



HP Universal CMDB

Software Version: 10.20

JMX Reference Guide

Document Release Date: January 2015
Software Release Date: January 2015

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 Notice

© 2002 - 2015 Hewlett-Packard Development Company, L.P.

Trademark Notices

Adobe™ is a trademark of Adobe Systems Incorporated.

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

UNIX® is a registered trademark of The Open Group.

Documentation Updates

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

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

To check for recent updates or to verify that you are using the most recent edition of a document, go to: <https://softwaresupport.hp.com/>.

This site requires that you register for an HP Passport and to sign in. To register for an HP Passport ID, click **Register** on the HP Support site or click **Create an Account** 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 site at: <https://softwaresupport.hp.com>.

This website 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 website 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 to sign in. Many also require a support contract. To register for an HP Passport ID, click **Register** on the HP Support site or click **Create an Account** on the HP Passport login page.

To find more information about access levels, go to: <https://softwaresupport.hp.com/web/softwaresupport/access-levels>.

HP Software Solutions Now accesses the HPSW Solution and Integration Portal website. This site enables you to explore HP Product Solutions to meet your business needs, includes a full list of Integrations between HP Products, as well as a listing of ITIL Processes. The URL for this website is <http://h20230.www2.hp.com/sc/solutions/index.jsp>.

Contents

Chapter 1: Introduction	6
Introduction	6
Java JMX Access Hardening	9
UCMDB JMX Methods	12
Data Flow Management JMX Methods	21
Configuration Manager JMX Methods	24
Chapter 2: Administration Methods	26
Unified Resource Manager (URM) JMX Methods	26
How to Manage UCMDB Licenses Using the JMX Console	27
How to Download a Zip File of Log Files and Thread Dumps	27
How to Retrieve UCMDB Server Logs for a Specific Time Frame	28
How to Access Support Using the JMX Console	29
How to Set Master Keys	33
How to Use the User Activity Log	37
How to Configure UCMDB Log Levels	38
How to Check the Database Connection	38
High Availability Mode JMX Methods	39
Troubleshooting	42
UCMDB Browser JMX Methods	42
Package Manager JMX Methods	46
Chapter 3: Modeling Methods	49
How to Define and View a Layout Selection for a TQL Query	49
How to Encrypt the Password of a Direct Link	50
How to Rebuild the Database in Case of an Error	50
How to Export the Class Model to XML	51

Chapter 4: Data Flow Management Methods	52
How to View Job Information on the Data Flow Probe	52
How to View Discovery Rules	62
How to View Discovery Resource History	63
How to Run Data Flow Ad Hoc Updates	65
How to Delete Unsent Probe Results	66
How to Configure Global ID Generation	67
How to Perform Initial UCMDB-UCMDB Synchronization	67
Data Flow Probe Log Files	68
How to Check XML Enricher Health Using JMX	72
How to Check the Confidential Manager Connection	73
 Chapter 5: Developer Reference Methods	 74
How to Debug Adapter Resources	74
How to Create an Integration User	74
Web Service API - executeTopologyQueryWithParameters	77
 Chapter 6: Configuration Manager Methods	 79
Configuration Manager JMX Methods	79
 Chapter 7: Hardening Methods	 83
How to Change the System User Name or Password for the JMX Console	84
How to Enable Mutual Certificate Authentication for SDK	85
How to Configure a Reverse Proxy	87
How to Change the Server Keystore Password	88
How to Enable or Disable HTTP/HTTPS Ports	89
How to Map the UCMDB Web Components to Ports	90
How to Modify the PostgreSQL Database Encrypted Password	92
How to Set the JMX Console Encrypted Password	93
How to Set the UpLoadScanFile Password	94
How to Retrieve the Current LW-SSO Configuration in a Distributed Environment	96

How to Configure LW-SSO Settings	96
How to Configure Confidential Manager Communication Encryption	97
How to Configure Confidential Manager Client Authentication and Encryption Settings on the Probe	98
How to Configure Confidential Manager Communication Encryption on the Probe	99
How to Configure the Confidential Manager Client's Cache Encryption Settings on the Probe ..	100
How to Export and Import Credential and Range Information in Encrypted Format	102
How to Generate or Update the Encryption Key for Confidential Manager	103
Generate a New Encryption Key	104
Update an Encryption Key on a UCMDB Server	105
Update an Encryption Key on a Probe	107
Manually Change the Encryption Key when the Probe Manager and Probe Gateway are Installed on Separate Machines	107
Define Several JCE Providers	108
How to Configure CAC Support on UCMDB	108
How to Configure CAC Support for UCMDB by Reverse Proxy	111
How to Harden the Data Flow Probe Connector in UCMDB	117
How to Encrypt the Probe Keystore and Truststore Passwords	118
How to Enable Login to HP Universal CMDB with LW-SSO	119
How to Test LDAP Connections	120
How to Enable and Define the LDAP Authentication Method	120
How to Configure the HP Universal CMDB Server with Confidential Manager	121
How to Set the IIS server as the Front-End Server for UCMDB	123
Chapter 8: Installation and Migration Methods	124
How to Integrate UCMDB with SiteMinder	124
How to Migrate DDMI Server Configuration Data to Universal Discovery	125
Send Documentation Feedback	130

Chapter 1: Introduction

This chapter includes:

Introduction	6
Java JMX Access Hardening	9
UCMDB JMX Methods	12
Data Flow Management JMX Methods	21
Configuration Manager JMX Methods	24

Introduction

This guide provides a reference for JMX methods included in the UCMDB documentation. Many UCMDB actions can be performed from the JMX console. You can search the JMX Quick Search page for JMX methods as described below.

Note: The methods in this guide were collected from existing documentation.

UCMDB JMX Console

1. On the UCMDB server, launch the Web browser and enter the following address:
http://localhost:8080/jmx-console.
2. Enter the JMX console authentication credentials, which by default are:
 - Login name = **sysadmin**
 - Password = **sysadmin**

The UCMDB JMX Quick Search page opens. There are three ways to access a JMX operation from the JMX home page.

- Use the JMX quick search

The JMX quick search feature provides the ability to:

- Search for a service. This is useful when you know that an operation is in a certain service category, but you do not know the name of the operation.
- Search for a JMX operation based on a keyword
 - Keywords can be an operation name, the description of the operation, or even the parameters used by the operation.
 - When typing, a suggestion list is displayed, providing links to quickly access suggested methods.
- Search and access a UCMDB server log from the JMX console
 - Typing the word **log**: in the search text displays a suggestion list with all the logs that contain the search word.
 - Clicking one of the suggested logs redirects to a new page displaying the full content of the log.
- Use the UCMDB JMX link

Do the following:

- i. Click the UCMDB JMX link to open the console.
- ii. Locate the required service and click the link to open the operations page.
- iii. Select the required operation.

- Use the JMX Operations Index link

Do the following:

- i. Click the UCMDB JMX Operations Index link to open the console operation index.
- ii. Go directly to the required method and select it.

Note: It is recommended to change the JMX password. For details, see "[Change the JMX Console Password](#)" on the next page.

Data Flow Probe JMX Console

1. On the probe machine, launch the 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**.
2. Enter the JMX console authentication credentials, which by default are:
 - Login name = **sysadmin**
 - Password = **sysadmin**


The Data Flow Probe JMX Quick Search page opens.

To search for a JMX method, enter a method name or part of a method name in the search box. The search results display all methods containing the search phrase.

3. Click the **Data Flow Probe JMX** link to open the console. Locate the required service and click the link to open the operations page. Select the required operation.
4. Click the **Data Flow Probe Operations Index** link to open the console operation index. Go directly to the required method and select it.

Note: It is recommended to change the JMX password. For details, see "[Change the JMX Console Password](#)" below.

Change the JMX Console Password

1. Log in to UCMDB with an administrator account and go to **Administration > Security > Users and Groups**.
2. Select the user for the JMX Console login (by default, **sysadmin**) and click the **Reset Password**  button.
3. In the Reset Password dialog box, enter the new password and confirm it. Click **OK**.
4. Log out of UCMDB and log in to the JMX Console using the new password.

Configuration Manager JMX Console

There is a separate JMX console for Configuration Manager.

On the Configuration Manager server, enter the following address: **http://<server name>:<application_port>/cnc/jmx-console**. The port is the port configured during the installation of Configuration Manager.

For details, see the interactive *HP Universal CMDB Deployment Guide*.

For details on accessing the Configuration Manager JMX Console, see "[Configuration Manager JMX Methods](#)" on page 79.

Java JMX Access Hardening

Note: The procedure described here can also be used for the Data Flow Probe JMX.

In order to ensure that the JMX RMI port is accessible only when providing user credentials, perform the following procedure:

1. In the **wrapper.conf** file on the server, located at **C:\hp\UCMDB\UCMDBServer\bin**, set the following:

```
wrapper.java.additional.16=-Dcom.sun.management.jmxremote.authenticate=true
```

This setting requires the JMX to ask for authentication.

- **For the Data Flow Probe JMX**, perform the following:

In the files **WrapperGateway.conf** and **WrapperManager.conf**, located at **C:\hp\UCMDB\DataFlowProbe\bin**, set the following:

```
wrapper.java.additional.17=-Dcom.sun.management.jmxremote.authenticate=true
```

2. Rename the file **jmxremote.password.template** (located at: **C:\hp\UCMDB\UCMDBServer\bin\jre\lib\management**) to **jmxremote.password**.

Note: For the Data Flow Probe JMX, this file is located at: **C:\hp\UCMDB\DataFlowProbe\bin\jre\lib\management**.

3. In **jmxremote.password**, add passwords for the roles **monitorRole** and **controlRole**.

For example:

monitorRole QED

controlRole R&D

would assign the password **QED** to **monitorRole** and the password **R&D** to **controlRole**.

Note: Ensure that only the owner has read and write permissions on **jmxremote.password** because it contains the passwords in clear text. The file owner must be the same user under which UCMDB Server is running.

4. In the file **jmxremote.access** (located at **C:\hp\UCMDB\UCMDBServer\bin\jre\lib\management**), assign access to **monitorRole** and **controlRole**.

For example:

monitorRole readonly

controlRole readwrite

would assign read-only access to **monitorRole** and read-write access to **controlRole**.

Note: For the Data Flow Probe JMX, this file is located at:
C:\hp\UCMDB\DataFlowProbe\bin\jre\lib\management.

5. Secure files as follows:

- **For Windows only:** Run the following commands from the command line to secure files:

```
icacls jmxremote.password /grant Administrator:F
```

```
icacls jmxremote.access /grant Administrator:R
```

where **<username>** is the file owner visible in the properties of both files. Open properties of these files and ensure that they are correct and have only one owner.

- **For Solaris and Linux operating systems:** Set the file permissions for the password file by

running:

chmod 600 jmxremote.password

6. **For Service Pack upgrades, Server migrations and Disaster Recovery:** Change ownership of the file **jmxremote.access** (located at **C:\hp\UCMDB\UCMDBServer\bin\jre\lib\management**) to the operating system user running the upgrade or migration installation.

Note:

- For the Data Flow Probe JMX, this file is located at:
C:\hp\UCMDB\DataFlowProbe\bin\jre\lib\management.
- Before uninstalling the product, edit the file permissions for **<UMCDB installation folder>\bin\jre\lib\management\jmxremote.password** so the user you are logged in with can edit it.

UCMDB JMX Methods

Service	Method	Link to document
Authorization Services	createUser	"How to Create an Integration User" on page 74
	grantRolesToUserForAllTenants	"How to Create an Integration User" on page 74
	grantRolesToUserForTenants	"How to Create an Integration User" on page 74
	removeUser	"How to Create an Integration User" on page 74
	resetPassword	"How to Create an Integration User" on page 74 "How to Change the System User Name or Password for the JMX Console" on page 84
	setRolesForUser	"How to Create an Integration User" on page 74
	UserAuthenticate	"How to Create an Integration User" on page 74
Class Model Services	exportClassModelToXml	"How to Export the Class Model to XML" on page 51
DAL Services	getDbContext	"How to Check the Database Connection" on page 38
	rebuildModelDBSchemaAndViews	"How to Rebuild the Database in Case of an Error" on page 50
	rebuildModelViews	"How to Rebuild the Database in Case of an Error" on page 50

Service	Method	Link to document
Discovery Manager	changeEncryptionKey	"How to Generate or Update the Encryption Key for Confidential Manager" on page 103
	changeEncryptionKey	"High Availability Mode JMX Methods" on page 39
	exportCredentialsAndRangesInformation	"How to Export and Import Credential and Range Information in Encrypted Format" on page 102
	generateEncryptionKey	"How to Generate or Update the Encryption Key for Confidential Manager" on page 103
	generateEncryptionKey	"High Availability Mode JMX Methods" on page 39
	importCredentialsAndRangesInformation	"How to Export and Import Credential and Range Information in Encrypted Format" on page 102
	importMigrationDataFromDDMI	"How to Migrate DDMI Server Configuration Data to Universal Discovery" on page 125
	recalculateAndUpdateDFMTasks	"How to Run Data Flow Ad Hoc Updates" on page 65
	recalculateAndUpdateDFMTasksForAdapter	"How to Run Data Flow Ad Hoc Updates" on page 65
High Availability Services	changeClusterAuthenticationKeystorePassword	"High Availability Mode JMX Methods" on page 39
	changeClusterEncryptionKeystorePassword	"High Availability Mode JMX Methods" on page 39

Service	Method	Link to document
LDAP Services	configureLDAP	"How to Enable and Define the LDAP Authentication Method" on page 120
	getLDAPSettings	"How to Enable and Define the LDAP Authentication Method" on page 120
	testLDAPConnection	"How to Test LDAP Connections" on page 120
	verifyLDAPCredentials	"How to Enable and Define the LDAP Authentication Method" on page 120
Licensing Services	addLicense	"How to Manage UCMDB Licenses Using the JMX Console" on page 27

Service	Method	Link to document
LW-SSO Configuration	setUserName	"How to Integrate UCMDB with SiteMinder" on page 124
	addTrustedDomains	"How to Enable Login to HP Universal CMDB with LW-SSO" on page 119
	setEnabledForUI	"How to Enable Login to HP Universal CMDB with LW-SSO" on page 119
	setDomain	"How to Enable Login to HP Universal CMDB with LW-SSO" on page 119
	addTrustedIPs	"UCMDB Browser JMX Methods" on page 42
	setValidationPointHandlerEnable	"How to Enable Login to HP Universal CMDB with LW-SSO" on page 119
	updateReverseProxy	"How to Enable Login to HP Universal CMDB with LW-SSO" on page 119
	setReverseProxyIPs	"How to Enable Login to HP Universal CMDB with LW-SSO" on page 119
	retrieveConfigurationFromSettings	"How to Enable Login to HP Universal CMDB with LW-SSO" on page 119
	retrieveConfiguration	"How to Enable Login to HP Universal CMDB with LW-SSO" on page 119
	setInitString	"How to Configure LW-SSO Settings" on page 96 "How to Enable Login to HP Universal CMDB with LW-SSO" on page 119

Service	Method	Link to document
Multiple CMDB Instances Services	fetchAllDataFromAnotherCMDB	"How to Perform Initial UCMDB-UCMDB Synchronization " on page 67
	getGlobalIdGeneratorScopes	"How to Configure Global ID Generation" on page 67
	setAsGlobalIdGenerator	"How to Configure Global ID Generation" on page 67
	setAsGlobalIdGeneratorForScopes	"How to Configure Global ID Generation" on page 67
	setAsNonGlobalIdGenerator	"How to Configure Global ID Generation" on page 67
Packaging Services	deployPackages	"Package Manager JMX Methods" on page 46
	displayDeployedPackages	"Package Manager JMX Methods" on page 46
	displayResourcesDeploymentHistory	"Package Manager JMX Methods" on page 46
	exportPacakges	"Package Manager JMX Methods" on page 46
	undeployPacakges	"Package Manager JMX Methods" on page 46

Service	Method	Link to document
Ports Management Services	ComponentsConfigurations	"How to Map the UCMDB Web Components to Ports" on page 90 "How to Configure CAC Support on UCMDB" on page 108 "How to Configure CAC Support for UCMDB by Reverse Proxy" on page 111
	HTTPSClientAuthSetEnable	"How to Enable or Disable HTTP/HTTPS Ports" on page 89
	HTTPSClientAuthSetPort	"How to Map the UCMDB Web Components to Ports" on page 90
	HTTPSetEnable	"How to Enable or Disable HTTP/HTTPS Ports" on page 89
	HTTPSetPort	"How to Map the UCMDB Web Components to Ports" on page 90
	HTTPSSetEnable	"How to Enable or Disable HTTP/HTTPS Ports" on page 89
	HTTPSSetPort	"How to Map the UCMDB Web Components to Ports" on page 90
	mapComponentToConnectors	"How to Map the UCMDB Web Components to Ports" on page 90 "How to Configure CAC Support on UCMDB" on page 108 "How to Configure CAC Support for UCMDB by Reverse Proxy" on page 111 "How to Harden the Data Flow Probe Connector in UCMDB" on page 117
	PortsDetails	"How to Enable Mutual Certificate Authentication for SDK" on page 85 "How to Harden the Data Flow Probe Connector in UCMDB" on page 117

Service	Method	Link to document
	serverComponentsNames	"How to Map the UCMDB Web Components to Ports" on page 90

Service	Method	Link to document
Security Services	changeKeystorePassword	"How to Change the Server Keystore Password" on page 88
	changeMasterKeyForCluster	"How to Set Master Keys" on page 33
	CMAddUser	"How to Configure the HP Universal CMDB Server with Confidential Manager" on page 121
	CMGetConfiguration	"How to Configure Confidential Manager Communication Encryption " on page 97 "How to Configure the HP Universal CMDB Server with Confidential Manager" on page 121
	CMSetConfiguration	"How to Configure Confidential Manager Communication Encryption " on page 97 "How to Configure the HP Universal CMDB Server with Confidential Manager" on page 121
	loginWithCAC	"How to Configure CAC Support on UCMDDB" on page 108 "How to Configure CAC Support for UCMDDB by Reverse Proxy" on page 111
	onlyCACCert	"How to Configure CAC Support on UCMDDB" on page 108 "How to Configure CAC Support for UCMDDB by Reverse Proxy" on page 111
	pathToCRL	"How to Configure CAC Support on UCMDDB" on page 108
	retrieveLWSSOConfiguration	"How to Retrieve the Current LW-SSO Configuration in a Distributed Environment" on page 96

Service	Method	Link to document
	usernameField	"How to Configure CAC Support on UCMDB" on page 108
	withReverseProxy	"How to Configure CAC Support for UCMDB by Reverse Proxy" on page 111
Server Services	executeLogGrabber	"How to Download a Zip File of Log Files and Thread Dumps" on page 27
	loggersLevels	"How to Use the User Activity Log" on page 37 "How to Configure UCMDB Log Levels" on page 38
Settings Services	getSettingDefaultValue	"UCMDB Browser JMX Methods" on page 42
	setSettingValue	"How to Use the User Activity Log" on page 37 "UCMDB Browser JMX Methods" on page 42
	showSettingsByCategory	"How to Use the User Activity Log" on page 37
Supportability Services	listSupportCategories	"How to Access Support Using the JMX Console" on page 29
	runSupportHandlersForAllCategories	"How to Access Support Using the JMX Console" on page 29
	runSupportHandlersForSpecificCategories	"How to Access Support Using the JMX Console" on page 29
	selectAndRunSupportHandlers	"How to Access Support Using the JMX Console" on page 29
Topology Search Services	debugSolrQuery	"UCMDB Browser JMX Methods" on page 42
	restoreFactoryDefaults	"UCMDB Browser JMX Methods" on page 42

Service	Method	Link to document
TQL Services	calculateTqlAdHoc	"How to Define and View a Layout Selection for a TQL Query" on page 49
	exportTQL	"Web Service API - executeTopologyQueryWithParameters " on page 77
UCMDB Integration	getEncryptedPasswordForURL	"How to Encrypt the Password of a Direct Link" on page 50
	setCMDBSuperIntegrationUser	"How to Create an Integration User" on page 74
UI Server frontend settings	setUseFrontendURLBySettings	"How to Configure a Reverse Proxy" on page 87 "How to Set the IIS server as the Front-End Server for UCMDB" on page 123
	showFrontendURLInSettings	"How to Configure a Reverse Proxy" on page 87
URM Services	listResourceTypes	"UCMDB Browser JMX Methods" on page 42 "How to View Discovery Resource History" on page 63

Data Flow Management JMX Methods

Service	Method	Link to document
CMClient	displayCacheConfiguration	"How to Configure the Confidential Manager Client's Cache Encryption Settings on the Probe" on page 100
	isCMClientInitialized	"How to Check the Confidential Manager Connection" on page 73

Service	Method	Link to document
	setCacheEncryptionAlgorithm	"How to Configure the Confidential Manager Client's Cache Encryption Settings on the Probe" on page 100
	setCacheEncryptionLibrary	"How to Configure the Confidential Manager Client's Cache Encryption Settings on the Probe" on page 100
	setCacheInitString	"How to Configure the Confidential Manager Client's Cache Encryption Settings on the Probe" on page 100
	setCacheMacDetails	"How to Configure the Confidential Manager Client's Cache Encryption Settings on the Probe" on page 100
	setLWSSOInitString	"How to Configure Confidential Manager Client Authentication and Encryption Settings on the Probe" on page 98
	setTransportEncryptionAlgorithm	"How to Configure Confidential Manager Communication Encryption on the Probe" on page 99
	setTransportEncryptionLibrary	"How to Configure Confidential Manager Communication Encryption on the Probe" on page 99
	setTransportInitString	"How to Configure Confidential Manager Communication Encryption on the Probe" on page 99
	setTransportMacDetails	"How to Configure Confidential Manager Communication Encryption on the Probe" on page 99
GeneralUtils	executeLogGrabber	"Data Flow Probe Log Files" on page 68
JobsInformation	activateJob	"How to View Job Information on the Data Flow Probe" on page 52
	activateJobOnDestination	"How to View Job Information on the Data Flow Probe" on page 52

Service	Method	Link to document
	start/stop	"How to View Job Information on the Data Flow Probe" on page 52
	viewJobErrorsSummary	"How to View Job Information on the Data Flow Probe" on page 52
	viewJobExecHistory	"How to View Job Information on the Data Flow Probe" on page 52
	viewJobProblems	"How to View Job Information on the Data Flow Probe" on page 52
	viewJobResultCilInstances	"How to View Job Information on the Data Flow Probe" on page 52
	viewJobResults	"How to View Job Information on the Data Flow Probe" on page 52
	viewJobsStatuses	"How to View Job Information on the Data Flow Probe" on page 52
	viewJobStatus	"How to View Job Information on the Data Flow Probe" on page 52
	viewJobTriggeredCIs	"How to View Job Information on the Data Flow Probe" on page 52
	viewJobTriggeredCIsWithErrorId	"How to View Job Information on the Data Flow Probe" on page 52
MainProbe	dropUnsentResults	"How to Delete Unsent Probe Results " on page 66
	getEncryptedDBPassword	"How to Modify the PostgreSQL Database Encrypted Password" on page 92
	getEncryptedKeyPassword	"How to Set the JMX Console Encrypted Password" on page 93 "How to Set the UpLoadScanFile Password" on page 94 "How to Encrypt the Probe Keystore and Truststore Passwords" on page 118

Service	Method	Link to document
NormalizationRuleBase	scanForScanFileRules	"How to View Discovery Rules" on page 62
	scanForSNMPRules	"How to View Discovery Rules" on page 62
	viewNormalizationRuleById	"How to View Discovery Rules" on page 62
	viewNormalizationRuleByNicId	"How to View Discovery Rules" on page 62
	viewNormalizationRules	"How to View Discovery Rules" on page 62
SecurityManagerService	importEncryptionKey	"How to Generate or Update the Encryption Key for Confidential Manager" on page 103
XmlEnricherMonitor	viewXmlEnricherStatuses	"How to Check XML Enricher Health Using JMX" on page 72

Configuration Manager JMX Methods

Service	Method	Link to document
ImportExport Service	activateAutoManageResource	"Configuration Manager JMX Methods" on page 79
	exportData	"Configuration Manager JMX Methods" on page 79
	exportPolicies	"Configuration Manager JMX Methods" on page 79
	exportViews	"Configuration Manager JMX Methods" on page 79
	importData	"Configuration Manager JMX Methods" on page 79
	listAllPolicies	"Configuration Manager JMX Methods" on page 79

Service	Method	Link to document
	listAllViews	"Configuration Manager JMX Methods" on page 79
Licensed Content Service	deactivateAutomanagedResources	"Configuration Manager JMX Methods" on page 79
View Service	supportLargeViews	"Configuration Manager JMX Methods" on page 79
	updateFoldingRules	"Configuration Manager JMX Methods" on page 79

Chapter 2: Administration Methods

This chapter includes:

Unified Resource Manager (URM) JMX Methods	26
How to Manage UCMDB Licenses Using the JMX Console	27
How to Download a Zip File of Log Files and Thread Dumps	27
How to Retrieve UCMDB Server Logs for a Specific Time Frame	28
How to Access Support Using the JMX Console	29
How to Set Master Keys	33
How to Use the User Activity Log	37
How to Configure UCMDB Log Levels	38
How to Check the Database Connection	38
High Availability Mode JMX Methods	39
Troubleshooting	42
UCMDB Browser JMX Methods	42
Package Manager JMX Methods	46

Unified Resource Manager (URM) JMX Methods

The Unified Resource Manager (URM) is an XML-based repository for CMDB resources. A resource is defined as all CMDB data other than CIs. Examples of resources include TQL queries, views, users, and the class model, as well as discovery resources such as discovery scripts, integration and discovery adapters, discovery jobs, and so on.

The URM can be accessed using the JMX console only. From the JMX console page, click **UCMDB:service=URM Services** to open the JMX page with the relevant methods.

For more information, see *How to View Discovery Resource History in the HP Universal CMDB Data Flow Management Guide*.

Caution: Never change a resource from the URM.

How to Manage UCMDB Licenses Using the JMX Console

You can manage the product licenses from the JMX Console. This task describes how to install a license.

1. On the UCMDB server, launch the Web browser and enter the following address:
http://localhost:8080/jmx-console

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

2. Click **UCMDB:service=Licensing Services** to open the JMX MBEAN View page.
3. Locate the **addLicense** method.
4. Enter your customer ID and the license key.
5. Click **Invoke**.

There are additional JMX methods available on the same page for the following functions:

- Installing a license from a file
- Displaying all active licenses
- Displaying all licenses (including expired licenses)
- Displaying a summary of active licenses
- Removing all licenses

How to Download a Zip File of Log Files and Thread Dumps

You can produce a zip file that includes all logs and thread dumps. You create the file either through a JMX operation on the client machine, or by running a batch file on the UCMDB Server.

Thread dumps are created periodically: Once a minute, a thread dump snapshot is taken and is saved to a new file in the **C:\hp\UCMDB\UCMDBServer\runtime\log\threadDumps** folder. Thread dump files from

the last hour are kept. This folder also holds the ad hoc Server snapshots that are generated during the **logGrabber** execution.

To generate the zip file from the client machine:

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=Server services** to open the JMX MBEAN View page.
3. Locate the **executeLogGrabber** operation.
4. Click **Invoke**.

A Server snapshot file with the name **LogGrabber_serverSnapshot_<current date and time>.txt** is created in the following location:

C:\hp\UCMDB\UCMDBServer\runtime\log\threadDumps. This is a thread dump that includes the threads of the Server framework only.

5. In the File Download dialog box, you can open the **logGrabber_<current time>.zip** file, or download it to the client machine.

To generate the zip file from the UCMDB Server:

1. Access the following folder on the UCMDB Server: **C:\hp\UCMDB\UCMDBServer\tools\logGrabber**.
2. Run the **logGrabber.bat** file.

The **LogGrabber_<current time>.zip** file is created in the following location:

C:\hp\UCMDB\UCMDBServer\runtime. This is a thread dump that includes the threads of the Server framework only.

How to Retrieve UCMDB Server Logs for a Specific Time Frame

You can produce a zip file containing all UCMDB server logs for a given time frame. This is intended for support engineers or other users who need to obtain logs for a specific time frame.

To generate the zip file from the client machine:

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=Server services** to open the JMX MBEAN View page.
3. Locate the **executeServerLogParser** operation.
4. Enter the start time in the required format.
5. (Optional.) Enter an end time. If you do not provide an end time, the time that the JMX method is invoked is used.
6. Click **Invoke**.

When the process has finished, the file can be downloaded from the browser.

Limitations

- The zip file is also located on the UCMDB server machine as the **c:\hp\UCMDB\UCMDBServer\runtime\ParsedLogGrabber_<time>.zip** file. For maintenance purposes, this file must be manually deleted.
- The folder **c:\hp\UCMDB\UCMDBServer\runtime\log\ParsedLogs_<date>** is also created and contains the unzipped contents. For maintenance purposes, this file must be manually deleted.
- In high availability UCMDB deployments, this JMX method is running against one server only.
- Only logs from the same date can be parsed.

How to Access Support Using the JMX Console

HP Universal CMDB provides Supportability JMX methods to help HP Software Support diagnose problems in your system. The methods use handlers for each category, which gather information relevant to that category from your system. When you run a handler for a category, it downloads a zip file of the information gathered for that category. Generally, HP Software Support runs the Supportability methods to help provide a solution for the issue raised.

To access the Supportability methods:

1. On the UCMDB server, launch the Web browser and enter the following address:
http://localhost:8080/jmx-console

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

2. Click **UCMDB:service=Supportability Services** to open the JMX MBEAN View page.
3. The **listSupportCategories** method displays all the support categories:
 - To run all the handlers, invoke the **runSupportHandlersForAllCategories** method.
 - To run specific handlers, invoke the **selectAndRunSupportHandlers** method and select the handlers you want to run.
 - Alternatively, you can run specific handlers using the **runSupportHandlersForSpecificCategories** method. In the **categories** field, enter all the required handlers separated by commas, and click **Invoke**.

Supportability Handlers

The following handlers are available:

- **TQL.** Records the following data in the **TQL.properties** file:
 - Number of TQL queries
 - Number of active TQL queries
 - Number of active persistent TQL queries
 - Number of non-active TQL queries
 - It also creates the **Failed TQLs.txt** file, containing the list of failed active TQL queries
- **View.** Records the following data in the **View.properties** file:
 - Number of views
 - Number of views with a hierarchy definition
 - Number of views with a rule based hierarchy definition

- Number of template based views
- Number of perspective based views
- Number of templates
- Number of perspectives
- Number of views of unknown type (this value should always be 0)
- **ViewArchive.** Records the following data in the **ViewArchive.properties** file:
 - Total number of archives
 - Total number of views with archives
- **Snapshots.** Records the following data in the **Snapshots.properties** file:
 - Total number of snapshots
- **Modeling.** Records the following data in the **Modeling.properties** file:
 - Number of business CIs
 - Number of models with content (models containing CIs)
 - Number of pattern based models
 - Number of instance based models
- **Enrichment.** Records the following data in the **Enrichment.properties** file:
 - Number of Enrichment rules
 - Number of all active Enrichment rules
 - Number of non-active Enrichment rules
 - Number of Enrichment business views
 - Number of all active Enrichment business views
 - Number of non-active Enrichment business views
- **High Availability.** Gathers the High Availability information from all of the servers in the cluster:

- The High Availability cluster information is recorded in **HA.properties**:
 - **Is_ha_enabled**
 - Cluster name (if high availability is enabled)
 - Cluster nodes number (if high availability is enabled)
 - Cluster nodes names (if high availability is enabled)
- The values for the High Availability settings (starting with **ha.**) are recorded in **HA settings.properties**
- **Domains.** Gathers IP range information and records in the **DomainsConfiguration Customer <CustomerID>.xml** file.
- **Management Zones.** Gathers rank, name, range definition, discovery activities, activity jobs, and scheduling information for management zones. Records this information in the **MngZonesConfiguration <CustomerID>.xml** file.
- **URM Counters.** Records each of the registered URM types and the number of instances of each one in the **Basic URM Counters.properties** file.
- **Settings.** Records the infrastructure settings and their values for this customer in the **Settings <customer ID>.properties** file.
- **Changed Settings.** Records the changed infrastructure settings and their values for this customer in the **Changed_Settings_<customer ID>.properties** file.
- **Authorization.** Records all the roles, users, user groups and role assignments in the **Authorization.properties** file. In a multi-tenancy environment, it records the tenant association of each role assignment.
- **Basic History.** Records the last date that the baseline process ran for each CI type in the **Basic History.properties** file.
- **History.** Records the number of history events in the current history table for each CI type in the **History.properties** file (only for CI types with history events)
- **Class Model.** Records the class model as an XML file, **Class Model.xml**. In a multi-customer environment, it records the number of different class models and their differences at the SDK level in the **Class Model.properties** file. (In a single-customer environment, this file contains only the

information for the single customer.)

- **Model Update.** Records the following data in the **Basic Model Update.properties** file:
 - Number of CIs per CI type (only for CIs with instances)
 - Number of CIs connected to a **Node** CI type or one of its descendants
- **Data In.** Records actual deletion period and deletion candidate period information of the root CI type that was overwritten by the settings for child CI types in the **Data In.properties** file. It also checks for inconsistency in the database (objects or links that exist in the root CIT's table but not in the subtype's table or the other way around). The inconsistent objects are recorded in the **inconsistencyInModel.txt** file and the inconsistent links are recorded in the **inconsistencyLinks.txt** file.

How to Set Master Keys

You can use the JMX console to change the master key that is used to encrypt all UCMDB keys.

Change the master key for a cluster

This method assumes that your UCMDB environment is deployed in a high-availability setup.

Caution:

- This method involves a restart of the entire cluster, so plan accordingly. It is recommended to change the master key of the cluster when there is little or no load on the servers. For example, you should avoid using this method during data-in operations.
- Do not change any settings in the time period between changing the master key and restarting the server. Not following this instruction may result in a failure to start the server.
- Machines that are not up or that will be added later to the cluster will need to be configured manually. Until they are configured, at most they can run as reader machines; trying to run them as writer machines will fail.

1. Back up the **c:\hp\UCMDB\UCMDBServer\conf\cmdb.conf** file and the values for the following settings:

- `ha.cluster.authentication.keystore.password`
 - `ha.cluster.authentication.shared.secret`
 - `ha.cluster.message.encryption.keystore.password`
 - `ssl.server.keystore.password`
 - `ssl.server.truststore.password`
2. Make sure all the servers in the cluster are up and running.
 3. On the writer machine, launch the Web browser and enter the following address to log in to the JMX console: **`http://localhost:8080/jmx-console`**.

Note: If a load balancer is present, you must bypass it and not log on to the writer machine through a load balancer.

4. Do one of the following:
 - Search for **`changeMasterKeyForCluster`**.
 - Click **UCMDB:service=Security Services > `changeMasterKeyForCluster`**.
5. Enter and confirm the master key, and click **Invoke**. The master key will be changed first on the writer machine and then on all reader machines.
6. Restart all the machines in the cluster. You can use the JMX method **High Availability Services > `restartCluster`** to do this.

Note: Restart the cluster immediately after changing the master key. If you do not, future database connections may fail.

Change the master key for a new machine in a cluster

If at least one of the following settings was changed, use Method A; otherwise, use Method B:

- `ha.cluster.authentication.keystore.password`
- `ha.cluster.authentication.shared.secret`

- `ha.cluster.message.encryption.keystore.password`
- `ssl.server.keystore.password`
- `ssl.server.truststore.password`

Method A

This method assumes that you already have properly configured a master key for the writer machine that is up and running in the cluster. If not, follow the instructions in ["Change the master key for a cluster" on page 33](#).

1. Copy the `c:\hp\UCMDB\UCMDBServer\bin\wrapper.conf` file from the writer machine to the same location on the new (reader) machine.
2. Restart the server.

Method B

1. Back up the `c:\hp\UCMDB\UCMDBServer\conf\cmdb.conf` file.
2. On the writer machine, launch the Web browser and enter the following address to log in to the JMX console: `http://localhost:8080/jmx-console`.
3. Do one of the following:
 - Search for `changeMasterKey`.
 - Click `UCMDB:service=Security Services > changeMasterKey`.
4. Enter and confirm the master key, and click `Invoke`.
5. Restart the machine.

Note: Restart the cluster immediately after changing the master key. If you do not, future database connections may fail.

Revert the master key for a cluster to its default value

This procedure resets the master key for an entire cluster.

1. Make sure all the servers in the cluster are up and running.
2. On the writer machine, launch the Web browser and enter the following address to log in to the JMX console: **http://localhost:8080/jmx-console**.

Note: If a load balancer is present, you must bypass it and not log on to the writer machine through a load balancer.

3. Do one of the following:
 - Search for **restoreMasterKeyForCluster**.
 - Click **UCMDB:service=Security Services > restoreMasterKeyForCluster**.
4. Click **Invoke**. The master key will be changed first on the writer machine and then on all reader machines.
5. Restart all the machines in the cluster. You can use the JMX method **High Availability Services > restartCluster** to do this.

Note: Restart the cluster immediately after changing the master key. If you do not, future database connections may fail.

Revert the master key for a machine that was down when master key was reverted for whole cluster

1. Back up the **c:\hp\UCMDB\UCMDBServer\conf\cmdb.conf** file.
2. On the writer machine, launch the Web browser and enter the following address to log in to the JMX console: **http://localhost:8080/jmx-console**.
3. Do one of the following:
 - Search for **restoreMasterKey**.
 - Click **UCMDB:service=Security Services > restoreMasterKey**.
4. Click **Invoke**.

5. Restart the machine.

Note: Restart the cluster immediately after changing the master key. If you do not, future database connections may fail.

How to Use the User Activity Log

When troubleshooting a problem in your system, another useful tool is the User Activity log. When activated, this log records all the actions performed on your system, enabling HP Software Support to reproduce the problem and troubleshoot it.

To activate the User Activity log, first verify that it is enabled:

1. On the UCMDDB server, launch the Web browser and enter the following address:
http://localhost:8080/jmx-console

You may have to log in with a user name and password.
2. Click **UCMDDB:service=Settings Services** to open the JMX MBEAN View page.
3. Locate the **showSettingsByCategory** method.
4. Enter General Settings as the category name and click **Invoke**.
5. Locate the **mam.web.user.activity.log.enabled** setting and verify that it is set to **true**.
6. If it is set to false, go back to the **Settings Services** page, and select the **setSettingValue** method.
7. Enter **mam.web.user.activity.log.enabled** as the setting and **true** as the value and click **Invoke**.

Next, change the log level to INFO:

1. In the JMX Console, click **UCMDDB:service=Server Services**
2. Locate the **loggersLevels** method and click **Invoke**.
3. Locate the **com.hp.ucmdb.uiserver.aspects** logger and select **INFO** from the drop-down list.
4. Click **Update loggers**.

The log is now activated. Perform the actions that led to the problem. The User Activity log automatically records them.

When you are finished, disable the log using the **loggersLevels** method and selecting **ERROR** as the level for the **com.hp.ucmdb.uiserver.aspects** logger.

How to Configure UCMDB Log Levels

This task describes how to specify the log level for UCMDB log files.

1. On the UCMDB server, launch the Web browser and enter the following address:
http://localhost:8080/jmx-console

You may have to log in with a user name and password.
2. Click **UCMDB:service=Server Services** to open the JMX MBean View page.
3. Locate the **loggersLevels** method.
4. Click **Invoke**.
5. From the list next to each log file name for which you want to set the level, select the required log level (OFF, FATAL, ERROR, WARN, INFO, DEBUG, TRACE, or ALL).
6. Click **Update loggers**.

How to 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 **UCMDB**, click **UCMDB:service=Dal Services** to open the JMX MBean View.
3. Invoke the function **getDbContext** with a **customerID** parameter value of **1**.
4. Check that the operation result shows no problems.

High Availability Mode JMX Methods

Replace the Writer Server

In the JMX Console, you can invoke the **High Availability Services > suggestNewWriterServer** method where you can suggest which server (serverID) should replace the Writer server.

High Availability Cluster Authentication

To enable cluster authentication:

1. In UCMDB, go to **Administration > Infrastructure Settings Manager**.
2. Find the setting **Enable joining High Availability cluster authentication** and set it to **true**.
3. Provide a single server authentication keystore (certificate + private and public keys) in JKS format. This keystore will be placed on all the servers and used for authenticating when connecting to a high availability cluster.

Place the keystore in the following location: **<UCMDB installation folder>\conf\security** and name it **cluster.authentication.keystore**.

Note: The UCMDB comes with this keystore pre-configured out-of-the-box. This keystore is the same for all clean UCMDB installations, and thus not secure. If you wish to securely authenticate join requests, delete this file and create a new one.

4. Generate a cluster authentication keystore as follows:
 - a. From C:\hp\UCMDB\UCMDBServer\bin\jre\bin, run the following command:

```
keytool -genkey -alias hpcert -keystore <UCMDB installation folder>\conf\security\cluster.authentication.keystore -keyalg RSA
```

The console dialog box opens and asks you for a new keystore password.
 - b. The default password is **hppass**. If you want to use a different password, update the server by running the following JMX method: **UCMDB:service=High Availability Services:changeClusterAuthenticationKeystorePassword**

- c. In the console dialog box, answer the question **What is your first and last name?** by entering the name of the cluster.
- d. Enter the other parameters according to your organization's details.
- e. Enter a key password. The key password must be the same as the keystore password.

A JKS keystore is created in **<UCMDB installation folder>\conf\security\cluster.authentication.keystore**

5. Replace the old **<UCMDB installation folder>\conf\security\cluster.authentication.keystore** on all the servers in the cluster with the new keystore.
6. Restart all the servers in the cluster.

Changing the Key in the key.bin

In a High Availability environment with several servers, change the **key** in the **key.bin** as follows:

1. Go to the writer machine in the JMX. You can choose any machine in the cluster and click on the **writer** link on the top of each page.
2. In the UCMDB section of the console, click **UCMDB:service=Discovery Manager**.
3. Change the key in one of the following ways:
 - Click **changeEncryptionKey** (this imports the existing encryption key)
 - Click **generateEncryptionKey** (this generates a random encryption key)
4. On the writer machine, go to the file system and find the **key.bin** at:
C:\hp\UCMDB\UCMDBServer\conf\discovery\key.bin
5. Copy the **key.bin** from the location on the writer machine to each one of other machines in the cluster to the folder: **C:\hp\UCMDB\UCMDBServer\conf\discovery\customer_1** and rename the destination file (for example, **key_new.bin**).
6. For each of the other servers (readers) do the following:
 - a. Switch the reader to be a writer (you can do this from the High Availability JMX) and wait until it changes.
 - b. Connect to the JMX of the current writer and click **UCMDB:service=Discovery Manager**.

- c. Click and invoke **changeEncryptionKey**, use the same details you entered in step 3 (for **newKeyFileName**, use the new name you assigned at step 5).
- d. Verify that you get the following message: **Key was created successfully**.

High Availability Cluster Message Encryption

Use cluster message encryption to encrypt all the messages in the cluster.

To enable cluster message encryption:

1. In UCMDB, go to **Administration>Infrastructure Settings Manager**.
2. Find the setting **Enable High Availability cluster communication encryption** and set it to **true**.
3. Provide a secret key for symmetric encryption on all the servers. The key should be placed in a keystore of type JCEKS in the following location **<UCMDB installation folder>\conf\security\cluster.encryption.keystore**.

Note: The UCMDB comes with this keystore pre-configured out of the box. This keystore is the same for all clean UCMDB installations, and thus not secure. If you wish to securely encrypt cluster messages, please delete this file, and create a new one by following this procedure.

4. From **<UCMDB installation folder>\bin\jre\bin**, run the following command:

```
Keytool -genseckey -alias hpcert -keystore <UCMDB installation folder>\conf\security\cluster.encryption.keystore -storetype JCEKS
```

5. You will be asked for the new keystore password. The default password is "hppass". If you want to use a different password, you need to update the server by running the following JMX method:

```
UCMDB:service=High Availability Services: changeClusterEncryptionKeystorePassword
```

6. Replace the old **<UCMDB installation folder>\conf\security\cluster.encryption.keystore** of all the servers in the cluster with this new keystore.
7. Restart the servers.

Troubleshooting

Upon every startup of the server, the server sends a test message to the cluster to verify if it successfully connected to the cluster. If there is a problem with the connection, the message fails and the server is stopped to avoid the whole cluster getting stuck.

Some examples of wrong cluster encryption configuration are:

- Disabled encryption on one node when another node enabled it.
- Wrong or missing cluster.encryption.keystore
- Wrong or missing key in the keystore

If the server gets stuck because of a configuration issue, the error message is:

```
2012-09-11 17:48:23,584 [Thread-14] FATAL - ##### Server failed to connect properly  
to the cluster and its service is stopped! Please fix the problem and start it  
again #####
```

```
2012-09-11 17:48:23,586 [Thread-14] FATAL - Potential problems can be: wrong  
security configuration (wrong or missing cluster.encryption.keystore, wrong key,  
disabled encryption in a cluster with enabled encryption)
```

UCMDB Browser JMX Methods

How to Modify the Currently Indexed List

1. Go to **JMX Console > UCMDB:service=Topology Search Services**.
2. Choose one or more of the following operations:
 - editIndexerConfiguration – displays and enables editing of the **Search_Indexer_Configuration_XML** file.
 - editParserConfiguration – displays and enables editing of the **Search_Parser_Configuration_XML** file.
 - editRankingConfiguration – displays and enables editing of the **Search_Ranking_Configuration_XML** file.

3. For each operation, enter the relevant customer ID and click **Invoke**.

How to Enable/Disable the Search Engine

By default, the search engine is enabled (unless it was disabled during UCMDB installation).

To change the enable/disable setting:

1. Go to **JMX Console > UCMDB:service=Settings Services > setSettingValue**.
2. In the name field enter **cmdb.search.enabled**.
3. In the value field enter:

true: If you want the search enabled.

false: If you want the search disabled.
4. Click **Invoke**.
5. Restart the UCMDB server.

Note: If you disable the Enhanced Search Engine, the UCMDB Browser automatically reverts to the legacy search engine.

How to Enable/Disable Searching for Federated Data

The search engine can be configured to perform searches on federated data. By default, it is disabled.

To enable or disable this setting:

1. Go to **JMX Console > UCMDB:service=Settings Services > setSettingValue**.
2. In the name field enter **cmdb.federation.search.enabled**.
3. In the value field enter:

true: If you want to enable searching federated data.

false: If you want to disable searching federated data.
4. Click **Invoke**.
5. Restart the UCMDB server.

How to Configure Repetition of the Enriching Mechanism

To configure the number of times that enriching is performed on search results:

1. Go to **JMX Console > UCMDB:service=Settings Services > setSettingValue**.
2. In the name field enter **cmdb.search.enriching.depth**.
3. In the value field enter the number of times that you want enriching to be repeated on search results.
4. Click **Invoke**.
5. Restart the UCMDB server.

How to Configure the Date Format

The search engine supports two dates formats: day-month-year (DMY) and month-day-year (MDY), which can be configured as follows:

1. Go to **JMX Console > UCMDB:service=Settings Services > setSettingValue**.
2. In the **name** field enter: **cmdb.search.date.format**.
3. In the **value** field enter the desired date format: **DMY**, **MDY**, or **both**.
4. Click **Invoke**.
5. Restart the UCMDB server.

How to Restore Factory Defaults

To restore the default configuration XML files from the factory content, go to **JMX Console > UCMDB:service=Topology Search Services** and invoke the **restoreFactoryDefaults()** method.

Caution: This method overwrites the current configuration. You should back up the configuration files before invoking it.

Content of Solr Database

The Solr search engine is embedded inside UCMDB server. To query it directly, go to **JMX Console > UCMDB:service=Topology Search Services** and invoke the **debugSolrQuery()** method.

How to Access the UCMDB Browser by IP Address

If you access the UCMDB Browser by IP address (not by FQDN), you should add the UCMDB Browser IP address to the UCMDB's trusted hosts. You can do this from the JMX console. Under **LW-SSO Configuration Management**, locate the **addTrustedIPs** method and invoke it using the UCMDB Browser IP address value.

How to Specify Persistency Values for Notifications

The length of time that notifications are retained and how often they are generated are defined in the JMX console:

1. Go to **JMX Console > UCMDB:service=Settings Services > setSettingValue**.
2. To change each setting, follow these steps:
 - a. In the **name** field, enter one of the strings listed below:
 - `tql.tracker.queue.evaluation.initial.delay.in.min` - the initial delay (in minutes) after startup, before a TQL query is calculated.
 - `tql.tracker.queue.evaluation.period.in.min` - the interval (in minutes) of how often a TQL query is scheduled to run.
 - `tql.tracker.queue.max.single.run.time.in.min` - the maximum length of time (in minutes) for the system to work on calculating changes on CIs or TQL queries during a single execution.
 - `tql.tracker.min.time.between.tracker.runs.in.min` - the minimum length of time between two runs of a TQL query.
 - b. In the **value** field, enter the value you want to set.
 - c. Click **Invoke**.
3. Restart the UCMDB server.

Note: To find the default value for each setting, enter the required string in the **name** field of **getSettingDefaultValue** and click **Invoke**.

Package Manager JMX Methods

How to Deploy a Package

Follow these steps to deploy a package 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.
2. Under **UCMDB**, click **UCMDB:service=Packaging Services** to open the JMX MBEAN View page.
3. Locate **deployPackages**.
4. In the **Value** box for the parameter **customerID**, enter the <customer id>.
5. In the **Value** box for the parameter **dir**, enter the name of the folder that contains the package's zip file. Ensure that you include the full path to the folder.

Note: To deploy the package from the **basic_packages** directory, leave this box empty.

6. In the **Value** box for the parameter **packagesNames**, enter the name of the packages.
7. Select **True** to override job configurations changed in Universal Discovery.
8. Click **Invoke** to deploy the package.

How to View Package Deployment History

Each time you deploy packages, a report is created displaying the deployment status of those packages. Use the JMX console to view the deployment status report.

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 **UCMDB**, click **UCMDB:service=Packaging Services** to open the JMX MBEAN View page.
3. Locate **displayResourcesDeploymentHistory**.
4. In the **Value** box for the parameter **customerID**, enter the <customer id>.

5. In the **Value** box for the parameter **reportNum**, enter the number of the report you want to view.
6. Click **Invoke** to view the deployment status report of the packages.

How to Undeploy a Package

Follow these steps to undeploy a package using the JMX console.

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 **UCMDB**, click **UCMDB:service=Packaging Services** to open the JMX MBEAN View page.
3. Locate **undeployPackages**.
4. In the **Value** box for the parameter **customerid**, enter the <customer id>.
5. In the **Value** box for the parameter **packagesNames**, enter the name of the package you want to remove.
6. Click **Invoke** to undeploy the package.

How to Display Currently Deployed Packages

Follow these steps to display currently deployed packages using the JMX console.

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 **UCMDB**, click **UCMDB:service=Packaging Services** to open the JMX MBEAN View page.
3. Locate **displayDeployedPackages**.
4. In the **Value** box for the parameter **customerid**, enter the <customer id>.
5. In the **Value** box for the parameter **packagesNames**, specify the names of the packages you want to display.
6. Click **Invoke** to display the packages that are currently deployed.

How to Export Packages

Follow these steps to export resources from the CMDB to the server on which HP Universal CMDB is

installed using the JMX console.

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 **UCMDB**, click **UCMDB:service=Packaging Services** to open the JMX MBEAN View page.
3. Locate **exportPackages**.
4. In the **Value** box for the parameter **customerId**, enter the <customer id>.
5. In the **Value** box for the parameter **packageName**, enter the name of the package you want to export.
6. In the **Value** box for the parameter **outputDir**, enter the name of the folder on the HP Universal CMDB server to which you want to export the package's zip file. Ensure that you include the full path to the folder.
7. In the **Value** box for the parameter **userOnly**, select one of the following:
 - **True**. Export only the custom packages.
 - **False**. Export both custom and factory packages.
8. Click **Invoke** to export the package.

Chapter 3: Modeling Methods

This chapter includes:

How to Define and View a Layout Selection for a TQL Query	49
How to Encrypt the Password of a Direct Link	50
How to Rebuild the Database in Case of an Error	50
How to Export the Class Model to XML	51

How to Define and View a Layout Selection for a TQL Query

You can specify the attributes to include in the query results for each query node or relationship in a TQL query in the Element Layout tab of the Query Node Properties dialog box. Select the **Select attributes for layout** radio button and then select a CIT or relationship in the CIT pane. If you select **Specific Attributes** for the Attributes condition, only the attributes you move to the Specific Attributes pane are included in the query results for that element. If you select **All** for the Attributes condition, all of the available attributes are included in the query results for that element. In this case, you can select **Exclude specific attributes** and move selected attributes to the Excluded Attributes pane.

There is also an option to select attributes by qualifiers. If you select qualifiers in the **Attributes with the following qualifiers** field, all attributes that have the selected qualifiers are included in the query results for that element, in addition to the attributes selected in the Specific Attributes pane. In this case too, you can exclude selected attributes by moving them to the Excluded Attributes pane.

By default, the attribute settings you select for a CIT are automatically applied to its descendant CITs in the query results; however, the settings are not visible in the Element Layout tab of the dialog box. For example, if you select specific attributes to be included for the **Database** CIT, the same attributes are included for the **Oracle** CIT (a child CIT of **Database**), but if you select **Oracle** in the CIT pane, the Attributes condition displayed is **None** (the default condition).

You can then make an attributes condition selection for the child CITs themselves. If the parent CIT has **All** selected as the attributes condition, then the **Specific Attributes** option is disabled for the child CITs. If the parent CIT has **Specific Attributes** selected as the attributes condition, you can select **All** or **Specific Attributes** for the child CIT. If you select **Specific Attributes**, you can add more attributes by moving them to the Specific Attributes pane. These are included in the query results along with the

attributes inherited from the parent CIT's setting. Similarly, you can select attributes from the parent CIT's setting to exclude for the child CIT, by moving them to the Excluded Attributes pane. If the parent CIT has qualifiers selected to determine the attribute selection, these are also inherited by the child CIT. If you select additional qualifiers to filter the child CIT's attribute selection, the combined set of selected qualifiers is used to filter the attribute selection for the child CIT.

When you change the type of a query node or relationship using the Change Query Node/Relationship Type dialog box, the attributes selection for that element is lost.

If you import a package with a query that includes an attributes selection that is invalid for the selected query node, or if you make an invalid attributes selection using the JMX console, the query can be saved successfully and a warning appears in the log.

Note: The layout selection is not visible in the query results in the user interface. To view the query results with the selected attributes, access the JMX console, select **TQL services**, and invoke the **calculateTqlAdHoc** method.

How to Encrypt the Password of a Direct Link

This task describes how to encrypt the password contained within a direct link using the JMX console.

To encrypt the password of a direct link using the JMX console:

1. Launch your Web browser and enter the following address: **http://<server_name>:<port number>/jmx-console**, where **<server_name>** is the name of the machine on which HP Universal CMDB is installed.
2. Under **UCMDB-UI**, locate **UCMDB Integration**.
3. Under **getEncryptedPasswordForURL**, enter your user name and the password to encrypt.
4. Click **Invoke** to view the encrypted string.

How to Rebuild the Database in Case of an Error

If an error occurs while working with views in the Modeling managers, when adding CIs to the CMDB, or when updating existing CIs, and the error log indicates that objects are missing in the database, access the JMX console and run the following methods under service = DAL services:

- **rebuildModelViews**
- **rebuildModelDBSchemaAndViews**

How to Export the Class Model to XML

The Export to UML tool enables you to export selected sections of the UCMDB class model to a format compatible with UML tools, and to view the model as a UML diagram.

The input for the tool is the UCMDB class model XML file retrieved by the JMX service

**UCMDB:service=Class Model Services/
exportClassModelToXml()**.

Note: To access the JMX console, enter the following address in your browser: **http://<server_name>:8080/jmx-console**, where **<server_name>** is the name of the machine on which HP Universal CMDB is installed.

Chapter 4: Data Flow Management Methods

This chapter includes:

How to View Job Information on the Data Flow Probe	52
How to View Discovery Rules	62
How to View Discovery Resource History	63
How to Run Data Flow Ad Hoc Updates	65
How to Delete Unsent Probe Results	66
How to Configure Global ID Generation	67
How to Perform Initial UCMDB-UCMDB Synchronization	67
Data Flow Probe Log Files	68
How to Check XML Enricher Health Using JMX	72
How to Check the Confidential Manager Connection	73

How to View Job Information on the Data Flow Probe

This task describes how to view job information (for example, job threads and Trigger CIs) saved to the Data Flow Probe's PostgreSQL database. You work with the JMX console.

This task includes the following steps:

1. Access the MBean operations

Use the following procedure to access the JMX console on the Data Flow Probe and to invoke the JMX operations.

- a. Launch the Web browser and enter the following address:

`http://<machine name or IP address>.<domain_name>:1977/`

where **<machine name or IP address>** is the machine on which the Data Flow Probe is installed. You may have to log in with the user name and password.

- b. Click the **Local_<machine name or IP address> > type=JobsInformation** link.

2. Locate the operation to invoke

On the MBean View page, select **type=JobsInformation**. Locate the required operation.

3. Run the operation

Click the **Invoke** button to run the operation. A message is displayed with the results of the operation run.

Reload	The number of seconds between automatic reloads of the JMX interface. 0: The interface is never reloaded. Click the Reload button to manually reload the current page (if more operations have been added or removed).
Unregister	Do not touch (the view becomes inaccessible to the application that is running).

The following is a list of operations that can be invoked in the above procedure:

activateJob

Enter the name of a job and click the button to activate the job immediately. This operation returns a message, for example, **<job name> was triggered**.

Note: The following message is displayed if the job has not been activated and there is no information about the job in the Probe's database:

Job '<job name>' does not exist in the Jobs Execution table (job was not activated!).

activateJobOnDestination

Enter the name of a job and a Trigger CI and click the button to activate the job immediately on a specific Trigger CI. This operation returns a message, for example, **The operation returned with the value: Job <job name> was triggered on destination <CI name>**.

Note: Both the **JobID** and **triggerCI** fields are mandatory.

start/stop

These operations start and stop the **JobsInformation** service. Do not use these operations; instead,

restart the Probe itself.

viewJobErrorsSummary

Enter the name of a job to return a list of error messages reported on this job, together with the error severity, the last time that the error was reported, and the number of Trigger CIs that have the error.

Click the entry in the **Number of Trigger CIs** column to view a list of one job's Trigger CIs with errors on the [viewJobTriggeredCIsWithErrorId](#) page.

viewJobExecHistory

Enter the name of a job to retrieve a history of job invocations. A table is displayed showing the job invocations (the last invocation is shown first).

For each invocation the number of triggered CIs and the total running time is shown. The Execution Details column shows at which times the job was executed. If the Probe shut down in the middle of a job execution and then resumed running or if there were blackout periods during the job execution, several running times are shown.

viewJobProblems

Enter the name of a job to retrieve a list of Trigger CIs that have problems for that job. Enter the name of a Trigger CI to retrieve a list of problems for that trigger CI. If no values are entered, problems all the jobs and triggers are displayed.

Column	Description
Job ID	Displayed if the jobID field is left empty. The job name as it appears in Data Flow Management. Click a job to go to its viewJobStatus page, to view its status and scheduling information.
Trigger CI	Displayed if the triggerID field is left empty. The CMDB object ID of the trigger for a job.
ErrMsgCode	The error message hash string (error hash ID).
ErrParams	The error parameters.
Severity	The severity of the error.

viewJobResultCilnstances

Fill in one or more of the parameters to return a list of CIs that have been discovered by a job.

The **Object State Holder** column displays the code for the CI or relationship defined in the CMDB. For details on the `appilog.common.system.typesClass ObjectStateHolder` method, see the **ObjectStateHolder** method in the online API documentation.

viewJobResults

Fill in one or more of the parameters to return a list of CIs that have been discovered by a job.

When **Hide Touched CIs Info** is set to **True**, the results page displays the following information:

Column	Description
Job Name	<p>Displayed if the jobID field is left empty.</p> <p>The job name as it appears in Data Flow Management.</p> <p>Click a job to go to its viewJobStatus page, to view its status and scheduling information.</p>
CI Type	Click to filter the list to show results for one CIT only.
Total CIs	Click to go to the viewJobResultCilnstances page, to view a list of all CIs that have been discovered by a job.
Triggered CIs	Click to go to the viewJobTriggeredCIs page, to view a list of all Trigger CIs that have been discovered by a job.
Last Discover Time	The date and time that the job was invoked.

When **Hide Touched CIs Info** is set to **False**, the results page displays the following information:

Column	Description
Job Name	<p>Displayed if the jobID field is left empty.</p> <p>The job name as it appears in Data Flow Management.</p> <p>Click a job to go to its viewJobStatus page, to view its status and scheduling information.</p>
CI Type	Click to filter the list to show results for one CIT only.

Column	Description
Touched CIs	Click to go to the viewJobResultCiInstances page, to view a list of those CIs discovered by the job that are Touched CIs .
Non Touched CIs	Click to go to the viewJobResultCiInstances page, to view a list of those CIs discovered by the job that are not Touched CIs.
Triggered CIs for Touched CIs	Click to go to the viewJobTriggeredCIs page, to view a list of those Trigger CIs included in a job that are Touched CIs.
Triggered CIs for Non Touched CIs	Click to go to the viewJobTriggeredCIs page, to view a list of those Trigger CIs included in the job that are not Touched CIs.
Last Discover Time	The date and time that the job was invoked.

You can further filter results in the results page by entering text filters in one of the fields, and clicking the **Search** button.

viewJobsStatuses

Click the **viewJobsStatuses** button to return status and scheduling information for all jobs. You can choose to filter the results.

Note: This page is saved under `\DataFlowProbe\runtime\jobsStatuses` once a day.

The results page displays the following information:

Column	Description
No.	The number of the job in the list.
Job Name	The job name as it appears in Data Flow Management. Click a job to go to its viewJobStatus page, to view its status and scheduling information.

Column	Description
<p>Status</p>	<p>The severity of the job's status, as calculated by the Probe.</p> <ul style="list-style-type: none"> • Blocked. Not in use. • Removed. The job is no longer active. • Done/Total Triggers. The number of trigger CIs that the Probe finished running on, against the total number of triggers for the job. <p>For example, (28/69) indicates that there is a total of 69 triggers for the job, while the Probe has completed running on 28 of those triggers.</p> <ul style="list-style-type: none"> • Scheduled. The job is scheduled to run. <p>A red background signifies that a thread has run longer than expected and may be stuck. A green background signifies that the job is running as expected.</p>
<p>Triggered CIs</p>	<p>The Trigger CIs that have been run by the job. Click to go to the viewJobTriggeredCIs page.</p>
<p>Errors & Warnings</p>	<p>The number of errors and warnings for a specific job. Click to go to the viewJobErrorsSummary page, to view a list of error and warning messages reported on this job.</p>
<p>Last Invocation</p>	<p>The date and time that the job was last run.</p>
<p>Next Invocation</p>	<p>The date and time that the job is next scheduled to run.</p>
<p>Last Total run duration (seconds)</p>	<p>The length of time, in seconds, taken to run the job in the previous invocation. This is calculated according to the start time of the first trigger until the end time of the last trigger, even if triggers were added later on.</p>
<p>Avg run duration (seconds)</p>	<p>The average duration (in seconds) per trigger of the time it took the Probe to run this job.</p>
<p>Recurrence</p>	<p>The number of times that the job was invoked. Click to go to the viewJobExecHistory page, to retrieve a history of job invocations.</p>

Column	Description
Results	<p>The number of CITs that have been discovered by the job. Click to go to the viewJobResults page to view the CITs.</p> <p>Note: Displayed when hideResults parameter is set to False.</p>

viewJobStatus

Enter the name of a job to return its status and scheduling information.

The results page displays the following information:

Column	Description
Threading info	The total number of worker threads created by the invocation, the free worker threads, and the stuck worker threads.
Total work time	The time that the Probe took to run this job.
Tasks waiting for execution	A list of jobs together with the number of Trigger CIs that are awaiting activation.
Max. Threads	The number of threads that are serving this job.
Progress	<p>A summary of the current run, that is, since the specific run was activated.</p> <p>For example, Progress: 2017 / 6851 destinations (29%) means that out of 6851 CIs, 2017 CIs have already run.</p>

Column	Description
<p>Working Threads information</p>	<ul style="list-style-type: none"> • Thread Name. The thread that is now running this job. Click to go to the viewJobThreadDump page. You use this page when a thread is running for a long time, and you must verify that this is because the thread is working hard, and not because there is a problem. • Curr Dest. ID. The name of the node on which the job is running. • Curr Dest. IP. The IP for which the job is discovering information. • Work Time (Sec). The length of time that this thread is running. • Communication Log. Click to go to the viewCommunicationLog page, to view an XML file that logs the connection between the Probe and a remote machine.
<p>Discovery Jobs Information table</p>	<ul style="list-style-type: none"> • Status. The severity of the job's status, as calculated by the Probe. For details, see "Status" on page 57. • Triggered CIs. Click to go to viewJobTriggeredCIs page, to view a list of Trigger CIs that are part of a job. • Errors & Warnings. Click to go to viewJobErrorsSummary page, to view a list of error and warning messages reported on this job. • Last invocation. The date and time that the job was last run. • Next invocation. The date and time that the job is next scheduled to run. • Last Total run duration (seconds). The length of time, in seconds, taken to run the job in the previous invocation. This is calculated according to the start time of the first trigger until the end time of the last trigger, even if triggers were added later on. • Avg run duration (seconds). The average duration (in seconds) per trigger of the time it took the Probe to run this job. • Recurrence. The number of times that the job was invoked. Click to go to viewJobExecHistory page, to view a history of job invocations.

Note: Click **Results** below the table to go to the [viewJobResults](#) page to view the CITs that have been discovered by the job.

viewJobTriggeredCIs

Fill in one or more of the parameters to return a list of Trigger CIs that are part of a job.

The results page displays the following information:

Note: Depending on the triggers, other information might also be displayed.

Column	Description
No.	The number of the job in the list.
Triggered CI ID	The CI instances that have been discovered by the job. Click to go to the viewJobTriggeredCIs page to view information about their CITs.
Last Execution Start Time	The date and time that the job last started running.
Last Execution End Time	The date and time that the job last finished running.
Service Exec. Duration (ms)	The maximum time that it took for a job to run in the last invocation, not including periods when the job did not run. Compare this result with the total execution duration. For example, when several jobs run simultaneously, but there is only one CPU, a job might have to wait for another job to finish. The service duration does not include this waiting time, whereas the total duration does.
Total Exec. Duration (ms)	The time that it took for a job to run in the last invocation, including the periods when the job did not run.
Last Run Status	The status of the last run, that is, whether the run succeeded or failed. In case of failure, click to go to the viewJobProblems page, to view a list of Trigger CIs with problems.
Priority	The priority of the job. Note: The lower the value, the higher the priority.

viewJobTriggeredCIsWithErrorId

Note: This operation is part of the inner interface and serves as a helper function. Do not use this page to view Trigger CIs information; instead, use the [viewJobTriggeredCIs](#) page.

The following is a list of parameters used in the above operations:

- **ciType.** The name of the CI type (for example, ip, host).
- **data.** A textual field in the **DiscoveryResults** table that contains information about the discovered object. For example:

```
<object class="ip">
<attribute name="ip_probename" type="String">EBRUTER02</attribute>
<attribute name="ip_address" type="String">16.59.58.200</attribute>
<attribute name="ip_domain" type="String">DefaultDomain</attribute>
</object>
```

- **Error Id.** The error message hash string (error hash ID) that is displayed in the **Jobs_Problems** table.
- **HideRemovedJobs.True:** do not display jobs that have run previously and are not relevant to the current run.
- **Hide Touched CIs Info.** Touched CIs are CIs which were discovered in previous invocations. DFM already has information about these CIs, so there is no need for the Probe to send the information to the server again. The server identifies that these CIs are relevant and that there is no need to enforce the aging mechanism on them. For details on aging, see "The Aging Mechanism Overview" in the *HP Universal CMDB Administration Guide*.

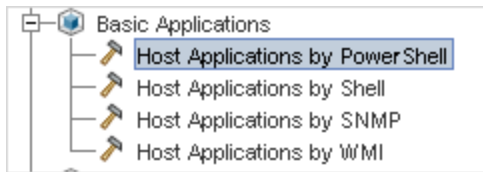
True: the table displays the total number of CIs and the total number of Trigger CIs for each CIT.

False: The table displays the total number of CIs and Trigger CIs divided between touched CIs and non-touched CIs.

- **includeNonTouched.** Enables filtering the table to view non-touched CIs. Choose between viewing non-touched CIs only, all CIs (touched and non-touched), or none:

	Non-touched CIs	All CIs	No CIs
(boolean)includeTouchedCis	<input type="radio"/> True <input checked="" type="radio"/> False	<input checked="" type="radio"/> True <input type="radio"/> False	<input type="radio"/> True <input checked="" type="radio"/> False
(boolean)includeNonTouchedCis	<input checked="" type="radio"/> True <input type="radio"/> False	<input checked="" type="radio"/> True <input type="radio"/> False	<input type="radio"/> True <input checked="" type="radio"/> False

- **includeNonTouchedCIs.** See **includeNonTouched.**
- **includeTouched.** Enables filtering the table to view touched CIs. Choose between viewing touched CIs only, all CIs (touched and non-touched), or none.
- **includeTouchedCIs.** See **includeTouched.**
- **jobID.** The name of the job, for example, **Host Applications by PowerShell:**



- **maxRows.** The maximum number of rows that should be displayed in the results table. The default is 100 or 1000.
- **maxTriggeredCIs.** See **maxRows.**
- **objectID.** The CMDB object ID.
- **hideRemovedJobs.** Hides information about jobs with the status, **REMOVED.** These are jobs that have run previously but that are not currently scheduled to run.
- **hideResults.** Indicates whether or not to hide the **Results** column. If the **Results** column is present, you can navigate to the job results.
- **triggerCI.** The CMDB object ID of the trigger for a job.
- **triggeredCiID.** See **triggerCI.**

How to View Discovery Rules

The Discovery Rules Engine is very large. You can search the rule base using search commands on the JMX console.

To search for a rule:

- Log in to the JMX console using the server administrator credentials
- Go to the service: **Normalization Rule Base Services**, and enter one of the following search commands:

Command	Description
scanForSNMPRules	Retrieves SNMP discovery rules that apply to the specified input attributes. <div style="background-color: #f0f0f0; padding: 5px;"> <p>Note:</p> <ul style="list-style-type: none"> ■ the sys_object_id value must always have a leading "." ■ Leave empty to ignore </div>
scanForScanFileRules	Retrieves Scan File discovery rules that apply to the specified input attributes. <div style="background-color: #f0f0f0; padding: 5px;"> <p>Note: Leave empty to ignore</p> </div>
viewNormalizationRuleById	Retrieves discovery rules by ID
viewNormalizationRuleByNiceId	Retrieves discovery rules by user friendly ID (NiceRuleID), <p>Example: 4323@SNMP</p>
viewNormalizationRules	Retrieves discovery rule outputs that apply to the specified input attributes <p>Format:</p> <ul style="list-style-type: none"> ■ Pair attributes in the following format: attrName;attrValue ■ Pairs must be separated by commas. <p>Example: Name;HP,Version;10</p>

How to View Discovery Resource History

Discovery resources are saved to the URM on the UCMDDB Server and from there are distributed to all the Data Flow Probes.

Whenever a user changes the definition of a resource, an updated version of the resource is stored in the URM. The URM keeps all the historical revisions of each resource.

You can view changes between an older version and the current version of resources such as discovery scripts, integration and discovery adapters, discovery jobs, and so on, from the JMX console of the UCMDB Server.

Note: The purpose of this task is to describe how to access the discovery resources in the JMX console for the purpose of **viewing** the resources and their history only.

Adding or modifying a discovery resource in the JMX console is not supported.

To view a discovery resource and its history:

1. Log in to the UCMDB JMX console.
2. In the UCMDB JMX Quick Search box, enter **listResourceTypes**.
3. Enter your Customer ID. (**Default: 1**)
4. Click **Invoke**. The **URM Services** mbean is displayed.
5. Among the UCMDB resource types displayed on this page, the following discovery resource types are displayed:

Resource Type	Description	Displays Diff Metadata	Displays Diff Content
Discovery_ADAPTER_METADATA	Adapter resources	✓	✓
Discovery_CONFIGURATION_FILE_METADATA	Configuration Files	✓	✓
Discovery_JOB_METADATA	Discovery job definitions	✓	✓
Discovery_MODULE_METADATA	Discovery modules	✓	✓
Discovery_WIZARD_METADATA	Activity types	✓	✓
Discovery_SCRIPT_METADATA	Script resources	✓	✓
Discovery_BIN_RESOURCE_METADATA	External resources	✓	✗

Resource Type	Description	Displays Diff Metadata	Displays Diff Content
Discovery_DOC_METADATA	PDF documents that come with the adapters	✓	✗
Discovery_MULTI_SCANNER_METADATA	Multiple scanner packages	✓	✗
Discovery_SCANNER_CONFIG_METADATA	Scanner configuration files	✓	✗
Discovery_SAI_RES_METADATA	SAI resources	✓	✗

6. Click a resource type to view all the resources of that type.
7. To see the history of a particular resource, click the **history** link in that resource's row.

[JMX Search](#) [JMX List](#) [Operations Index](#) [Back to MBean](#) [Reinvoke MBean](#) (Current Server is a writer: SERVER001)

Mbean: UCMDB:service=URM Services. Method: listResources[`java.lang.Integer`,`java.lang.String`]

[Add new resource](#)

Resources of type: Discovery_ADAPTER_METADATA

Real Id	Resource ID	Last updated time				
11511	ALMAdapter	Tue Jul 09 13:39:21 IDT 2013	delete	incoming_deps	outgoing_deps	history
7413	AMAdapter	Mon Jul 08 07:25:03 IDT 2013	delete	incoming_deps	outgoing_deps	history
7438	AMPushAdapter	Mon Jul 08 07:25:04 IDT 2013	delete	incoming_deps	outgoing_deps	history
7345	ARIS_To_UCMDB	Mon Jul 08 07:25:00 IDT 2013	delete	incoming_deps	outgoing_deps	history

A page opens displaying the current version of the resource, as well as all its previous revisions.

8. Click the **Diff Content** link to view the actual change. All changes between the selected and current revisions are displayed.

Note: The **Diff Content** link appears only for those resources whose changes you are able to see (see table above).

How to Run Data Flow Ad Hoc Updates

1. Log in to the UCMDB JMX console. (Launch the Web browser and enter the following address: **http://localhost:8080/jmx-console**. You may have to log in with a user name and password.)

2. Click **UCMDB:service=Discovery Manager** to open the JMX MBEAN View page.
3. Run one of the following methods, depending on which is relevant:

JMX Method	Description
recalculateAndUpdateDFMTasks	Updates data flow tasks for all the adapters for which data flow task update is enabled. <div style="background-color: #f0f0f0; padding: 5px; margin-top: 10px;"> Note: Data flow task updates are enabled in the adapter's configuration file. </div>
recalculateAndUpdateDFMTasksForAdapter	Updates data flow tasks for selected adapters without checking the adapter configurations. That is, even if the data flow task update is not enabled for a selected adapter, the updates are run.

How to Delete Unsent Probe Results

This task describes how to empty the Probe queue that contains results that have not yet been transmitted to the UCMDB Server.

1. Access the Data Flow Probe JMX console: Launch a Web browser and enter the following address: **http://<Probe Gateway 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.

2. Locate the **Probe_<Probe Name> > type=MainProbe** service and click the link to open the JMX MBEAN View page.
3. Invoke the operation by clicking the **dropUnsentResults** button.

Note: This operation deletes 100 results at a time. To delete more results, re-invoke the operation as many times as necessary.

How to Configure Global ID Generation

1. Launch the Web browser and enter the following address:
http://<CMS server>:8080/jmx-console.
2. Click **UCMDB:service=Multiple CMDB Instances Services** to open the JMX MBEAN View page.
3. Click one of the following methods and enter values as required:

setAsGlobalIdGenerator	Specifies that the CMDB will act as the global ID generator for all locally existing scopes
setAsGlobalIdGeneratorForScopes	Specifies the scopes for which global IDs will be generated
setAsNonGlobalIdGenerator	Stops the CMDB from acting as the global ID generator for all scopes

4. Click **Invoke**.

Note: If you want to check which scopes are currently set, use the **getGlobalIdGeneratorScopes** method.

How to Perform Initial UCMDB-UCMDB Synchronization

This procedure performs a full synchronization of CIs and relations between CMDBs, while retaining the original CMDB IDs. CIs are replicated from the external CMS to the UCMDB. The procedure is generally intended to be performed only once, on a new system.

1. Launch a Web browser that connects to the CMS, and enter the following address: **http://<CMS server>:8080/jmx-console.**
2. Click **UCMDB:service=Multiple CMDB Instances Services** to open the JMX MBEAN View page.
3. Click the **fetchAllDataFromAnotherCMDB** method.
4. Enter values as required for the following fields:

Note: You must enter information in fields that do not have default values.

- Customer ID
- Remote user name
- Remote password
- Remote host name
- Remote port **8080**
- Remote Customer name (default value is **Default Client**)
- Maximum chunk size
- CI type to sync (default value is **managed_object**, causing all CI types to be synchronized)
- Relation type to sync (the default value is **managed_relationship**, causing all relation types to be synchronized)

5. Click **Invoke**.

Data Flow Probe Log Files

Data Flow Probe logs store information about job activation that occurs on the Probe Gateway and Probe Manager. The log files can be accessed from the following location:

C:\hp\UCMDB\DataFlowProbe\runtime\log

Note: Alternatively, to access the Data Flow Probe's log files, log in to the JMX console (http://<probe_machine>:1977/jmx-console/) and, from the main page, select the **GeneralUtils** mbean. Activating the **executeLogGrabber** function zips all the Data Flow Probe's log files. Save the .zip file locally on your client machine.

General Logs

<p>WrapperProbeGw.log</p>	<p>Records all the Probe's console output in a single log file.</p> <ul style="list-style-type: none"> • Levels: <ul style="list-style-type: none"> ■ Error. Any error that occurs within the Probe Gateway. ■ Information. Important information messages, such as the arrival or removal of a new task. ■ Debug. N/A • Basic Troubleshooting: Use this file for any Probe Gateway problems to verify what occurred with the Probe Gateway at any time as well as any important problems it encountered.
<p>probe-error.log</p>	<p>Summary of the errors from the Probe.</p> <ul style="list-style-type: none"> • Levels: <ul style="list-style-type: none"> ■ Error. All errors in the Probe components. ■ Information. N/A ■ Debug. N/A • Basic Troubleshooting: Messages from the Probe's infrastructure only.
<p>wrapperLocal.log</p>	<p>When running the Probe in separate mode (that is, the Probe Manager and Probe Gateway are installed on separate machines), a log file is also saved to the Probe Manager.</p> <ul style="list-style-type: none"> • Levels: <ul style="list-style-type: none"> ■ Error. Any error that occurs within the Probe Manager. ■ Information. Important information messages such as received tasks, task activation, and the transferring of results. ■ Debug. N/A • Basic Troubleshooting: Use this file for any Probe Manager problems to verify what occurred with the Probe Manager at any time as well as any important problems it encountered.

<p>postgresql.log</p>	<p>Displays database related error during the installation.</p> <p>Note: If this log is empty check in the Event Viewer logs.</p>
------------------------------	--

Probe Gateway Logs

<p>probeGW-taskResults.log</p>	<p>Records all the task results sent from the Probe Gateway to the server.</p> <ul style="list-style-type: none"> • Levels: <ul style="list-style-type: none"> ■ Error. N/A ■ Information. Result details: task ID, job ID, number of CIs to delete or update. ■ Debug. The ObjectStateHolderVector results that are sent to the server (in an XML string). • Basic Troubleshooting: <ul style="list-style-type: none"> ■ If there is a problem with the results that reach the server, check this log to see which results were sent to the server by the Probe Gateway. ■ The results in this log are written only after they are sent to the server. Before that, the results can be viewed through the Probe JMX console (use the ProbeGW Results Sender MBean). You may have to log in to the JMX console with a user name and password.
---------------------------------------	---

<p>probeGW-tasks.log</p>	<p>Records all the tasks received by the Probe Gateway.</p> <ul style="list-style-type: none"> • Levels: <ul style="list-style-type: none"> ■ Error. N/A ■ Information. N/A ■ Debug. The task's XML. • Basic Troubleshooting: <ul style="list-style-type: none"> ■ If the Probe Gateway tasks are not synchronized with the server tasks, check this log to determine which tasks the Probe Gateway received. ■ You can view the current task's state through the JMX console (use the Discovery Scheduler MBean).
---------------------------------	---

Probe Manager Logs

<p>probeMgr-performance.log</p>	<p>Performance statistics dump, collected every predefined period of time, which includes memory information and thread pool statuses.</p> <ul style="list-style-type: none"> • Levels: <ul style="list-style-type: none"> ■ Error. N/A ■ Information. N/A ■ Debug. N/A • Basic Troubleshooting: <ul style="list-style-type: none"> ■ Check this log to investigate memory issues over time. ■ The statistics are logged every 1 minute, by default.
<p>probeMgr-adaptersDebug.log</p>	<p>Contains messages that are created following a job execution.</p>

Discovery Rules Engine Log Files

normalization.audit.log	<p>Logs information about the processing of the Discovery Rules Engine.</p> <ul style="list-style-type: none">• Levels:<ul style="list-style-type: none">▪ Error. N/A▪ Information. Audits the number of element processed and the number of CIs that were changed.• Example:<div style="background-color: #f0f0f0; padding: 5px; margin: 5px 0;"><pre>Normalization (OSHV: 8 elements) (Time: 125 ms) (Modified CIs: 1)</pre></div>▪ Debug. N/A
normalization.log	<p>Logs detailed information about the processing of the Discovery Rules Engine, enabling you to trace detailed information of the Discovery Rule Engine process.</p> <ul style="list-style-type: none">• Levels:<ul style="list-style-type: none">▪ Error. All discovery rule processing errors.▪ Information. Logs all levels of information about the processing of the Discovery Rules Engine.▪ Debug. Logs mainly for debugging purposes.• Basic Troubleshooting. Check this log when you need to analyze why a CI was not enriched by the Discovery Rules Engine.

How to Check XML Enricher Health Using JMX

This task describes how to view health statistics of an XML Enricher service using the JMX console.

1. Prerequisites

The Data Flow Probe where the XML Enricher service is running is started.

2. Connect to the Data Flow Probe

Launch your Web browser and enter the following address: **http://<DataFlowProbe>:1977**, where **<DataFlowProbe>** is the name of IP address of the machine on which the XML Enricher service is running.

3. View statistics

- a. Under the **Local_<DataFlowProbe>** section, click the **XMLEnricherMonitor** service.
- b. Select the **viewXmlEnricherStatuses method** and click **Invoke**.

4. Results

Health statistics for the XML Enricher are displayed.

How to Check the Confidential Manager Connection

1. Access the Data Flow Probe JMX console by launching a Web browser and entering the following address: **http://<Probe Gateway 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.

2. Enter **isCMClientInitialized** in the quick search field and click the link that appears.
3. Click **Invoke**.

The current status of the Confidential Manager server is displayed.

Chapter 5: Developer Reference Methods

This chapter includes:

How to Debug Adapter Resources	74
How to Create an Integration User	74
Web Service API - executeTopologyQueryWithParameters	77

How to Debug Adapter Resources

This task describes how to use the JMX console to create, view, and delete adapter state resources (any resources created using the resource manipulation methods in the DataAdapterEnvironment interface, which are saved in the UCMDB database or the Probe database) for debugging and development purposes.

1. Launch the Web browser and enter the server address, as follows:
 - For the UCMDB server: `http://localhost:8080/jmx-console`
 - For the Probe: `http://localhost:1977`

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

2. To open the JMX MBEAN View page, do one of the following:
 - On the UCMDB server: click **UCMDB:service=FCMDB Adapter State Resource Services**
 - On the Probe: click **type=AdapterStateResources**
3. Enter values in the operations that you want to use, and click **Invoke**.

How to Create an Integration User

You can create a dedicated user for integrations between other products and UCMDB. This user enables a product that uses the UCMDB client SDK to be authenticated in the server SDK and execute the APIs. Applications written with this API set must log on with integration user credentials.

Caution: It is also possible to connect with a regular UCMDB user (for instance, admin). However, this option is not recommended. To connect with a UCMDB user, you must grant the user API authentication permission.

To create an integration user:

1. Launch the Web browser and enter the server address, as follows:

`http://localhost:8080/jmx-console`

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

2. Under UCMDB, click **service=UCMDB Authorization Services**.
3. Locate the **createUser** operation. This method accepts the following parameters:
 - **customerId**. The customer ID.
 - **username**. The integration user's name.
 - **userDisplayName**. The integration user's display name.
 - **userLoginName**. The integration user's login name.
 - **password**. The integration user's password.

The default password policy requires the UCMDB password to include at least one of each of the four following types of characters:

- Uppercase alphabetic characters
- Lowercase alphabetic characters
- Numeric characters
- Symbol characters ,\:/._?&%="+-[]()

It also requires the password to adhere to the minimum length, which is set by the **Password minimum length** setting.

4. Click **Invoke**.
5. In a single-tenant environment, locate the **setRolesForUser** method and enter the following

parameters:

- **userName**. The integration user's name.
- **roles**. SuperAdmin.

Click **Invoke**.

6. In a multi-tenant environment, locate the **grantRolesToUserForAllTenants** method and enter the following parameters to assign the role in connection with all tenants:

- **userName**. The integration user's name.
- **roles**. SuperAdmin.

Click **Invoke**.

Alternatively, to assign the role in connection with specific tenants, invoke the **grantRolesToUserForTenants** method, using the same **userName** and **roles** parameter values. For the **tenantNames** parameter, enter the required tenants.

7. Either create more users, or close the JMX console.
8. Log on to UCMDB as an administrator.
9. From the **Administration** tab, run **Package Manager**.
10. Click the **Create custom package** icon.
11. Enter a name for the new package, and click **Next**.
12. In the Resource Selection tab, under **Settings**, click **Users**.
13. Select a user or users that you created using the JMX console.
14. Click **Next** and then **Finish**. Your new package appears in the Package Name list in Package Manager.
15. Deploy the package to the users who will run the API applications.

For details, see the section "How to Deploy a Package" in the *HP Universal CMDB Administration Guide*.

Note: The integration user is per customer. To create a stronger integration user for cross-customer usage, use a **systemUser** with the **isSuperIntegrationUser** flag set to **true**. Use the **systemUser** methods (**removeUser**, **resetPassword**, **UserAuthenticate**, and so on).

There are two out-of-the-box system users. It is recommended to change their passwords after installation using the **resetPassword** method.

- **sysadmin/sysadmin**
- **UISysadmin/UISysadmin** (this user is also the **SuperIntegrationUser**).

If you change the UISysadmin password using **resetPassword**, you must do the following:

- i. In the JMX Console, locate the **UCMDB-UI:name=UCMDB Integration** service.
- ii. Run **setCMDBSuperIntegrationUser** with the user name and new password of the integration user.

Web Service API - executeTopologyQueryWithParameters

The `executeTopologyQueryWithParameters` method retrieves a `topologyMap` element that matches the parameterized query.

The query is passed in the `queryXML` argument. The values for the query parameters are passed in the `parameterizedNodeList` argument. The TQL must have unique labels defined for each `CINode` and each `relationNode`.

The `executeTopologyQueryWithParameters` method is used to pass ad hoc queries, rather than accessing a query defined in the CMDB. You can use this method when you do not have access to the UCMDB user interface to define a query, or when you do not want to save the query to the database.

To use an exported TQL as the input of this method, do the following:

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. Click **UCMDB:service=TQL Services**.

3. Locate the **exportTql** operation.
 - In the **customerId** parameter box, enter **1** (the default).
 - In the **patternName** parameter box, enter a valid TQL name.
4. Click **Invoke**.

Chapter 6: Configuration Manager Methods

This chapter includes:

Configuration Manager JMX Methods	79
---	----

Configuration Manager JMX Methods

How to Enable Advanced Content

If you purchased the relevant license after deploying Configuration Manager, perform the following procedure to activate the content:

1. Launch your Web browser and enter the following address: **http://<server_name>:<port_number>/cnc/jmx-console**, where **<server_name>** is the name of the machine on which Configuration Manager is installed.
2. Enter the JMX console authentication credentials.
3. Under **Configuration Manager**, click **ImportExport service**.
4. Locate the **activateAutomanageResource** operation and click **Invoke**.

How to Delete Advanced Content

If you want to delete advanced content that was previously installed, do the following:

1. Launch your Web browser and enter the following address: **http://<server_name>:<port_number>/cnc/jmx-console**, where **<server_name>** is the name of the machine on which Configuration Manager is installed.
2. Enter the JMX console authentication credentials.
3. Under **Configuration Manager**, click **Licensed content service**.
4. Locate the **deactivateAutomanagedResources** operation and click **Invoke**.

How to Export the System Data

This task describes how to list and export the system data, views, and policies of Configuration Manager and store this information in its file system.

1. Launch your Web browser and enter the following address: **http://<server_name>:<port_number>/cnc/jmx-console**, where **<server_name>** is the name of the machine on which Configuration Manager is installed.
2. Enter the JMX console authentication credentials.
3. Under **Configuration Manager**, click **ImportExport service**.
4. Locate one of the following operations:
 - **exportData**
 - **listAllViews**
 - **exportViews**
 - **listAllPolicies**
 - **exportPolicies**
5. In the **Value** field, enter the file name and the full path of the directory in the file system of the Configuration Manager server to which the data is exported. You can also provide a network path if you do not want the exported file to reside on the same server.
6. Click **Invoke** to export the data. The data is exported as an XML file to the specified directory.

How to Import the System Data

This task describes how to import the XML file containing the system data from Configuration Manager's file system to another Configuration Manager of the same version using the JMX console.

1. Launch your Web browser and enter the following address: **http://<server_name>:<port_number>/cnc/jmx-console**, where **<server_name>** is the name of the machine on which Configuration Manager is installed.
2. Enter the JMX console authentication credentials.

3. Under **Configuration Manager**, click **ImportExport service**.
4. Locate the **importData** operation.
5. In the **Value** field, enter the file name and the full path of the directory in the file system of the Configuration Manager server from which the data is imported. You can provide a network path to import data from a file which does not reside on the same server.
6. Click **Invoke** to import the data.

How to Update the Configuration Manager Folding Rules

After defining folding rules for composite CIs in UCMDB, execute the following JMX commands to update the folding rules in Configuration Manager:

1. Access the JMX console by launching your Web browser and entering the following address:
http://<server_name>:<port_number>/cnc/jmx-console, where **<server_name>** is the name of the machine on which Configuration Manager is installed.
2. Enter the JMX console authentication credentials.
3. Click **Configuration Manager > View Service**. Select **updateFoldingRules** and click **Invoke**.

How to Enable Large Capacity

Configuration Manager supports working with up to 20,000 composite CIs in a single managed view. To enable this functionality, do the following:

Note:

- If you want to enable this functionality, it is recommended to install Configuration Manager on a server that has a minimum of 8 GB of memory (RAM).
- Managed views that are based on dynamic TQL queries and result in more than 20,000 composite CIs are not supported.

1. To access the JMX console, launch your Web browser and enter the following address:
http://<server_name>:<port_number>/cnc/jmx-console, where **<server_name>** is the name of the machine on which Configuration Manager is installed.
2. Enter the JMX console authentication credentials.

3. Click **Configuration Manager > View Service**. Select **supportLargeViews** and click **Invoke**.
4. In UCMDB, change the value of the TQL Group View Result Size setting to 500,000 (**Administration > Infrastructure Settings Manager > TQL Settings**).
5. Do one of the following:
 - If you use the HP Universal CMDB Configuration Manager Windows service to start Configuration Manager, navigate to the **<Configuration_Manager_installation_directory>/bin/** folder and double-click the **edit-server-0.bat** file. In the Java tab, increase the value of the Maximum memory pool parameter to 4096 or greater.
 - If you use the **start-server-0.bat** file to start Configuration Manager, edit the **start-server-0.bat** file and raise the value of the **-Xmx** parameter to 4096m or greater.

Chapter 7: Hardening Methods

This chapter includes:

How to Change the System User Name or Password for the JMX Console	84
How to Enable Mutual Certificate Authentication for SDK	85
How to Configure a Reverse Proxy	87
How to Change the Server Keystore Password	88
How to Enable or Disable HTTP/HTTPS Ports	89
How to Map the UCMDB Web Components to Ports	90
How to Modify the PostgreSQL Database Encrypted Password	92
How to Set the JMX Console Encrypted Password	93
How to Set the UpLoadScanFile Password	94
How to Retrieve the Current LW-SSO Configuration in a Distributed Environment	96
How to Configure LW-SSO Settings	96
How to Configure Confidential Manager Communication Encryption	97
How to Configure Confidential Manager Client Authentication and Encryption Settings on the Probe	98
How to Configure Confidential Manager Communication Encryption on the Probe	99
How to Configure the Confidential Manager Client's Cache Encryption Settings on the Probe	100
How to Export and Import Credential and Range Information in Encrypted Format	102
How to Generate or Update the Encryption Key for Confidential Manager	103
Generate a New Encryption Key	104
Update an Encryption Key on a UCMDB Server	105
Update an Encryption Key on a Probe	107
Manually Change the Encryption Key when the Probe Manager and Probe Gateway are Installed on Separate Machines	107
Define Several JCE Providers	108
How to Configure CAC Support on UCMDB	108
How to Configure CAC Support for UCMDB by Reverse Proxy	111

How to Harden the Data Flow Probe Connector in UCMDB	117
How to Encrypt the Probe Keystore and Truststore Passwords	118
How to Enable Login to HP Universal CMDB with LW-SSO	119
How to Test LDAP Connections	120
How to Enable and Define the LDAP Authentication Method	120
How to Configure the HP Universal CMDB Server with Confidential Manager	121
How to Set the IIS server as the Front-End Server for UCMDB	123

How to Change the System User Name or Password for the JMX Console

The JMX console uses system users, that is, cross-customer users in a multi-customer environment. You can log in to the JMX console with any system user name.

You change the password either through the JMX console or through the Server Management tool.

To change the default system user name or password through the JMX console:

1. Launch a Web browser and enter the following address: **http://localhost.<domain_name>:8080/jmx-console**.
2. Enter the JMX console authentication credentials.
3. Locate **UCMDB:service=Authorization Services** and click the link to open the Operations page.
4. Locate the **resetPassword** operation.
 - In the **userName** field, enter **sysadmin**.
 - In the **password** field, enter a new password.
5. Click **Invoke** to save the change.

To change the default system user name or password through the Server Management tool:

1. **For Windows:** run the following file: **C:\hp\UCMDB\UCMDBServer\tools\server_management.bat**.
For Linux: Run **server_management.sh** located in the following folder:
/opt/hp/UCMDB/UCMDBServer/tools/.
2. Log in to the tool with the authentication credentials: **sysadmin/sysadmin**.
3. Click the Users link.
4. Select the system user and click **Change password for logged-on user**.
5. Enter the old and new passwords and click **OK**.

How to Enable Mutual Certificate Authentication for SDK

This mode uses SSL and enables both server authentication by the UCMDB and client authentication by the UCMDB-API client. Both the server and the UCMDB-API client send their certificates to the other entity for authentication.

Note: The following method of enabling SSL on the SDK with mutual authentication is the most secure of the methods and is therefore the recommended communication mode.

1. Harden the UCMDB-API client connector in UCMDB:
 - a. Access the UCMDB JMX console: Launch a Web browser and enter the following address:
http://<UCMDB machine name or IP address>:8080/jmx-console. You may have to log in with a user name and password.
 - b. Locate **UCMDB:service=Ports Management Services** and click the link to open the Operations page.
 - c. Locate the **PortsDetails** operation and click **Invoke**. Make a note of the HTTPS with client authentication port number. The default is 8444 and it should be enabled.
 - d. Return to the Operations page.
 - e. To map the ucmdb-api connector to the mutual authentication mode, invoke the **mapComponentToConnectors** method with the following parameters:

- **componentName:** ucmdb-api
- **isHTTPSWithClientAuth:** true
- All other flags: false

The following message is displayed:

Operation succeeded. Component ucmdb-api is now mapped to: HTTPS_CLIENT_AUTH ports.

- f. Return to the Operations page.
2. Repeat [step 1](#) for the **ping** component.
 3. Make sure the JRE that runs the UCMDB-API client has a keystore containing a client certificate.
 4. Export the UCMDB-API client certificate from its keystore.
 5. Import the exported UCMDB-API client certificate to the UCMDB Server Truststore.

- a. On the UCMDB machine, copy the created UCMDB-API client certificate file to the following directory on UCMDB:

C:\HP\UCMDB\UCMDBServer\conf\security

- b. Run the following command:

```
C:\HP\UCMDB\UCMDBServer\bin\jre\bin\keytool.exe -import -v -keystore  
C:\HP\UCMDB\UCMDBServer\conf\security\server.truststore -file <exported  
UCMDB-api client certificate> -alias ucmdb-api
```

- c. Enter the UCMDB Server Truststore password (default **hpass**).
 - d. When asked, **Trust this certificate?**, press **y** and then **Enter**.
 - e. Make sure the output **Certificate** was added to the keystore.
6. Export the UCMDB server certificate from the server keystore.
- a. On the UCMDB machine, run the following command:

```
C:\HP\UCMDB\UCMDBServer\bin\jre\bin\keytool.exe -export -alias hpcert  
-keystore  
C:\HP\UCMDB\UCMDBServer\conf\security\server.keystore  
-file C:\HP\UCMDB\conf\security\server.cert
```

- b. Enter the UCMDB Server Truststore password (default **hpass**).
- c. Verify that the certificate is created in the following directory:

C:\HP\UCMDB\UCMDBServer\conf\security\server.cert

- 7. Import the exported UCMDB certificate to the JRE of the UCMDB-API client truststore.
- 8. The certificate used by the API Client must contain in it's Common Name (CN) field the name of a user that's present in UCMDB.

This user **MUST** have an **EMPTY** password and all required permissions for SDK access.

To set an empty password to an existing UCMDB user,

- a. Go to **JMX Console > UCMDB:service=URM Services > listResourceTypes**.
 - b. Click **Auth_USER**.
 - c. Click your user and wait for the XML to load.
 - d. In the XML, replace the password with **s39t30*tfoZXg30xd/nvJGL5is8=**.
 - e. Click **Save resource**.
- 9. Restart the UCMDB Server and the UCMDB-API client.
 - 10. To connect from the UCMDB-API client to UCMDB-API server, use the following code:

```
UcmdbServiceProvider provider = UcmdbServiceFactory.getServiceProvider
("https", <SOME_HOST_NAME>, <HTTPS_WITH_CLIENT_AUTH_PORT_NUMBER
(default:8444>));
UcmdbService ucldbService = provider.connect
(provider.createCertificateCredentials(<TheClientKeystore.
e.g: "c:\\client.keystore">, <KeystorePassword>), provider.createClientContext
(<ClientIdentification>));
```

How to Configure a Reverse Proxy

You can make changes to the reverse proxy configuration by using the JMX console on the HP Universal CMDB server machine. This configuration is only necessary when creating a direct link to a report using the Scheduler.

To change a reverse proxy configuration:

1. On the HP Universal CMDB server machine, launch the Web browser and enter the following address:

http://<machine name or IP address>.<domain_name>:8080/jmx-console

where **<machine name or IP address>** is the machine on which HP Universal CMDB is installed. You may have to log in with the user name and password.

2. Click the **UCMDB-UI > UCMDB-UI:name=UI Server frontend settings** link.

In the **setUseFrontendURLBySettings** field, enter the server proxy URL, for example, `https://my_proxy_server:443/`.

3. Click **Invoke**.
4. To see the value of this setting, use the **showFrontendURLInSettings** method.

How to Change the Server Keystore Password

After installing the Server, the HTTPS port is open and the store is secured with a weak password (the default **hppass**). If you intend to work with SSL only, you must change the password.

The following procedure explains how to change the **server.keystore** password only. However, you should perform the same procedure for changing the **server.truststore** password.

Note: You must perform every step in this procedure.

1. Start the UCMDB Server.
2. Execute the password change in the JMX console:
 - a. Launch the Web browser and enter the Server address, as follows: **http://<UCMDB Server Host Name or IP>:8080/jmx-console**.

You may have to log in with a user name and password.
 - b. Under UCMDB, click **UCMDB:service=Security Services** to open the Operations page.
 - c. Locate and execute the **changeKeystorePassword** operation.

This field must not be empty and must be at least six characters long. The password is changed in the database only.

3. Stop the UCMDB Server.
4. Run commands.

From **C:\hp\UCMDB\UCMDBServer\bin\jre\bin**, run the following commands:

- a. Change the store password:

```
keytool -storepasswd -new <new_keystore_pass> -keystore  
C:\hp\UCMDB\UCMDBServer\conf\security\server.keystore -storepass <current_keystore_  
pass>
```

- b. The following command displays the inner key of the keystore. The first parameter is the alias. Save this parameter for the next command:

```
keytool -list -keystore C:\hp\UCMDB\UCMDBServer\conf\security\server.keystore
```

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

```
keytool -keypasswd -alias <alias> -keypass <currentPass> -new <newPass> -keystore  
C:\hp\UCMDB\UCMDBServer\conf\security\server.keystore
```

- d. Enter the new password.
5. Start the UCMDB Server.
6. Repeat the procedure for the Server truststore.

How to Enable or Disable HTTP/HTTPS Ports

To enable or disable the HTTP/HTTPS ports from the JMX console:

1. Launch a Web browser and enter the following address: `http://localhost.<domain_name>:8080/jmx-console`.
2. Enter the JMX console authentication credentials.

3. Locate **UCMDB:service=Ports Management Services** and click the link to open the Operations page.
4. To enable or disable the HTTP port, locate the **HTTPSetEnable** operation and set the value.
 - **True:** the port is enabled.
 - **False:** the port is disabled.
5. To enable or disable the HTTPS port, locate the **HTTPSSetEnable** operation and set the value.
 - **True:** the port is enabled.
 - **False:** the port is disabled.
6. To enable or disable the HTTPS port with client authentication, locate the **HTTPSClientAuthSetEnable** operation and set the value.
 - **True:** the port is enabled.
 - **False:** the port is disabled.

How to Map the UCMDB Web Components to Ports

You can configure the mapping of each UCMDB component to the available ports from the JMX console.

To view the current component configurations:

1. Launch a Web browser and enter the following address: **http://localhost.<domain_name>:8080/jmx-console**.
2. Enter the JMX console authentication credentials.
3. Locate **UCMDB:service=Ports Management Services** and click the link to open the Operations page.
4. Locate the **ComponentsConfigurations** method and click **Invoke**.
5. For each component, the valid ports and current mapped ports are displayed.

To map the components:

1. Locate **UCMDB:service=Ports Management Services** and click the link to open the Operations page.
2. Locate the **mapComponentToConnectors** method.
3. Enter a component name in the Value box. Select **True** or **False** for each of the ports corresponding to your selection. Click **Invoke**. The selected component is mapped to the selected ports. You can find the component names by invoking the **serverComponentsNames** method.
4. Repeat the process for each relevant component.

Note:

- Every component must be mapped to at least one port. If you do not map a component to any port, it is mapped by default to the HTTP port.
- If you map a component to both the HTTPS port and the HTTPS port with client authentication, only the client authentication option is mapped (the other option is redundant in this case).
- If you set **isHTTPSWithClientAuth** to **True** for the UCMDB UI component, you must also set it to **True** for the root component.

You can also change the value assigned to each of the ports.

To set values for the ports:

1. Locate **UCMDB:service=Ports Management Services** and click the link to open the Operations page.
2. To set a value for the HTTP port, locate the **HTTPSetPort** method and enter a value in the **Value** box. Click **Invoke**.
3. To set a value for the HTTPS port, locate the **HTTPSSetPort** method and enter a value in the **Value** box. Click **Invoke**.
4. To set a value for the HTTPS port with client authentication, locate the **HTTPSClientAuthSetPort** method and enter a value in the **Value** box. Click **Invoke**.

How to Modify the PostgreSQL Database Encrypted Password

This section explains how to modify the encrypted password for the PostgreSQL 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.

- b. Locate the **Type=MainProbe** service and click the link to open the Operations page.
- c. Locate the **getEncryptedDBPassword** operation.
- d. In the **DB Password** field, enter the password to be encrypted.
- e. Invoke the operation by clicking the **getEncryptedDBPassword** button.

The result of the invocation is an encrypted password string, for example:

66,85,54,78,69,117,56,65,99,90,86,117,97,75,50,112,65,53,67,114,112,65,61,61

2. Stop the Data Flow Probe

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

3. Run the `set_dbuser_password.cmd` Script

This script is located in the following folder: **C:\hp\UCMDB\DataFlowProbe\tools\dbscripts\set_dbuser_password.cmd**

Run the **set_dbuser_password.cmd** script with the new password as the first argument, and the PostgreSQL Root Account password as the second argument.

For example:

set_dbuser_password <my_password><root_password>.

The password must be entered in its unencrypted form (as plain text).

4. Update the Password in the Data Flow Probe Configuration Files
 - a. The password must reside encrypted in the configuration files. To retrieve the password's encrypted form, use the **getEncryptedDBPassword** JMX method, as explained in step 1.
 - b. Add the encrypted password to the following properties in the **C:\hp\UCMDB\DataFlowProbe\conf\DataFlowProbe.properties** file.
 - **appilog.agent.probe.jdbc.pwd**

For example:

```
appilog.agent.probe.jdbc.user = mamprobe  
appilog.agent.probe.jdbc.pwd =  
66,85,54,78,69,117,56,65,99,90,86,117,97,75,50,112,65,53,67,114,112,65,61  
,61
```

- **appilog.agent.local.jdbc.pwd**
- **appilog.agent.normalization.jdbc.pwd**

5. Start the Data Flow Probe

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

How to 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 DataFlowProbe.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.

- b. Locate the **Type=MainProbe** service and click the link to open the Operations page.

- c. Locate the **getEncryptedKeyPassword** operation.
- d. In the **Key Password** field, enter the password to be encrypted.
- e. Invoke the operation by clicking the **getEncryptedKeyPassword** button.

The result of the invocation is an encrypted password string, for example:

```
85, -9, -61, 11, 105, -93, -81, 118
```

2. Stop the Data Flow Probe

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

3. Add the Encrypted Password

Add the encrypted password to the following property in the **C:\hp\UCMDB\DataFlowProbe\conf\DataFlowProbe.properties** file.

appilog.agent.Probe.JMX.BasicAuth.Pwd

For example:

```
appilog.agent.Probe.JMX.BasicAuth.User=sysadmin  
appilog.agent.Probe.JMX.BasicAuth.Pwd=12, -35, -37, 82, -2, 20, 57, -40, 38, 80, -111, -  
99, -64, -5, 35, -122
```

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

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

Test the result in a Web browser.

How to Set the UploadScanFile Password

This section explains how to set the password for **UploadScanFile**, used for off-site scan saving. The encrypted password is stored in the **DataFlowProbe.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.

- b. Locate the **Type=MainProbe** service and click the link to open the Operations page.
- c. Locate the **getEncryptedKeyPassword** operation.
- d. In the **Key Password** field, enter the password to be encrypted.
- e. Invoke the operation by clicking the **getEncryptedKeyPassword** button.

The result of the invocation is an encrypted password string, for example:

85, -9, -61, 11, 105, -93, -81, 118

2. Stop the Data Flow Probe

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

3. Add the Encrypted Password

Add the encrypted password to the following property in the **C:\hp\UCMDB\DataFlowProbe\conf\DataFlowProbe.properties** file.

com.hp.ucmdb.discovery.Probe.JMX.UploadAuth.Pwd

For example:

```
com.hp.ucmdb.discovery.Probe.JMX.UploadAuth.User=UploadScanFile  
com.hp.ucmdb.discovery.Probe.JMX.UploadAuth.Pwd=116,116,21,34,-59,77,-  
108,14,127,4,-89,101,-33,-31,116,53
```

4. Start the Data Flow Probe

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

Test the result in a Web browser.

How to Retrieve the Current LW-SSO Configuration in a Distributed Environment

When UCMDB is embedded in a distributed environment, for example, in a BSM deployment, perform the following procedure to retrieve the current LW-SSO configuration on the processing machine.

To retrieve the current LW-SSO configuration:

1. Launch a Web browser and enter the following address: `http://localhost.<domain_name>:8080/jmx-console`.

You may be asked for a user name and password.

2. Locate **UCMDB:service=Security Services** and click the link to open the Operations page.
3. Locate the **retrieveLWSSOConfiguration** operation.
4. Click **Invoke** to retrieve the configuration.

How to Configure LW-SSO Settings

This procedure describes how to change the LW-SSO init string on the UCMDB server. This change is automatically sent to Probes (as an encrypted string), unless the UCMDB server is configured to not automatically do this. For details, see *Disable Automatic Synchronization of the Confidential Manager Client Authentication and Encryption Settings Between the Server and Probes* in the *HP Universal CMDB and Configuration Manager Hardening Guide*.

1. On the UCMDB server, launch the Web browser and enter the following address:
`http://localhost:8080/jmx-console`.
2. Click **UCMDB-UI:name=LW-SSO Configuration** to open the JMX MBEAN View page.
3. Locate the **setInitString** method.
4. Enter a new LW-SSO init string.
5. Click **Invoke**.

How to Configure Confidential Manager Communication Encryption

This procedure describes how to change the Confidential Manager communication encryption settings on the UCMDB Server. These settings specify how the communication between the Confidential Manager client and the Confidential Manager server is encrypted. This change is automatically sent to Probes (as an encrypted string), unless the UCMDB server is configured to not automatically do this. For details, see *Disable Automatic Synchronization of the Confidential Manager Client Authentication and Encryption Settings Between the Server and Probes* in the *HP Universal CMDB and Configuration Manager Hardening Guide*.

1. On the UCMDB server, launch the Web browser and enter the following address:
http://localhost:8080/jmx-console.
2. Click **UCMDB:service=Security Services** to open the JMX MBEAN View page.
3. Click the **CMGetConfiguration** method.
4. Click **Invoke**.

The XML of the current Confidential Manager configuration is displayed.

5. Copy the contents of the displayed XML.
6. Navigate back to the **Security Services** JMX MBean View page.
7. Click the **CMSetConfiguration** method.
8. Paste the copied XML into the **Value** field.
9. Update the relevant transport-related settings and click **Invoke**.

Example:

```
<transport>
  <encryptTransportMode>true</encryptTransportMode>
  <CMEncryptionDecryption>
    <encryptDecryptInitString>radiohead</encryptDecryptInitString>
```

```
<cryptoSource>lw</cryptoSource>
<lwJCEPBCompatibilityMode>true</lwJCEPBCompatibilityMode>
<cipherType>symmetricBlockCipher</cipherType>
<engineName>AES</engineName>
<algorithmModeName>CBC</algorithmModeName>
<algorithmPaddingName>PKCS7Padding</algorithmPaddingName>
<keySize>256</keySize>
<pbeCount>20</pbeCount>
<pbeDigestAlgorithm>SHA1</pbeDigestAlgorithm>
<encodingMode>Base64Url</encodingMode>
<useMacWithCrypto>false</useMacWithCrypto>
<macType>hmac</macType>
<macKeySize>256</macKeySize>
<macHashName>SHA256</macHashName>
</CMEncryptionDecryption>
</transport>
```

For details about the values that can be updated, see Confidential Manager Encryption Settings in the *HP Universal CMDB and Configuration Manager Hardening Guide*.

How to Configure Confidential Manager Client Authentication and Encryption Settings on the Probe

This procedure is relevant if the UCMDB Server has been configured to not send LW-SSO/Confidential Manager configuration and settings automatically to Probes. For details, see *Disable Automatic Synchronization of the Confidential Manager Client Authentication and Encryption Settings Between the Server and Probes* in the *HP Universal CMDB and Configuration Manager Hardening Guide*.

1. On the Probe machine, launch the Web browser and enter the following address:
<http://localhost:1977>.

Note: If the Probe Manager and the Probe Gateway are running as separate processes, the address should be entered on the machine that is running the Probe Manager as follows:
http://localhost:1978.

2. Click **type=CMClient** to open the JMX MBEAN View page.
3. Locate the **setLWSSOInitString** method and provide the same init string that was provided for UCMDB's LW-SSO configuration.
4. Click the **setLWSSOInitString** button.

How to Configure Confidential Manager Communication Encryption on the Probe

This procedure is relevant if the UCMDB Server has been configured to not send LW-SSO/Confidential Manager configuration and settings automatically to Probes.

1. On the Probe machine, launch the Web browser and enter the following address:
http://localhost:1977.

Note: If the Probe Manager and the Probe Gateway are running as separate processes, the address should be entered on the machine that is running the Probe Manager as follows:
http://localhost:1978.

2. Click **type=CMClient** to open the JMX MBEAN View page.
3. Update the following transport-related settings:

Note: You must update the same settings that you updated on the UCMDB server. To do this, some of the methods that you update on the Probe may require more than one parameter.

- a. **setTransportInitString** changes the **encryptDecryptInitString** setting.
- b. **setTransportEncryptionAlgorithm** changes Confidential Manager settings on the Probe according to the following map:

- **Engine name** refers to the <engineName> entry
 - **Key size** refers to the <keySize> entry
 - **Algorithm padding name** refers to the <algorithmPaddingName> entry
 - **PBE count** refers to the <pbeCount> entry
 - **PBE digest algorithm** refers to the <pbeDigestAlgorithm> entry
- c. **setTransportEncryptionLibrary** changes Confidential Manager settings on the Probe according to the following map:
- **Encryption Library name** refers to the <cryptoSource> entry
 - **Support previous lightweight cryptography versions** refers to the <lwJCEPBCompatibilityMode> entry
- d. **setTransportMacDetails** change Confidential Manager settings on the Probe according to the following map:
- **Use MAC with cryptography** refers to the <useMacWithCrypto> entry
 - **MAC key size** refers to the <macKeySize> entry
4. Click the **reloadTransportConfiguration** button to make the changes effective on the Probe.

How to Configure the Confidential Manager Client's Cache Encryption Settings on the Probe

This procedure describes how to change the encryption settings of the Confidential Manager client's file system cache file. Note that changing the encryption settings for the Confidential Manager client's file system cache causes the file system cache file to be recreated. This recreation process requires restarting the Probe and full synchronization with the UC MDB Server.

1. On the Probe machine, launch the Web browser and enter the following address:
http://localhost:1977.

Note: If the Probe Manager and the Probe Gateway are running as separate processes, the

address should be entered on the machine that is running the Probe Manager as follows:
http://localhost:1978.

2. Click **type=CMClient** to open the JMX MBEAN View page.
3. Update the following cache-related settings:

Note: Some of the methods that you update on the Probe may require more than one parameter. To see the current probe configuration, click **displayCacheConfiguration** in the JMX MBEAN View page.

- a. **setCacheInitString** changes the file system cache <encryptDecryptInitString> setting.
 - b. **setCacheEncryptionAlgorithm** changes the file system cache settings according to the following map:
 - **Engine name** refers to the <engineName> entry
 - **Key size** refers to the <keySize> entry
 - **Algorithm padding name** refers to the <algorithmPaddingName> entry
 - **PBE count** refers to the <pbeCount> entry
 - **PBE digest algorithm** refers to the <pbeDigestAlgorithm> entry
 - c. **setCacheEncryptionLibrary** changes the cache file system settings according to the following map:
 - **Encryption Library name** refers to the <cryptoSource> entry
 - **Support previous lightweight cryptography versions** refers to the <lwJCEPBCompatibilityMode> entry
 - d. **setCacheMacDetails** changes the cache file system settings according to the following map:
 - **Use MAC with cryptography** refers to the <useMacWithCrypto> entry
 - **MAC key size** refers to the <macKeySize> entry
4. Click the **reloadCacheConfiguration** button to make the changes effective on the Probe. This causes the Probe to restart.

Note: Make sure that no job is running on the Probe during this action.

How to Export and Import Credential and Range Information in Encrypted Format

You can export and import credentials and network range information in encrypted format in order to copy the credentials information from one UCMDB Server to another. For example, you might perform this operation during recovery following a system crash or during upgrade.

- **When exporting credentials information**, you must enter a password (of your choosing). The information is encrypted with this password.
- **When importing credentials information**, you must use the same password that was defined when the DSD file was exported.

Note: The exported credentials document also contains ranges information that is defined on the system from which the document was exported. During the import of the credentials document, ranges information is imported as well.

To export credentials information from the UCMDB Server:

1. On the UCMDB Server, launch the Web browser and enter the following address:
http://localhost:8080/jmx-console. You may have to log in with a user name and password.
2. Click **UCMDB:service=DiscoveryManager** to open the JMX MBEAN View page.
3. Locate the **exportCredentialsAndRangesInformation** operation. Do the following:
 - Enter your customer ID (the default is 1).
 - Enter a name for the exported file.
 - Enter your password.
 - Set **isEncrypted=True** if you want the exported file to be encrypted with the provided password, or **isEncrypted=False** if you want the exported file to not be encrypted (in which case passwords and other sensitive information are not exported).
4. Click **Invoke** to export.

When the export process completes successfully, the file is saved to the following location:
c:\hp\UCMDB\UCMDBServer\conf\discovery\<customer_dir>.

To import credentials information from the UCMDB Server:

1. On the UCMDB Server, launch the Web browser and enter the following address:
http://localhost:8080/jmx-console.

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

2. Click **UCMDB:service=DiscoveryManager** to open the JMX MBEAN View page.
3. Locate the **importCredentialsAndRangesInformation** operation.
4. Enter your customer ID (the default is 1).
5. Enter the name of the file to import. This file must be located in
c:\hp\UCMDB\UCMDBServer\conf\discovery\<customer_dir>.
6. Enter the password. This must be the same password that was used when the file was exported.
7. Click **Invoke** to import the credentials.

How to Generate or Update the Encryption Key for Confidential Manager

You can generate or update an encryption key to be used for encryption or decryption of Confidential Manager communication and authentication configurations exchanged between the UCMDB Server and the Data Flow Probe. In each case (generate or update), the UCMDB Server creates a new encryption key based on parameters that you supply (for example, key length, extra PBE cycles, JCE provider) and distributes it to the Probes.

The result of running the **generateEncryptionKey** method is a new generated encryption key. This key is stored only in secured storage and its name and details are not known. If you reinstall an existing Data Flow Probe, or connect a new Probe to the UCMDB Server, this new generated key is not recognized by the new Probe. In these cases, it is preferable to use the **changeEncryptionKey** method to change encryption keys. This way, when you reinstall a Probe or install a new Probe, you can import the existing key (whose name and location you know) by running the **importEncryptionKey** method on the Probe JMX console.

Note:

- The difference between the methods used to create a key (**generateEncryptionKey**) and update a key (**changeEncryptionKey**) is that **generateEncryptionKey** creates a new, random encryption key, while **changeEncryptionKey** imports an encryption key whose name you provide.
- Only one encryption key can exist on a system, no matter how many Probes are installed.

This task includes the following steps:

- ["Generate a New Encryption Key" below](#)
- ["Update an Encryption Key on a UCMDB Server" on the next page](#)
- ["Update an Encryption Key on a Probe" on page 107](#)
- ["Manually Change the Encryption Key when the Probe Manager and Probe Gateway are Installed on Separate Machines" on page 107](#)
- ["Define Several JCE Providers" on page 108](#)

Generate a New Encryption Key

You can generate a new key to be used by the UCMDB Server and Data Flow Probe for encryption or decryption. The UCMDB Server replaces the old key with the new generated key, and distributes this key among the Probes.

To generate a new encryption key through the JMX console:

1. On the UCMDB server, launch the Web browser and enter the following address:
http://localhost:8080/jmx-console.

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

2. Click **UCMDB:service=DiscoveryManager** to open the JMX MBEAN View page.
3. Locate the generateEncryptionKey operation.
 - a. In the **customerId** parameter box, enter 1 (the default).
 - b. For **keySize**, specify the length of the encryption key. Valid values are 128, 192, or 256.

- c. For **usePBE**, specify **True** or **False**:
 - **True**: use additional PBE hash cycles.
 - **False**: do not use additional PBE hash cycles.
- d. For **jceVendor**, you can choose to use a non-default JCE provider. If the box is empty, the default provider is used.
- e. For **autoUpdateProbe**, specify **True** or **False**:
 - **True**: the server distributes the new key to the Probes automatically.
 - **False**: the new key should be placed on the Probes manually.
- f. For **exportEncryptionKey**, specify **True** or **False**.
 - **True**: In addition to creating the new password and storing it in secured storage, the Server exports the new password to the file system (**c:\hp\UCMDB\UCMDBServer\conf\discovery\key.bin**). This option enables you to update Probes manually with the new password.
 - **False**: The new password is not exported to the file system. To update Probes manually, set **autoUpdateProbe** to False and **exportEncryptionKey** to True.

Note: Make sure that the Probe is up and connected to the server. If the Probe goes down, the key cannot reach the Probe. If you change the key before the Probe goes down, once the Probe is up again, the key is sent again to the Probe. However, if you have changed the key more than once before the Probe goes down, you must change the key manually through the JMX console. (Select **False** for **exportEncryptionKey**).

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

Update an Encryption Key on a UCMDB Server

You use the **changeEncryptionKey** method to import your own encryption key to the UCMDB server and distribute it among all Probes.

To update an encryption key through the JMX Console:

1. Copy the `key.bin` file you generated in "[Generate a New Encryption Key](#)" on page 104 to the `C:\hp\UCMDB\UCMDBServer\conf\discovery\customer_1` directory, and rename the `key.bin` file. For example, `key_1.bin`.

Note: Make sure you rename the `key.bin` file.

2. On the UCMDB Server, launch the Web browser and enter the following address:
`http://localhost:8080/jmx-console`. You may have to log in with a user name and password.
3. Click **UCMDB:service=DiscoveryManager** to open the JMX MBEAN View page.
4. Locate the **changeEncryptionKey** operation.
 - a. In the **customerId** parameter box, enter **1** (the default).
 - b. For **newKeyFileName**, enter the name of the new key.
 - c. For **keySizeInBits**, specify the length of the encryption key. Valid values are 128, 192, or 256.
 - d. For **usePBE**, specify **True** or **False**:
 - **True:** use additional PBE hash cycles.
 - **False:** do not use additional PBE hash cycles.
 - e. For **jceVendor**, you can choose to use a non-default JCE provider. If the box is empty, the default provider is used.
 - f. For **autoUpdateProbe**, specify **True** or **False**:
 - **True:** the server distributes the new key to the Probes automatically.
 - **False:** the new key should be distributed manually using the Probe JMX console.

Note: Make sure that the Probe is up and connected to the server. If the Probe goes down, the key cannot reach the Probe. If you change the key before the Probe goes down, once the Probe is up again, the key is sent again to the Probe. However, if you have changed the key more than once before the Probe goes down, you must change the key manually through the JMX console. (Select **False** for **autoUpdateProbe**).

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

Update an Encryption Key on a Probe

If you choose not to distribute an encryption key from the UCMDDB Server to all Probes automatically (because of security concerns), you should download the new encryption key to all Probes and run the **importEncryptionKey** method on the Probe:

1. Place the encryption key file in **C:\hp\UCMDB\DataFlowProbe\conf\security**.
2. On the Probe machine, launch the Web browser and enter the following address:
http://localhost:1977.

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

Note: If the Probe Manager and the Probe Gateway are running as separate processes, the address should be entered on the machine that is running the Probe Manager as follows:
http://localhost:1978.

3. On the Probe domain, click **type=SecurityManagerService**.
4. Locate the **importEncryptionKey** method.
5. Enter the name of the encryption key file that resides in **C:\hp\UCMDB\DataFlowProbe\conf\security**. This file contains the key to be imported.
6. Click the **importEncryptionKey** button.
7. Perform a restart of the probe.

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

1. On the Probe Manager machine, start the Probe Manager service (**Start > Programs > HP UCMDDB > Probe Manager**).

2. Import the key from the server, using the Probe Manager JMX. For details, see "[Generate a New Encryption Key](#)" on page 104.
3. After the encryption key is imported successfully, restart the Probe Manager and Probe Gateway services.

Define Several JCE Providers

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

To change the default JCE provider:

1. Register the JCE provider jar files in **\$JRE_HOME/lib/ext**.
2. Copy the jar files to the \$JRE_HOME folder:
 - 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 website.
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.

How to Configure CAC Support on UCMDB

This section describes how to configure Smart Card Authentication or PKI Authentication (CAC) support on UCMDB.

Note: CAC support is only available when using Internet Explorer 8, 9, or 10.

1. Import the root CA and any intermediate certificates into the UCMDB Server Truststore as follows:

a. On the UCMDB machine, copy the certificate files to the following directory on UCMDB:

C:\HP\UCMDB\UCMDBServer\conf\security

Note: If your certificate is in Microsoft p7b format, you may need to convert it to PEM format.

b. For each certificate, run the following command:

```
C:\HP\UCMDB\UCMDBServer\bin\jre\bin\keytool.exe -import -v -keystore  
C:\HP\UCMDB\UCMDBServer\conf\security\server.truststore -file  
<certificate> - alias <certificate alias>
```

c. Enter the UCMDB Server Truststore password (default **hpass**).

d. When asked, **Trust this certificate?**, press **y** and then **Enter**.

e. Make sure the output **Certificate** was added to the keystore.

2. Open the JMX console by launching the Web browser and entering 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.

3. Under UCMDB, click **UCMDB:service=Ports Management Services** to open the Operations page.

■ (optional) Click **ComponentsConfigurations**. Do the following:

○ Set **HTTPSetPort** to **8444** and click **Invoke**.

○ Click **Back to MBean**.

■ Click **mapComponentToConnectors**. Do the following:

○ In the mapComponentToConnectors service, set **componentName** to **ucmdb-ui**.

○ Set only **isHTTPSWithClientAuth** to **true**, and click **Invoke**.

○ Click **Back to MBean**.

- In the `mapComponentToConnectors` service, set **componentName** to **root**.
 - Set only **isHTTPSWithClientAuth** to **true**, and click **Invoke**.
4. Under UCMDB, click **UCMDB:service=Security Services** to open the Operations page. In the **loginWithCAC** service, do the following:
- Set **loginWithCAC** to **true**, and click **Invoke**.
 - Click **Back to MBean**.
 - (optional) Click **usernameField** to specify the field from the certificate that will be used by UCMDB to extract a username, and click **Invoke**.

Note: If you do not specify a field, the default of `PRINCIPAL_NAME_FROM_SAN_FIELD` is used.

- Click **Back to MBean**.
- Click **pathToCRL** to set a path to an offline Certificate Revocation List (CRL) to be used if the online list (from the certificate) is not available, and click **Invoke**.

Note: When you are working with a local CRL and there is a working Internet connection to the UCMDB server, the local CRL is used. The validation of any certificate (even if it is not revoked) fails in the following situations:

- if the CRL path is set but the CRL file itself is missing
- if the CRL is expired
- if the CRL has an incorrect signature

If you do not set the path to an offline CRL and the UCMDB server cannot access the online CRL, all certificates that contain a CRL or OCSP URL are rejected (since the URL cannot be accessed, the revocation check fails). To give the UCMDB server access to the Internet, uncomment the following lines in the **wrapper.conf** file and provide a valid proxy and port:

```
#wrapper.java.additional.40=-Dhttp.proxyHost=<PROXY_ADDR>
#wrapper.java.additional.41=-Dhttp.proxyPort=<PORT>
#wrapper.java.additional.42=-Dhttps.proxyHost=<PROXY_ADDR>
#wrapper.java.additional.43=-Dhttps.proxyPort=<PORT>
```

- Click **Back to MBean**.
- (optional) Set **onlyCACCCerts** to **true**, and click **Invoke**.

Set this operation to **true** to accept only certificates that come from a physical CAC device.

You should now be able to log into UCMDB with `https://<UCMDB Server Host Name or IP>.<domainname>:8444`.

5. Configure UCMDB to use LW-SSO authentication and restart the UCMDB Server.

For details on LW-SSO authentication, see "Enabling Login to HP Universal CMDB with LW-SSO" in the *HP Universal CMDB and Configuration Manager Hardening Guide*.

How to Configure CAC Support for UCMDB by Reverse Proxy

This section describes how to configure Common Access Card (CAC) support on UCMDB using a reverse proxy.

1. Open the JMX console by launching the Web browser and entering 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=Ports Management Services** to open the Operations page.

- (optional) Click **ComponentsConfigurations**. Do the following:
 - Set **HTTPSetPort** to **8080** and click **Invoke**.
 - Click **Back to MBean**.
- Click **mapComponentToConnectors**. Do the following:
 - In the `mapComponentToConnectors` service, set **componentName** to **ucmdb-ui**.
 - Set only **isHTTP** to **true**, and click **Invoke**.
 - Click **Back to MBean**.

- In the mapComponentToConnectors service, set **componentName** to **root**.
 - Set only **isHTTP** to **true**, and click **Invoke**.
3. Under UCMDB, click **UCMDB:service=Security Services** to open the Operations page.
- Set **loginWithCAC** to **true**, and click **Invoke**.
 - Click **Back to MBean**.
 - Set **withReverseProxy** to **true**, and click **Invoke**.

This setting tells the UCMDB server to extract from the UCMDB_SSL_CLIENT_CERT header the user name to be used in UCMDB and the certificate to be used for authentication.

- Click **Back to MBean**.
- (optional) Set **onlyCAC Certs** to **true**, and click **Invoke**.

Set this operation to **true** to accept only certificates that come from a physical CAC device.

- (optional) Click **usernameField** to specify the field from the certificate that will be used by UCMDB to extract a username, and click **Invoke**.

Note: If you do not specify a field, the default of PRINCIPAL_NAME_FROM_SAN_FIELD is used.

4. Restart the UCMDB Server.

Example: Apache 2.4.4 Configuration

This section describes a sample configuration file for Apache 2.4.4.

Note: This example presumes that the Apache server was installed in **c:\Apache24**; if it is installed in a different folder, you must change the example in all cases to specify the correct location.

The port for mutual authentication used in this example is 443. In the **c:\Apache24\conf** folder, copy the following:

- the certificate used by the apache server (**server.crt**)
- the private key of the Apache server (**server.key**)
- the trusted CAs of the Apache server (**ssl.crt**)
- the certification revocation list (**ssl.crt**).

Note: These four files must all be in PEM format.

Replace the content of **c:\Apache24\conf\httpd.conf** with the following (change the [APACHE_MACHINE_FQD] accordingly):

```
ServerRoot "c:/Apache24"
Listen 80
LoadModule access_compat_module modules/mod_access_compat.so
LoadModule actions_module modules/mod_actions.so
LoadModule alias_module modules/mod_alias.so
LoadModule allowmethods_module modules/mod_allowmethods.so
LoadModule asis_module modules/mod_asis.so
LoadModule auth_basic_module modules/mod_auth_basic.so
LoadModule authn_core_module modules/mod_authn_core.so
LoadModule authn_file_module modules/mod_authn_file.so
LoadModule authz_core_module modules/mod_authz_core.so
LoadModule authz_groupfile_module modules/mod_authz_groupfile.so
LoadModule authz_host_module modules/mod_authz_host.so
LoadModule authz_user_module modules/mod_authz_user.so
LoadModule autoindex_module modules/mod_autoindex.so
LoadModule cgi_module modules/mod_cgi.so
LoadModule dir_module modules/mod_dir.so
LoadModule env_module modules/mod_env.so
LoadModule headers_module modules/mod_headers.so
LoadModule include_module modules/mod_include.so
LoadModule isapi_module modules/mod_isapi.so
LoadModule log_config_module modules/mod_log_config.so
LoadModule mime_module modules/mod_mime.so
LoadModule negotiation_module modules/mod_negotiation.so
LoadModule proxy_module modules/mod_proxy.so
LoadModule proxy_html_module modules/mod_proxy_html.so
LoadModule proxy_http_module modules/mod_proxy_http.so
LoadModule setenvif_module modules/mod_setenvif.so
LoadModule socache_shmcb_module modules/mod_socache_shmcb.so
LoadModule ssl_module modules/mod_ssl.so
LoadModule xml2enc_module modules/mod_xml2enc.so
<IfModule unixd_module>
User daemon
Group daemon
```

```
</IfModule>
ServerAdmin admin@example.com
ServerName [APACHE_MACHINE_FQD]:80
<Directory />
    AllowOverride none
    Require all denied
</Directory>
DocumentRoot "c:/Apache24/htdocs"
<Directory "c:/Apache24/htdocs">
    Options Indexes FollowSymLinks
    AllowOverride None
    Require all granted
</Directory>
<IfModule dir_module>
    DirectoryIndex index.html
</IfModule>
<Files ".ht*">
    Require all denied
</Files>
ErrorLog "logs/error.log"
LogLevel warn
<IfModule log_config_module>
    LogFormat "%h %l %u %t \"%r\" %>s %b \"%{Referer}i\" \"%{User-Agent}i\""
combined
    LogFormat "%h %l %u %t \"%r\" %>s %b" common
    <IfModule logio_module>
        LogFormat "%h %l %u %t \"%r\" %>s %b \"%{Referer}i\" \"%{User-Agent}i\" %I
%O" combinedio
    </IfModule>
    CustomLog "logs/access.log" common
</IfModule>
<IfModule alias_module>
    ScriptAlias /cgi-bin/ "c:/Apache24/cgi-bin/"
</IfModule>
<IfModule cgid_module>
</IfModule>
<Directory "c:/Apache24/cgi-bin">
    AllowOverride None
    Options None
    Require all granted
</Directory>
<IfModule mime_module>
    TypesConfig conf/mime.types
    AddType application/x-compress .Z
    AddType application/x-gzip .gz .tgz
</IfModule>
<IfModule proxy_html_module>
Include conf/extra/proxy-html.conf
```

```

</IfModule>
Include conf/extra/httpd-ssl.conf
<IfModule ssl_module>
SSLRandomSeed startup builtin
SSLRandomSeed connect builtin
</IfModule>

```

Also, replace the content of **c:\Apache24\conf\extra\httpd-ssl.conf** with the following (change the [APACHE_MACHINE_FQD], [UCMDB_SERVER_NAME], and [UCMDB_CM_SERVER_NAME] accordingly):

```

Listen 443
SSLCipherSuite HIGH:MEDIUM:!aNULL:!MD5
SSLPassPhraseDialog builtin
SSLSessionCache "shmcb:c:/Apache24/logs/ssl_scache(512000)"
SSLSessionCacheTimeout 300
<VirtualHost _default_:443>
DocumentRoot "c:/Apache24/htdocs"
ServerName [APACHE_MACHINE_FQD]:443
ServerAdmin admin@example.com
ErrorLog "c:/Apache24/logs/error.log"
TransferLog "c:/Apache24/logs/access.log"
SSLEngine on
SSLCertificateFile "c:/Apache24/conf/server.crt"
SSLCertificateKeyFile "c:/Apache24/conf/server.key"
SSLCACertificateFile "c:/Apache24/conf/ssl.crt"
SSLCARevocationFile "c:/Apache24/conf/ssl.crl"
SSLCARevocationCheck leaf
SSLVerifyClient require
SSLVerifyDepth 10
SSLOptions +ExportCertData
<FilesMatch "\.(cgi|shtml|phtml|php)$">
    SSLOptions +StdEnvVars
</FilesMatch>
<Directory "c:/Apache24/cgi-bin">
    SSLOptions +StdEnvVars
</Directory>
BrowserMatch "MSIE [2-5]" \
    nokeepalive ssl-unclean-shutdown \
    downgrade-1.0 force-response-1.0
CustomLog "c:/Apache24/logs/ssl_request.log" \
    "%t %h %{SSL_PROTOCOL}x %{SSL_CIPHER}x \"%r\" %b"
RequestHeader set UCMDB_SSL_CLIENT_CERT %{SSL_CLIENT_CERT}e
ProxyRequests off
<Proxy *>
    Order deny,allow
    Deny from all
    Allow from all
</Proxy>
ProxyPass / http://[UCMDB_SERVER_NAME]:8080/

```

```
ProxyPassReverse / http://[UCMDB_SERVER_NAME]:8080/
ProxyPass /mam http://[UCMDB_SERVER_NAME]:8080/mam
ProxyPassReverse /mam http://[UCMDB_SERVER_NAME]:8080/mam
ProxyPass /mam_images http://[UCMDB_SERVER_NAME]:8080/mam_images
ProxyPassReverse /mam_images http://[UCMDB_SERVER_NAME]:8080/mam_images
ProxyPass /mam-collectors http://[UCMDB_SERVER_NAME]:8080/mam-collectors
ProxyPassReverse /mam-collectors http://[UCMDB_SERVER_NAME]:8080/mam-collectors
ProxyPass /ucmdb http://[UCMDB_SERVER_NAME]:8080/ucmdb
ProxyPassReverse /ucmdb http://[UCMDB_SERVER_NAME]:8080/ucmdb
ProxyPass /site http://[UCMDB_SERVER_NAME]:8080/site
ProxyPassReverse /site http://[UCMDB_SERVER_NAME]:8080/site
ProxyPass /ucmdb-ui http://[UCMDB_SERVER_NAME]:8080/ucmdb-ui
ProxyPassReverse /ucmdb-ui http://[UCMDB_SERVER_NAME]:8080/ucmdb-ui
ProxyPass /status http://[UCMDB_SERVER_NAME]:8080/status
ProxyPassReverse /status http://[UCMDB_SERVER_NAME]:8080/status
ProxyPass /jmx-console http://[UCMDB_SERVER_NAME]:8080/jmx-console
ProxyPassReverse /jmx-console http://[UCMDB_SERVER_NAME]:8080/jmx-console
ProxyPass /axis2 http://[UCMDB_SERVER_NAME]:8080/axis2
ProxyPassReverse /axis2 http://[UCMDB_SERVER_NAME]:8080/axis2
ProxyPass /icons http://[UCMDB_SERVER_NAME]:8080/icons
ProxyPassReverse /icons http://[UCMDB_SERVER_NAME]:8080/icons
ProxyPass /ucmdb-api http://[UCMDB_SERVER_NAME]:8080/ucmdb-api
ProxyPassReverse /ucmdb-api http://[UCMDB_SERVER_NAME]:8080/ucmdb-api
ProxyPass /ucmdb-docs http://[UCMDB_SERVER_NAME]:8080/ucmdb-docs
ProxyPassReverse /ucmdb-docs http://[UCMDB_SERVER_NAME]:8080/ucmdb-docs
ProxyPass /ucmdb-api/8.0 http://[UCMDB_SERVER_NAME]:8080/ucmdb-api/8.0
ProxyPassReverse /ucmdb-api/8.0 http://[UCMDB_SERVER_NAME]:8080/ucmdb-api/8.0
ProxyPass /cm http://[UCMDB_SERVER_NAME]:8080/cm
ProxyPassReverse /cm http://[UCMDB_SERVER_NAME]:8080/cm
ProxyPass /cnc http://[UCMDB_CM_SERVER_NAME]/cnc
ProxyPassReverse /cnc http://[UCMDB_CM_SERVER_NAME]/cnc
ProxyPass /docs http://[UCMDB_CM_SERVER_NAME]/docs
ProxyPassReverse /docs http://[UCMDB_CM_SERVER_NAME]/docs
ProxyPass /ucmdb-browser http://[UCMDB_CM_SERVER_NAME]/ucmdb-browser
ProxyPassReverse /ucmdb-browser http://[UCMDB_CM_SERVER_NAME]/ucmdb-browser
```

```
</VirtualHost>
```

Now you can access the UC MDB server through revers proxy by going to [https://\[APACHE_MACHINE_FQD\]](https://[APACHE_MACHINE_FQD]).

Note: You must have a valid certificate imported in Internet Explorer. A valid certificate is one that was signed by a CA of the Apache trusted CAs (it must be present in the **ssl.crt** file).

How to Harden the Data Flow Probe Connector in UCMDB

1. Access the UCMDB JMX console: In your Web browser, enter the following URL: **http://<ucmdb machine name or IP address>:8080/jmx-console**. You may have to log in with a user name and password.
2. Select the service: **Ports Management Services**.
3. Invoke the **PortsDetails** method, and note the port number for HTTPS. (Default: 8443) Ensure that the value in the **Is Enabled** column is **True**.
4. Return to **Ports Management Services**.
5. To map the Data Flow Probe connector to server authentication mode, invoke the **mapComponentToConnectors** method with the following parameters:
 - **componentName**: mam-collectors
 - **isHTTPS**: true
 - **All other flags**: false

The following message is displayed:

Operation succeeded. Component mam-collectors is now mapped to: HTTPS ports.

6. Return to **Ports Management Services**.
7. To map the Confidential Manager connector to server authentication mode, invoke the **mapComponentToConnectors** method with the following parameters:
 - **componentName**: cm
 - **isHTTPS**: true
 - **All other flags**: false

The following message is displayed:

Operation succeeded. Component cm is now mapped to: HTTPS ports.

How to Encrypt the Probe Keystore and Truststore Passwords

The Probe keystore and truststore passwords are stored encrypted in **C:\HP\UCMDB\DataFlowProbe\conf\security\ssl.properties**. This procedure explains how to encrypt the password.

1. Start Data Flow Probe (or verify that it is already running).
2. Access the Data Flow Probe JMX console: Launch a Web browser and enter the following address: `http://<Data Flow Probe machine name or IP address>:1977`. If you are running the Data Flow Probe locally, enter `http://localhost:1977`.

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

3. Locate the **Type=MainProbe** service and click the link to open the Operations page.
4. Locate the **getEncryptedKeyPassword** operation.
5. Enter your keystore or truststore password in the **Key Password** field and invoke the operation by clicking **getEncryptedKeyPassword**.
6. The result of the invocation is an encrypted password string, for example:

`66,85,54,78,69,117,56,65,99,90,86,117,97,75,50,112,65,53,67,114,112,65,61,61`
7. Copy and paste the encrypted password into the line relevant to either the keystore or the truststore in the following file: **C:\HP\UCMDB\DataFlowProbe\conf\security\ssl.properties**.

How to Enable Login to HP Universal CMDB with LW-SSO

1. Access the JMX console by entering the following address into your Web browser: **http://<server_name>:8080/jmx-console**, where **<server_name>** is the name of the machine on which HP Universal CMDB is installed.
2. Under **UCMDB-UI**, click the **name=LW-SSO Configuration** to open the Operations page.
3. Set the init string using the **setInitString** method.
4. Set the domain name of the machine on which UCMDB is installed using the **setDomain** method.
5. Invoke the method **setEnabledForUI** with the parameter set to **True**.
6. **Optional.** If you want to work using multi-domain functionality, select the **addTrustedDomains** method, enter the domain values and click **Invoke**.
7. **Optional.** If you want to work using a reverse proxy, select the **updateReverseProxy** method, set the **is reverse proxy enabled** parameter to **True**, enter a URL for the **Reverse proxy full server URL** parameter, and click **Invoke**. If you want to access UCMDB both directly and using a reverse proxy, set the following additional configuration: select the **setReverseProxyIPs** method, enter the IP address for the **Reverse proxy ip/s** parameter and click **Invoke**.
8. **Optional.** If you want to access UCMDB using an external authentication point, select the **setValidationPointHandlerEnable** method, set the **is validation point handler enabled** parameter to **True**, enter the URL for the authentication point in the **Authentication point server** parameter, and click **Invoke**.
9. To view the LW-SSO configuration as it is saved in the settings mechanism, invoke the **retrieveConfigurationFromSettings** method.
10. To view the actual loaded LW-SSO configuration, invoke the **retrieveConfiguration** method.

Note: You cannot enable LW-SSO via the user interface.

How 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:service=LDAP Services** to open the Operations page.
3. Locate **testLDAPConnection**.
4. In the **Value** box for the parameter **customer id**, enter the customer ID.
5. Click **Invoke**.

The JMX MBEAN Operation Result page indicates whether the LDAP connection is successful. If the connection is successful, the page also shows the LDAP root groups.

How to Enable and Define the LDAP Authentication Method

This task describes how to configure LDAP authentication settings using the JMX console.

Note:

- In a high availability environment, make sure you log in to the JMX console of the Writer server.
- You can also configure LDAP authentication settings in UCMDB. For details, see "How to Enable and Define the LDAP Authentication Method" in the *HP Universal CMDB and Configuration Manager Hardening Guide*.
- For an example of LDAP authentication settings, see "LDAP Authentication Settings - Example" in the *HP Universal CMDB and Configuration Manager Hardening Guide*.

To configure LDAP authentication settings:

1. Launch your Web browser and enter the following address: **http://<server_name>:8080/jmx-console**, where **<server_name>** is the name of the machine on which HP Universal CMDB is installed.

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

2. Under **UCMDB**, click **UCMDB:service=LDAP Services** to open the Operations page.
3. To view the current LDAP authentication settings, locate the **getLDAPSettings** method. Click **Invoke**. A table displays all the LDAP settings and their values.
4. To change the values of LDAP authentication settings, locate the **configureLDAP** method. Enter the values for the relevant settings and click **Invoke**. The JMX MBEAN Operation Result page indicates whether the LDAP authentication settings were updated successfully.

Note: If you do not enter a value for a setting, the setting retains its current value.

5. After configuring the LDAP settings, you can verify the LDAP user credentials:
 - a. Locate the **verifyLDAPCredentials** method.
 - b. Enter the customer ID, username, and password.
 - c. Click **Invoke**.

The JMX MBEAN Operation Result page indicates whether the user passes LDAP authentication.

6. **Important:** If you are configuring LDAP on a high availability environment, you must restart the cluster for the changes to take effect.

Note: Every LDAP user has a first name, last name, and email address saved in the local repository. If the value of any of these parameters that is stored on the LDAP server differs from the value in the local repository, the LDAP server values will overwrite the local values at each login.

How to Configure the HP Universal CMDB Server with Confidential Manager

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 Confidential Manager 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.

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.

In most cases there is no need to restart the Server. You may need to restart the Server when changing one of the following resources:

- Storage type
- Database table name or column names
- The creator of the database connection

- The connection properties to the database (that is, URL, user, password, driver class name)
- Database type

Note:

- It is important that the UCMDB Server and its clients have the same transport crypto-properties. If these properties are changed on the UCMDB Server, you must change them on all clients. (This is not relevant for the Data Flow Probe because it runs on the same process as the UCMDB Server—that is, there is no need for the Transport crypto-configuration.)
- Confidential Manager Replication is not configured by default, and can be configured if needed.
- If Confidential Manager Replication is enabled, and the Transportation **initString** or any other crypto-property of the master changes, all slaves must adopt the changes.

How to Set the IIS server as the Front-End Server for UCMDB

1. Launch the Web browser and enter the following address:

http://<UCMDB server name>:<port>/jmx-console.

2. Click **UCMDB-UI:name=UI Server frontend settings** to open the JMX MBEAN View page.
3. Click the **setUseFrontendURLBySettings** method and enter the address of the IIS server as the value (**http://<IIS server name>:<port>**).
4. Click **Invoke**.

Note: You cannot open the JMX Console from IIS. That is, basic authentication cannot be passed from Jetty.

Chapter 8: Installation and Migration Methods

This chapter includes:

How to Integrate UCMDB with SiteMinder	124
How to Migrate DDMI Server Configuration Data to Universal Discovery	125

How to Integrate UCMDB with SiteMinder

The following procedure enables integration of UCMDB with SiteMinder:

1. Prerequisites:

- Ensure that CA SiteMinder is installed on your user environment.
- Ensure that Microsoft IIS Web Server is installed on the same machine as the CA SiteMinder Client Agent.

2. Set up IIS to enable access to UCMDB.

3. Enable AJP connections.

In the Administration module, select **Infrastructure Settings Manager > General Settings**, and set **Enable AJP Connections** to **True**.

4. Configure UCMDB to enable LW-SSO:

- Enable logging in to UCMDB with LW-SSO. For details, see the [HP Universal CMDB and Configuration Manager Hardening Guide](#).
- In the JMX console, go to **UCMDB-UI:name=LW-SSO Configuration**. Invoke the **setUserName** method and set the LW-SSO IDM user name settings as follows:
 - **Is inbound handler enabled = True**
 - **LW-SSO IDM User Name = sm-user**

5. Verify successful integration of UCMDB with SiteMinder.

Access **http://ucmdb-server/ucmdb-ui** using the user name and password in your user directory.

After SiteMinder validates the user credentials, you are forwarded directly to UCMDB with no need to enter your UCMDB user name and password.

How to Migrate DDMI Server Configuration Data to Universal Discovery

The following task describes how to migrate DDMI server configuration data to Universal Discovery. Migration tools, including Perl scripts and a JMX console are provided which automatically export DDMI server data and automatically import the data to UCMDB. In most cases, server data from DDMI is migrated into newly-created activities in UCMDB. For more information about activities in UCMDB, see the *HP UCMDB Discovery and Integrations Content Guide*.

Note:

- Perform this task for each DDMI server that you want to migrate.
- DDMI Aggregator Server configuration data is not supported.
- Data Flow Probes that are members of probe clusters are not supported and should not be migrated.
- To ensure Agent-related information, such as software utilization and callhome configuration data, is migrated, select the **Deploy** option in the Agent Deployment Actions field on the Agent Profile page.

This task includes the following steps:

1. ["Prerequisite" below](#)
 2. ["Run the export script" on the next page](#)
 3. ["Copy the archive file" on page 127](#)
 4. ["Import the migration data" on page 127](#)
 5. ["Results" on page 128](#)
1. Prerequisite
 - Ensure that UCMDB is running.

Note: For information about installing UCMDB, see the interactive *HP Universal CMDB Deployment Guide*.

- Ensure that the DDMI server database is running.
 - (Optional) Back up the UCMDB database. For more information, see the documentation for your database product
 - If you want the discovery schedules that are contained in DDMI network profiles to migrate to Universal Discovery, ensure that the Force ARP Table to Be Read option is selected.
 - (Optional) If you do not know the **customer id** parameter for the customer you are migrating, do the following:
 - i. In UCMDB, go to **Data Flow Management > Data Flow Probe Setup**.
 - ii. In the **Domains and Probes** pane, select a Data Flow Probe and note the customer name at the top right of the window.
 - iii. Go to the **JMX console > Customer & States > Show all Customers** method and note the **customer Id** that maps to the customer name.
 - (Optional) To validate that devices were migrated, run a Perl script on each DDMI Server that generates a device inventory report. The data in this report can be compared with data in UCMDB after migration, and it is useful for troubleshooting purposes. For more information, see *How to Run the Device Inventory Report* in the *HP Universal CMDB DDMI to Universal Discovery Migration Guide*
2. Run the export script
- a. Locate the **DDMIMigration.pl** script on the UCMDB Server at the following location:
 - **Windows: C:\hp\UCMDB\UCMDBServer\tools\migration**
 - **Linux: C:/opt/hp/UCMDB/UCMDBServer/tools/migration**
 - b. Copy the script to any directory on each DDMI server that you want to migrate.
 - c. For each DDMI server, open a Command prompt and navigate to the directory where you copied the script. At the Command prompt, run the following command:

perl DDMIMigration.pl

You should see the following message:

"The migration data is successfully saved to **DDMIMigrationData.zip**".

Note:

- By default, the data is archived in a file called **DDMIMigrationData.zip**.
- Maximum amount of device groups that can be imported is 20. If device groups exceed 20, remove some groups and run the script again. Then, create the remaining management zones in Universal Discovery manually.

3. Copy the archive file

Copy the archive file that was created in step 2 to the following location on the UCMDB Server:

- Windows: **C:\hp\UCMDB\UCMDBServer\conf\discovery\customer_<customer id>**
- Linux: **C:/opt/hp/UCMDB/UCMDBServer/conf/discovery/customer_<customer id>**

where **customer id** is the value for the **customer id** parameter.

Note: Usually, this value is **1** by default.

4. Import the migration data

- a. Open the JMX Console and go to **Discovery Manager > ImportMigrationDataFromDDMI**.
- b. In the **importMigrationDataFromDDMI** method, the following parameters are displayed:
 - **customerId**. The customer ID that you want to migrate.
 - **isCreateActivity**.
 - **True**. Creates new activities in Management Zones. These activities contain the migrated data.
 - **False**. No activities are created. However, Management Zones are created.
 - **Primary|Secondary Call Home Address**. The primary and the secondary call home

IP addresses for the Data Flow Probe.

For example:

<UD_CallHomeIPAddressPrimary> , <UD_CallHomeIPAddressSecondary>

Note:

- If this field is left blank, the IP address of the Data Flow Probe is used.
 - In some cases, data that is entered in these fields may not appear in the UCMDB Infrastructure activity. In these cases, reenter the data in the activity.
 - The DDMI call home IP addresses are pre-populated, so it is not necessary to enter this information.
- **probeName.** The name of the Data Flow Probe to which to map the data.
 - **configurationzipPackageName.** The name of the archive file that was created in step 2.
 - **overrideGlobalConfig.**
 - **True.** The XML Enricher global configuration file in UCMDB is overwritten by the DDMI configuration file.
 - **False.** The XML Enricher global configuration file in UCMDB is not overwritten and the DDMI configuration file is ignored.
 - **stopWhenConflict.**

Specifies how to handle IP address range conflicts.

- **True.** If overlapping IP address ranges exist in DDMI and UCMDB, no IP address ranges are imported to UCMDB.
- **False.** If the same IP address range exists in UCMDB, only IP address ranges that are not in conflict are imported. Ranges that are in conflict are ignored. Additionally, Management Zones that contained the conflicted ranges are not imported.

5. Results

- Success messages and warning messages are displayed.

- In addition to the data that is contained in the archive file that was created in step 2, the following information is imported into UCMDB:
 - **Deployment credentials.** Credentials are imported and keys are regenerated automatically.
 - **SNMP configuration profile.**
 - **Device groups.**
 - **System configuration.**
 - **VMWare configuration.**
 - **XML Enricher configuration file.**
 - **Certificates**
 - acstrust.cert
 - agentca.pem
 - acskeystore.bin
 - **IP address ranges.**
- Additionally, the following resources are imported:
 - Pre-scan and post-scan scripts
 - Scanner configuration files (.cxz)
 - User SAI files

Send Documentation Feedback

If you have comments about this document, you can [contact the documentation team](#) by email. If an email client is configured on this system, click the link above and an email window opens with the following information in the subject line:

Feedback on JMX Reference Guide (Universal CMDB 10.20)

Just add your feedback to the email and click send.

If no email client is available, copy the information above to a new message in a web mail client, and send your feedback to cms-doc@hp.com.

We appreciate your feedback!