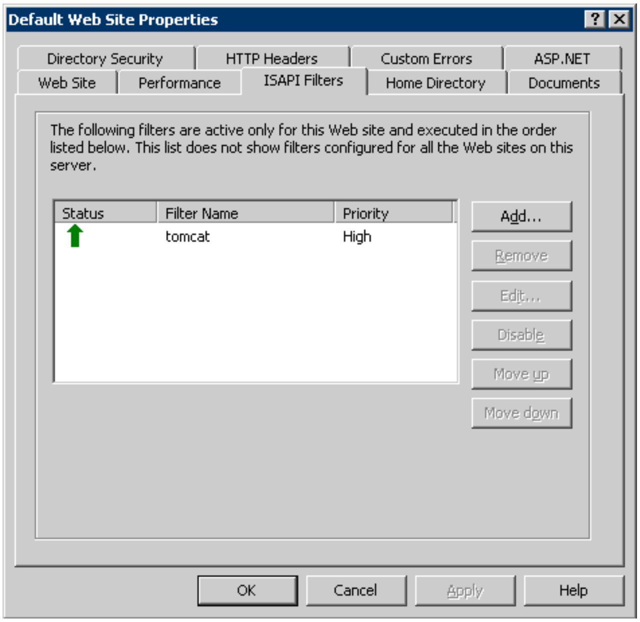
□ Browse

To complete the wizard, click Next .

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 Elements** 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:



The following filters are active only for this Web site and executed in the order listed below. This list does not show filters configured for all the Web sites on this server.

Status	Filter Name	Priority
⬆	tomcat	High

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:

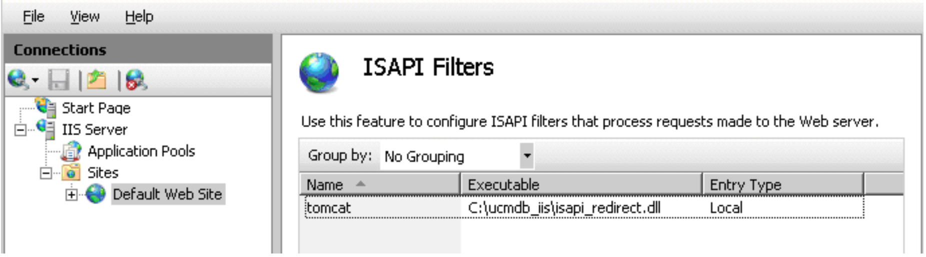
   a. the **log_file** should point to a folder containing the integration logs, for example, **C:\hp\UCMDB\UCMDBServer\runtime\log\isapi.log**.

   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 Managemet 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.



ISAPI Filters

Use this feature to configure ISAPI filters that process requests made to the Web server.

Group by: No Grouping

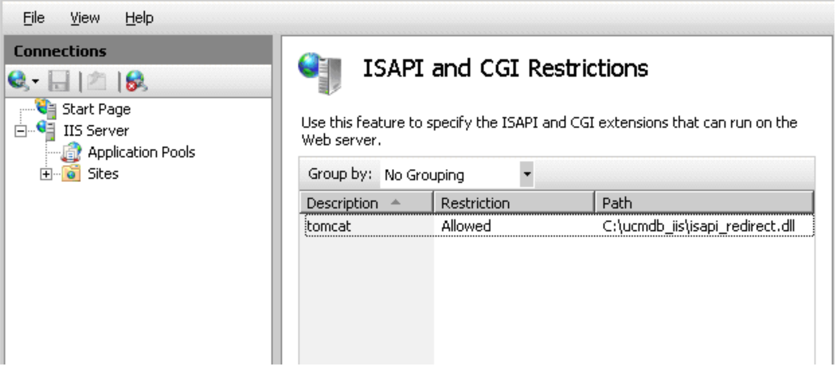
Name	Executable	Entry Type
tomcat	C:\ucmdb_iis\isapi_redirect.dll	Local

8 Select the name of the IIS server from the Connections pane.

9 Double-click **ISAPI and CGI restrictions**.

10 Right-click and enter the same information you added in step 7 above.

11 Check the box to allow the **Execution Path** to execute.



ISAPI and CGI Restrictions

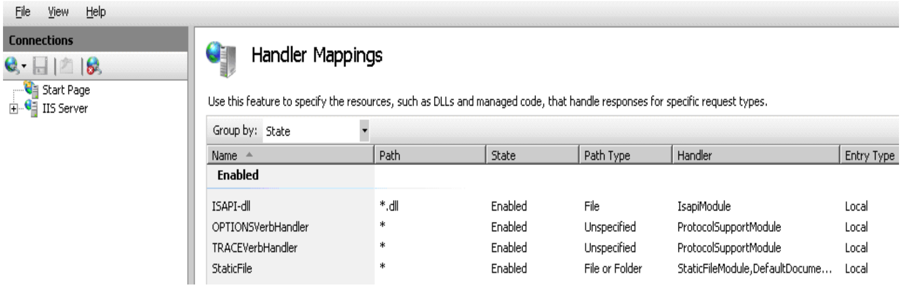
Use this feature to specify the ISAPI and CGI extensions that can run on the Web server.

Group by: No Grouping

Description	Restriction	Path
tomcat	Allowed	C:\ucmdb_iis\isapi_redirect.dll

12 Open **Handler Mappings**.

13 Select ISAPI-dll. Right-click and select **Edit Feature Permissions**. Click **Execute**.



Handler Mappings

Use this feature to specify the resources, such as DLLs and managed code, that handle responses for specific request types.

Group by: State

Name	Path	State	Path Type	Handler	Entry Type
Enabled					
ISAPI-dll	*.dll	Enabled	File	IsapiModule	Local
OPTIONSVerbHandler	*	Enabled	Unspecified	ProtocolSupportModule	Local
TRACEVerbHandler	*	Enabled	Unspecified	ProtocolSupportModule	Local
StaticFile	*	Enabled	File or Folder	StaticFileModule,DefaultDocume...	Local

14 Restart IIS.

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.

25

HP Universal CMDB Login Authentication

This chapter includes:

Concepts

➤ Authentication for HP Universal CMDB Login on page 327

Tasks

➤ Set Up an Authentication Method on page 328

➤ Enable and Define the LDAP Authentication Method on page 328

➤ Set a Secure Connection with the SSL (Secure Sockets Layer) Protocol on page 329

Reference

➤ Using the JMX Console to Test LDAP Connections on page 331

Concepts

Authentication for HP Universal CMDB Login

To perform authentication, you can work:

- Against the internal HP Universal CMDB service
- Through the Lightweight Directory Access Protocol (LDAP). For details, see "Enable and Define the LDAP Authentication Method" on page 328 and "LDAP Mapping" in *HP UCMDB Administration Guide*.

These options apply to logins performed through Web services as well as through the user interface.

Tasks

Set Up an Authentication Method

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.

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.

To define the LDAP authentication method, see "Enable and Define the LDAP Authentication Method" on page 328.

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**.
2. In the Categories pane, locate and select the **LDAP General** category.
3. In the table, locate and select **LDAP server URL**.
4. 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`
5. Locate **Enable LDAP authentication**, and select **True**.
6. In the Categories pane, locate and select the **LDAP Group Definition** category.
7. Locate **Groups base DN** and enter the distinguished name of the general group.

8. Locate **Root groups base DN** and enter the distinguished name of the root group.
9. In the Categories pane, locate and select the **LDAP General** category.
10. Locate **Enable User Synchronization** and verify that the value is set to **True.**
11. In the Categories pane, locate and select the **LDAP General Authentication** category.
12. Locate **Password of Search-Entitled User** and fill in the password.
13. Save the new values. To replace an entry with the default value, click **Restore Default**.
14. Map LDAP user groups to UCMDB user roles. For details, see "HP Universal CMDB Login Authentication" in *HP UCMDB Administration Guide*.

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 329.

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 237.

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\j2f\JRE\bin** folder.

   b. Run the following command: Keytool -import -file <your certificate file> -keystore C:\hp\UCMDB\UCMDBServer\j2f\JRE\lib\security\cacerts. For example, Keytool -import -file c:\ca2ss_ie.cer -keystore C:\hp\UCMDB\UCMDBServer\j2f\JRE\lib\security\cacerts

2. Select **Admin** > **Settings** > **Infrastructure Settings Manager**. Select the **Foundations** context and choose **LDAP Configuration** from the list.

3. In the **LDAP Configuration - LDAP General** table, access the LDAP Server URL dialog box by clicking the **Edit** button.

4. Enter the LDAP URL 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".

5. Click **Save** to save the new value, **Restore Default** to replace the entry with the default value (a blank URL), or **Cancel** to close the dialog box without changing the value.

Reference

Using 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 JMX MBEAN View page.

3 Locate **java.lang.String 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.

26

Logging In to HP Universal CMDB

This chapter includes:

Concepts

➤ Accessing HP Universal CMDB on page 333

Tasks

➤ Log In and Log Out on page 334

➤ Automatic Login on page 336

➤ Change Default Time Limit for User Inactivity Log Out on page 337

Troubleshooting and Limitations on page 338

Concepts

Accessing HP Universal CMDB

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 *Modeling Guide*.

For details on Web browser requirements, as well as minimum requirements to successfully view HP Universal CMDB, see Chapter 2, "HP Universal CMDB Support Matrix."

Tasks

Log In and Log Out

This task explains how to log in to HP Universal CMDB from the login page. To set up an LDAP authentication method for logging in, see "HP Universal CMDB Login Authentication" on page 327

Tip: Click the **Help** button on the login page for complete login help.

Note:

- For login troubleshooting information, see "Troubleshooting and Limitations" on page 338.
- For details on setting up HP Universal CMDB for secure access, see Part VI, "Hardening HP Universal CMDB."

1 Log In

a In the Web browser, enter the URL of the HP Universal CMDB server, for example, **http://<server name or IP address>.<domain name>:8080/ucmdb** 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 338.

Note: If HP Universal CMDB is installed in a multiple customer or multiple state environment (for example, Software as a Service or Amber), a Customer field is displayed. Choose the **Customer name** from the list.

b Enter the default superuser login parameters:

- User Login=**admin**, User Password=**admin**, Customer: For UCMDB, leave empty, for HP Software-as-a-Service, enter the customer number.
- Select **Open in new window** to open the application is another browser window.
- **Remember me on this machine**: Select for an automatic login. That is, the next time you log in to UCMDB, you do not need to enter your user name and password.

c Click **Log In**. After logging in, the user name appears at the top right.

d (Recommended) Change the superuser password immediately to prevent unauthorized entry. For details on changing the password, see "Reset Password Dialog Box" in *HP UCMDB Administration Guide*.

e (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 *HP UCMDB Administration Guide*.

For details on login authentication strategies that can be used in HP Universal CMDB, see "Authentication for HP Universal CMDB Login" on page 327.

For login troubleshooting information, see "Troubleshooting and Limitations" on page 338.

Note: For details on accessing HP Universal CMDB securely, see Part VI, "Hardening HP Universal CMDB."

2 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.

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 select **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.

Troubleshooting and Limitations

Use the information below to troubleshoot possible causes of failure to log into HP Universal CMDB. For additional troubleshooting information, refer to the HP Software Self-solve knowledge base, accessed by selecting **Troubleshooting & Knowledge Base** from the HP Universal CMDB Help menu.

Problem/Possible Causes	Solutions
HP Universal CMDB is not started successfully. **Indication:** The **jboss_boot.log** file does not include the following line: ======== server is up ========	**Solution 1:** Verify that the HP Universal CMDB server is up and running by accessing the Web console **http://<server name> :8080/web-console** where <**server nam**e> is the name of the HP Universal CMDB server to which you are connecting. **Solution 2:** Check the database connection. **To check that the database server is up and running:** **1** Launch the Web browser and navigate to: **http://<server_name>:8080/jmx-console**, where <**server_name**> is the name of the machine on which HP Universal CMDB is installed. **2** Under Topaz, click **service=CMDB Dal Services** to open the JMX MBean View. **3** Invoke the function **java.lang.String getDbContext()** with a customerID parameter value of **1**. **4** Check that the operation result shows no problems. **Solution 3:** Check that the database connection parameters are correct. Ensure that you can log into Oracle Server or Microsoft SQL Server using the credentials you provided during the installation procedure.

Problem/Possible Causes	**Solutions**
HP Universal CMDB is not started successfully. *(cont'd)*	**Solution 4:** Use the log file EJBContainer\cmdb.dal_ejb.log to verify the database connections. (For details, see "CMDB Dal Log" in *Modeling Guide*.) **Solution 5:** To verify that the database connection is valid, in the Windows command interpreter (cmd.exe), type sqlplus cmdb/cmdb@skazal.
The CMDB is corrupted (for example, a user record may have been deleted accidentally from the CMDB).	Import a previously backed up database file. For details, see the *HP Universal CMDB Database Guide* PDF. **Important:** The HP Universal CMDB server must be down while importing the database. **Note:** When you import a previously backed up database file, you lose all data previously existing in the system.
The HP Universal CMDB login fails. This may be due to an incorrect login name/password combination.	Ensure that you enter a correct login user name/password combination.
HP Universal CMDB login fails due to unexpected errors.	**Solution 1**: Select **Start** > **Programs** > **HP UCMDB** > **UCMDB Server Status** and ensure that the service MAMBASIC is running. **Solution 2**: Look for errors in the following log files: ➤ **<HP Universal CMDB root directory>\UCMDBServer\j2f\log\J2F_all.ejb.log** ➤ **<HP Universal CMDB root directory>\UCMDBServer\j2f\log\mam\ucmdb_all.log** If you find errors that are unfamiliar to you, contact HP Software Support.

This section describes troubleshooting and limitations for initial login.

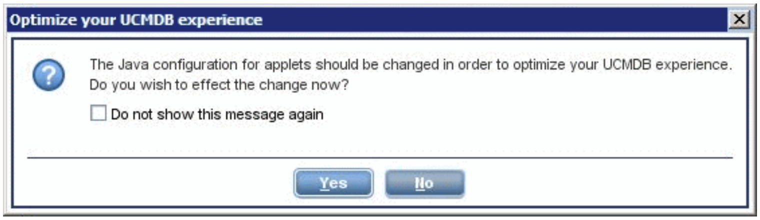
Java Not Installed on Client Machine

If Java is not installed on your machine, during login a message is displayed asking you whether to install the correct Java Runtime Environment version. JRE is needed to view HP Universal CMDB applets.

Click the relevant button to allow HP Universal CMDB to install Java from either sun.com or the HP Universal CMDB Server.

Updating the Java Configuration

The following message is displayed when HP Universal CMDB detects problems with initial memory:



Optimize your UCMDB experience

The Java configuration for applets should be changed in order to optimize your UCMDB experience.
Do you wish to effect the change now?

☐ Do not show this message again

Note: From Java version 6 update 10, this message is no longer displayed as it is no longer relevant.

27

Navigating HP Universal CMDB

This chapter includes:

Concepts

➤ Navigating the HP Universal CMDB User Interface on page 341

➤ Working with the HP Universal CMDB Documentation on page 344

Reference

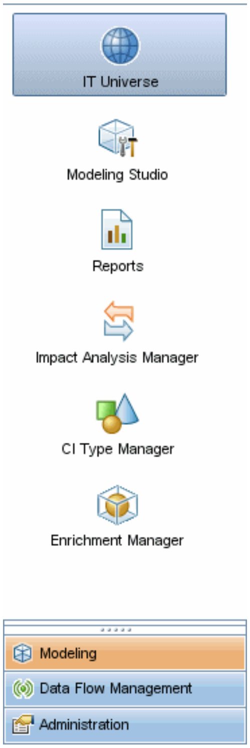
➤ Menus and Options on page 346

Concepts

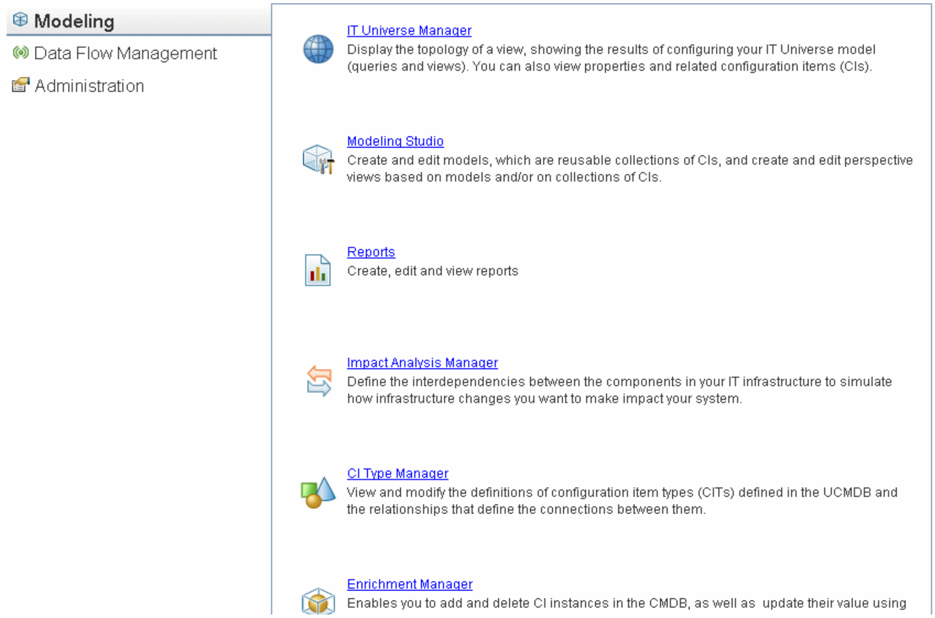
Navigating the HP Universal CMDB User Interface

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**.



Modeling

Data Flow Management

Administration

IT Universe Manager
Display the topology of a view, showing the results of configuring your IT Universe model (queries and views). You can also view properties and related configuration items (CIs).

Modeling Studio
Create and edit models, which are reusable collections of CIs, and create and edit perspective views based on models and/or on collections of CIs.

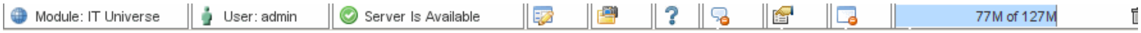
Reports
Create, edit and view reports

Impact Analysis Manager
Define the interdependencies between the components in your IT infrastructure to simulate how infrastructure changes you want to make impact your system.

CI Type Manager
View and modify the definitions of configuration item types (CITs) defined in the UCMDB and the relationships that define the connections between them.

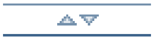
Enrichment Manager
Enables you to add and delete CI instances in the CMDB, as well as update their value using

- **Status Bar.** Provides information on the CMDB application and enables you to configure certain aspects of your interface.



Module: IT Universe | User: admin | Server Is Available | 77M of 127M

- **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.

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 is divided into the following tabs:

  - **Main Topics tab.** The Main Topics tab organizes the various guides contained in the UCMDB Help into logical sections.
  - **PDFs tab**. The PDFs tab is organized similar to the Main Topics tab, but provides links to the guides in PDF format.

- **From the Navigation pane.** To access the navigation pane if it is not being displayed, click the **Show Navigation** 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.

- **Show Navigation 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 344. 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 *Modeling Guide*.
Data Flow Management	Click to open the Data Flow Management Mapping (DFM) menu, where you set up and run the DFM process to populate the IT Universe model with configuration items (CIs). For details, see *Data Flow Management Guide*. For details on DFM content, see *Data Flow Management Guide*.
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 UCMDB 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.
- **Content Pack Help.** Describes the default, out-of-the-box content: what is being discovered, the credentials required in discovery, and how to troubleshoot the discovery results.
- **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 "HP Universal CMDB High Availability" on page 215.

28

Available Troubleshooting Resources

This chapter includes:

Troubleshooting Resources on page 349

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" in the *HP Universal CMDB Deployment Guide* PDF.
- **Login troubleshooting.** Use to troubleshoot possible causes of failure to log in to HP Universal CMDB. For details, see "Troubleshooting and Limitations" in the *HP Universal CMDB Deployment Guide* PDF.
- **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 "CMDBODB Log Files" in *HP UCMDB Administration Guide*.
- **Data Flow Management Mapping log files.** Use to troubleshoot DFM problems. For details, see "Data Flow Management Log Files" in *HP UCMDB Administration Guide*.

- **Query log files.** Use to view definitions for query parameter log files. For details, see "CMDBODB Log Files" in *HP UCMDB Administration Guide*.

29

Working in Non-English Locales

This chapter includes:

Reference

- Installation and Deployment Issues on page 352
- Database Environment Issues on page 353
- Administration Issues on page 353
- Report Issues on page 353
- Multi-Lingual User (MLU) Interface Support on page 354

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 & 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 platform. Other platforms are not supported (for example Solaris, UNIX, Linux, and so on). For details on installing HP Universal CMDB on a Windows platform, see "HP Universal CMDB Installation on a Windows Platform" on page 59.
- 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 Uprgrade Wizard for version 9.00 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 on working with Oracle databases, see "HP Universal CMDB Installation on a Solaris Platform" on page 107.
- 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 353.

Report Issues

- HP Universal CMDB does not support Custom Report names that contain more than 50 multibyte characters.
- Reports downloaded from HP Universal CMDB to Excel cannot be displayed properly on an operating system whose language differs from the data language.

  To download Excel files with multibyte data when HP Universal CMDB is installed on an English-language machine, set the **user.encoding** entry in the **C:\hp\UCMDB\UCMDBServer\j2f\AppServer\resources\G11N_Strings.properties** file to the correct encoding.

- 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 (like Japanese, Chinese, Korean) and the report is sent as an email attachment, the name becomes unreadable.
- By default, Excel does not open UTF-8 encoded CSV documents correctly. After saving a report as a .csv file, you can import it into Excel by doing the following in Excel:

  a On the **Data** menu, select **Import External Data**, and click **Import Data**.

  b In the **Files of type** box, click **Text Files.**

  c In the **Look in** box, locate and double-click the text file to be imported as an external data range.

  d To specify how to divide the text into columns, follow the instructions in the Text Import Wizard, and click **Finish**.
- When exporting a CI instance to a PDF file, multi-byte characters (such as Japanese, Chinese, Korean, and so on) are not displayed in the PDF file.
- Charts in Topology reports which were defined in a non-English locale are not displayed properly in the Reports module.

Multi-Lingual User (MLU) Interface Support

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

Language	Localized UI	Localized Materials	Availability
Korean	Yes		Part of initial product release
Simplified Chinese	Yes		Part of initial product release
Dutch	Yes		Media pack A
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 Multilingual 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 *HP UCMDB 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 *HP UCMDB 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 *HP UCMDB 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 *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 351:
  - 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.

Index

A

accessing UCMDB
 set up IIS Web server 318, 322
 through IIS web server 317
 through IIS Web server, overview 317
Advanced Edition Licensing 40
authentication
 Lightweight Single Sign-On General Reference 281
authentication methods 327
 defining for LDAP 328
 setting secure SSL 329
 setting up 328

B

basic authentication
 enabling on UCMDB Data Probe 278
Books Online 15
browser language preference 354

C

capacity planning 223
 managed hosts and host-related CIs 225
class model conflict 205
Confidential Manager 295
 credentials encryption 256
 overview 296
 security considerations 296
configuration management database (CMDB)
 introduction 24
credentials
 managing hardening 257

D

Data Flow Management
 hardening 253
Data Flow Probe
 configure for IIS 325
database
 system installation requirements 36
database installation
 configuring the UCMDB server 85
 restarting the server 96
 setting database parameters 87
deployment
 in secure architecture 234
 installation 103
 Windows server installation 59, 73
disaster recovery
 before startup cleanup procedure 311
 HP Universal CMDB 305
 installing HP Universal CMDB software in the Failover environment 307
 introduction 306
 preparing the environment 307
 preparing the HP Universal CMDB failover instance for activation 310
 system configuration backup, data configuration backup 307
Discovery
 overview 25
documentation updates 17
documentation, online 15
domainScopeDocument
 controlling location of 280
 export, import in encrypted format 265

E

encryption keys
- generating or updating 259

G

getting started 48
- administration tasks 49
- predeployment planning 45

H

hardening 231
- enabling SSL from Certification Authority 239
- enabling SSL on UCMDB Data Probe 278
- enabling SSL on UCMDB Server machine 237
- enabling SSL on Web clients 241
- example of Apache 2.0.x configuration 250
- export, import domainScopeDocument in encrypted format 265
- manage credentials storage 257
- preparations 233
- reverse proxy overview 246
- reverse proxy, security aspects 247
- reverse proxy, using 245
- secure architecture deployment 234
- SSL 237

hardware
- requirements 116

high availability 215
- installation of UCMDB 217

high availability. See the HP Universal CMDB Deployment Guide PDF

HP Software Support Web site 16

HP Software Web site 16

HP Universal CMDB
- about 22
- deployment 24
- disaster recovery 305
- getting started 45
- introduction 21
- launching 28
- overview 21
- running on VMware platform 28
- server status 51
- services 51, 53
- Start menu 315
- starting/stopping Server 99
- support matrix 31
- system architecture 23

HP Universal CMDB server
- starting, stopping on a Windows platform 315

I

I18N
- administration issues 353
- database environment issues 353
- installation and deployment issues 352
- report issues 353

IIS
- configure for Data Flow Probe 325

installation
- choosing database or schema 85
- connecting to an existing Microsoft SQL Server database 96
- connecting to an existing Oracle schema 96
- creating a Microsoft SQL Server database 90
- creating an Oracle schema 94
- deploying Microsoft SQL Server 87
- on one machine 103
- overview 26
- prerequisites for Windows 59, 73
- procedure 103
- procedure for typical deployment with Oracle Server 61, 74
- stages 27
- UCMDB Data Probe 116

J

Java
- installing during login 340

Java applets
- change memory allocation 29

JMX console
- change user name or password 235
- set password to encrypt 270

K

keys
- generating or updating encryption key 259

Knowledge Base 16

L

language preference 354

languages
- working in non-English locales 351

LDAP
- defining authentication method 328

licensing 39
- Data Flow Probe installation 41
- for HP ServiceCenter/Service Manager 41
- for HP Software-as-a-Service 40
- overview 39
- troubleshooting and limitations 43
- upgrading to standard or advanced 42

Lightweight Single Sign-On
- General Reference 281

Lightweight Single Sign-On General Reference 281

locales
- non-English 351

logging in 333
- automatic login 336
- installing Java 340
- troubleshooting 338

logging in and out 334

login
- supported browsers 333

login authentication 327

logout
- automatic with user inactivity 337

LTU 40

LW-SSO
- retrieving current configuration in distributed environment 283
- security warnings 286
- system requirements 285
- troubleshooting 288

LW-SSO Troubleshooting
- LW-SSO Related Use Cases 291
- SAML2 Related Use Cases 294

M

Mananged Server 40

memory
- allocating to processes 89

Microsoft SQL Server
- connecting to existing database 96
- creating a database 90
- deployment 87
- installation requirements 36

multi-lingual user interface support 354

MySQL
- set password to encrypt database 268

N

navigation 341
- menus and options 346
- user interface 341
- working with documentation 344

O

online documentation 15

Online Help 15

online resources 16

Oracle
- connecting to existing schema 96
- creating a schema 94
- installation requirements 36
- user schema parameters 87

OS Instance 40

P

Package Migration Utility 207

packages
- upgrading to 9.00 207

passwords
encrypt the JMX console 270
encrypt the MySQL database 268
processes
allocating memory 89

R

Readme 15
requirements
database system 36
Microsoft SQL Server 36
Oracle 36
UCMDB Data Probe 116
reverse proxy
connect UCMDB Data Probe to UCMDB server 278
overview 246
security aspects 247
using 245

S

secure architecture
deployment 234
security
hardening 231
server installation
on Windows 59, 73
services 51, 53
server status, viewing 51
starting/stopping Server 99
software
requirements 116
SSL 237
changing UCMDB Server keystore passwords 242
enabling on client SDK 242
enabling on UCMDB Data Probe 278
enabling on UCMDB Server machine 237
enabling on Web clients 241
enabling with Certification Authority 239
setting secure connection for authentication 329
Start menu 315
system requirements
VMware platform 28

T

Topology Query Language (TQL)
introduction 25
troubleshooting
logging in 338
Troubleshooting and Knowledge Base 16
troubleshooting resources 349

U

UCMDB
change service user 97
Server service 97
UCMDB client
software requirements 37
UCMDB Data Probe
connect by reverse proxy to UCMDB server 278
enabling SSL with basic authentication 278
hardening 267
hardware requirements 116
installation requirements 116
software requirements 116
UCMDB help
navigating 344
UCMDB server
hardware requirements 32
software requirements 33
supported browsers 34
virtual environments 35
UCMDB services
troubleshooting 54
uninstall
on a Windows platform 71
updates, documentation 17
upgrade
input parameters, data model, and log files 123
upgrading to version 8.00 121
user inactivity

automatic logout 337
user interface
multi-lingual support 354
navigating 341

V

VMware, running HP Universal CMDB 28

W

What's New 15
Windows
server installation 59, 73
Windows service user
change 97