



Universal CMDB

Software Version: 10.31

Release Notes

Document Release Date: December 2016

Software Release Date: December 2016



Hewlett Packard
Enterprise

Legal Notices

Warranty

The only warranties for Hewlett Packard Enterprise 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. Hewlett Packard Enterprise 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 Hewlett Packard Enterprise 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 - 2016 Hewlett Packard Enterprise Development LP

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

To check for recent updates or to verify that you are using the most recent edition of a document, go to: <https://softwaresupport.hpe.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 HPE Software 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 HPE sales representative for details.

Support

Visit the HPE Software Support site at: <https://softwaresupport.hpe.com/>.

This website provides contact information and details about the products, services, and support that HPE Software offers.

HPE 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 HPE 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 HPE 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>.

HPSW Integrations Catalog accesses the new HPSW Integrations and Solutions Catalog website. This site enables you to explore HPE Product Solutions to meet your business needs, includes a full list of Integrations between HPE Products, as well as a listing of ITIL Processes. The URL for this website is <https://softwaresupport.hpe.com/km/KM01702731>.

Contents

HPE Universal CMDB and HPE Universal Discovery Release Notes	4
Installation Notes	5
HPE Universal CMDB 10.31 Files/Components	5
System Requirements	6
Install Version 10.31 on the UCMDB Servers	7
Upgrade HPE Universal CMDB 10.31 Data Flow Probe Manually	9
Install a New HPE Universal CMDB 10.31 Data Flow Probe	10
Universal CMDB 10.31 Uninstall Procedure	16
Re-Enable the FIPS Mode for Configuration Manager	18
Known Problems, Limitations, and Workarounds	20
Tenant Owner Related Known Issues, Problems, and Workaround ...	48
Enhancements Requests	51
Fixed Defects for UCMDB and UD 10.31	54
How to Configure Configuration Manager 10.22 to Connect to UCMDB Server	62
Send documentation feedback	64

HPE Universal CMDB and HPE Universal Discovery Release Notes

Software version: 10.31

Publication date: December 2016

This document provides information about version 10.31 of the HPE Configuration Management System, which consists of HPE Universal CMDB 10.31 (UCMDB) and HPE UCMDB Universal Discovery 10.31 (UD). It contains important information that is not included in books or Help. You can find information about the following in this document:

["Installation Notes" on the next page](#)

["Known Problems, Limitations, and Workarounds" on page 20](#)

["Enhancements Requests" on page 51](#)

["Fixed Defects for UCMDB and UD 10.31"](#)

Important Note: The HPE Configuration Management System (UCMDB and UD) version 10.31 is a lightweight and easy to deploy release (similar to a CUP release), where the probes are automatically upgraded as part of the process. HPE strongly encourages you to move to UCMDB version 10.31 and the accompanying Content Pack 22.00. There will be no further CUP releases on top of UCMDB version 10.30.

Note: Before deploying Content Pack 22.00, you must install version 10.31 on the UCMDB server, and deploy version 10.31 Data Flow Probes. Do not deploy Content Pack 22.00 while you are still updating the Data Flow Probes.

For supported versions of UCMDB and other information about HPE UCMDB Universal Discovery Content Pack 22.00, see the *Release Notes* for HPE UCMDB Universal Discovery Content Pack 22.00.

Note: Starting from version 10.30 of the HPE Configuration Management System, there is no new release for UCMDB Configuration Manager (CM). The latest release of CM is version 10.22 CUP4, you can use it (or a later CUP on top of version 10.22) in tandem with version 10.31 of Universal CMDB.

Installation Notes

HPE Universal CMDB 10.31 Files/Components

HPE Universal CMDB (UCMDB) and Data Flow Probe 10.31 are provided with the following files:

	Included Files
Windows	<p>The UCMDB_00189.zip includes the following files/components:</p> <ul style="list-style-type: none"> • HPUCMDB_Server_Patch_10.31.107.exe. Launches the installation of the version 10.31 HP UCMDB Server for the Windows platform. • HPUCMDB_DataFlowProbe_10.31.107.exe. Launches the installation of the version 10.31 HP UCMDB Data Flow Probe for the Windows platform. <p>This installer can also be used to deploy the Universal Discovery Inventory Tools in a standalone installation.</p> <ul style="list-style-type: none"> • *.sha256. Checksum files.
Linux	<p>The UCMDB_00190.zip includes the following files/components:</p> <ul style="list-style-type: none"> • HPUCMDB_Server_Patch_10.31.107.bin. Launches the installation of the version 10.31 HP UCMDB Server for the Linux platform. • HPUCMDB_DataFlowProbe_10.31.107.bin. Launches the installation of the version 10.31 HP UCMDB Data Flow Probe for the Linux platform (for integrations only). • *.sha256. Checksum files. • *.sig. Linux code signing files. For detailed instructions about how verify the code signatures, see HPE GPG or RPM Signature Verification. <p>Note: The current key used in this release is B564A643.</p>
Both	<ul style="list-style-type: none"> • Read Me (Read_Me.txt)

Note: The updated full documentation set (including both online help and PDF files) is available with the CMS 10.31 release. You can access the documentation from **Help > UCMDB Help** after upgrading UCMDB to version 10.31.

To read the *Support Matrix* and the *What's New* document before you proceed with the installation, click [Support Matrix](#) and [What's New](#).

System Requirements

For a list of system requirements, see the *HPE Universal CMDB Support Matrix* document (click [Support Matrix](#)). Check the most previous Release Notes for any additions or changes to the matrix.

Note: Embedded PostgreSQL is only supported for small deployments of UCMDB.

The table below describes supported upgrade paths for the HPE CMS products:

Supported Upgrade Paths

Supported Upgrade Paths	CMS product supporting upgrades		
	UCMDB	Data Flow Probe	UCMDB Browser ^{[1][2]}
10.30 > 10.31	Yes	Yes	No
10.30 FIPS > 10.31 FIPS	Yes	Yes	No
10.31 full installer	No	Yes	Yes

Supported Downgrade Paths

Supported Downgrade Paths	UCMDB Server	Data Flow Probe	UCMDB Browser
10.31 > 10.30	Yes	No	No
10.31 FIPS > 10.30 FIPS	Yes	No	No

Note:

1. UCMDB Browser does not support upgrades. You need to deploy the **HPE-Browser-<version_number>.<build_number>-all-in-one-standalone.zip** package for UCMDB Browser version 4.12 in order to perform a fresh deployment.
2. UCMDB server version 10.31 (or later) does not support embedded UCMDB Browser versions older than 4.10. For more details, see "[Software Coexistence](#)" on page 1.
3. Version 10.31 of the HPE Configuration Management System does not include a new release for UCMDB Configuration Manager (CM). The latest release of CM is version 10.22 CUP4, you can use it (or a later CUP on top of version 10.22) in tandem with UCMDB 10.31.

For supported upgrade path for Configuration Manager, check the [Release Notes for version 10.22](#). For documentation about Configuration Manager, see [HPE Universal CMDB Configuration Manager User Guide of version 10.22](#). To download the Release Notes for UCMDB 10.22 CUP4 (or a later CUP), go to [Overview of UCMDB 10.2x Releases](#).

Install Version 10.31 on the UCMDB Servers

Version 10.31 uses patch installers for HPE Universal CMDB and Data Flow Probe. The patch installer provides an installation wizard and performs automated installation.

You can still install the Data Flow Probes separately by upgrading the Data Flow Probes using the UCMDB user interface. For details, see "[Upgrade HPE Universal CMDB 10.31 Data Flow Probe Manually](#)" on page 9.

Pre-requisites - UCMDB Server and Data Flow Probes

1. Extract **UCMDB_00189.zip** (for Windows) or **UCMDB_00190.zip** (for Linux) to a temporary directory.
2. If you enabled basic authentication (BA), check the BA password to make sure that it meets the security policy. If not, update the BA password by following the instructions in the *Enable Basic Authentication between UCMDB Server and Data Flow Probe* section in the *HPE Universal CMDB Hardening Guide*.
3. Stop the Universal CMDB server and the HP Universal CMDB Integration Service (if running) before starting the 10.31 installation.

Note: If you have a High Availability configuration, 10.31 must be installed on all the servers in the cluster, and prior to the installation, you must stop all the servers in the cluster.

4. Back up the **<UCMDB installation folder>/UCMDBServer/lib** folder.
5. Back up the database.
6. If you have received private patches for the UCMDB Server or Data Flow Probe, you must delete these patches before upgrading the probe (no matter if you upgrade the probe by using the installation wizard, or you upgrade the probe by using the UCMDB user interface after the installation).

Follow these steps to delete a private patch:

- a. Delete all private patches from the UCMDB Server.
 - i. Stop the UCMDB server.
 - ii. Delete all private patches that were installed on the system prior to version 10.31 by deleting the following directory:

\\hp\UCMDB\UCMDBServer\classes

- b. Delete all private patches from the Data Flow Probe.
 - i. Stop the Data Flow Probe.
 - ii. Delete all private patches that were installed on the system prior to version 10.31 by deleting the following directory:

\\hp\UCMDB\DataFlowProbe\classes
 - iii. Start up the version 10.30 Data Flow Probe.

Note: The upgrade process may take longer than usual when the workload of the probe is heavy. For example, when the probe is busy with running discovery jobs.

Installation

1. For Universal CMDB Server, open the installation wizard by using the following method:
 - On Windows, double-click the file **HPUCMDB_Server_Patch_10.31.exe**.
 - On Linux, run the sh *<path to the installer>/HPUCMDB_Server_Patch_10.31.bin* command.

Note: On Linux, make sure the graphic environment is set up before running the command to open the installation wizard.

2. While running the wizard:
 - In the **Choose Install Folder** screen, select the installation directory in which UCMDB is already installed.
 - For UCMDB, in the **Install Data Flow Probe** screen, select one of the following options:
 - **Automatically update Data Flow Probe** to automatically update during this installation all the Data Flow Probes reporting to this UCMDB.

Note: Make sure all the Data Flow Probes you want upgrade are connected to the UCMDB server.

 - **Update the Data Flow Probe manually** to update the Data Flow Probes reporting to this UCMDB server manually after completing the installation on the UCMDB server. For details, see ["Upgrade HPE Universal CMDB 10.31 Data Flow Probe Manually" on the next page](#).
 - In the **Required Actions** screen, follow the instruction to ensure that the server is stopped.

3. Once the installation wizard for UCMDB is completed, start up the UCMDB server.
4. Verify and make sure that each of your Data Flow Probes has been successfully upgraded to version 10.31.

To do so, log in to UCMDB UI, go to **Data Flow Management > Data Flow Probe Setup**, check and make sure that the probe is on the same version with the UCMDB Server.

Note: Do not stop the probe unless you find the probe is not upgraded successfully.

5. (Optional) Clear user preferences.

On the Status Bar in UCMDB UI, click **Configure User Preferences** , and then in the User Preferences dialog box click **Reset All**.)

Note that this step is recommended but not a must. Also, it has no functional impact.

Upgrade HPE Universal CMDB 10.31 Data Flow Probe Manually

(Applicable only when **Update the Data Flow Probes manually** is selected in the installation wizard.)

The following steps upgrade all Data Flow Probes that are associated with the UCMDB server.

1. If you have received private patches for the Data Flow Probe, perform the steps in the section ["Pre-requisites - UCMDB Server and Data Flow Probes" on page 7](#).
2. In UCMDB, go to **Data Flow Management > Data Flow Probe Setup**, and then click **Deploy Probe Upgrade**.
3. In the Deploy Probe Upgrade dialog box, navigate to the **<SERVER_HOME>\content\probe_patch\probe-patch-10.31-windows.zip**, and then click **OK**.
4. Upgrade data flow probes using the **deployProbePatch** JMX method. To do so,
 - a. Launch the Web browser and navigate to: **https://<server_name>:8443/jmx-console**, where **<server_name>** is the name of the machine on which Universal CMDB is installed.
 - b. Go to **UCMDB:service=Discovery Manager**.
 - c. Locate **deployProbePatch**.
 - d. In the **Value** box for the parameter **customerId**, enter the **<customer id>**. The default value is **1**.

- e. In the **Value** box for the parameter **filePath**, enter the full file path of the patch file.
 - f. Click **Invoke**.
5. Verify and make sure that each of your Data Flow Probes has been successfully upgraded to version 10.31.

To do so, log in to UCMDB UI, go to **Data Flow Management > Data Flow Probe Setup**, check and make sure that the probe is on the same version with the UCMDB Server.

Note: Do not stop the probe unless you find the probe not upgraded successfully.

Note: For instructions about deploying a data flow probe CUP on all the connected Data Flow Probes, see the *HPE Universal CMDB Data Flow Management Guide*.

Install a New HPE Universal CMDB 10.31 Data Flow Probe

This section describes the procedure to install the Universal CMDB 10.31 Data Flow Probe on a new machine.

Preparation

The preparation tasks for installing the Universal CMDB 10.31 Data Flow Probe are the same as those for 10.30. For details, see the following sections in the *HPE Universal CMDB Deployment Guide* for version 10.30:

- *Data Flow Probe - Notes Before you install*
- *Data Flow Probe - Ports*

Note: You can access the *HPE Universal CMDB Deployment Guide* for version 10.30 from **UCMDB UI > Help > UCMDB Help > Get Started > Navigate the documentation > expand the HPE UCMDB Documentation Set** section. You can also download it from [here](#).

Install the Data Flow Probe

The following procedure describes how to install the Universal CMDB 10.31 Data Flow Probe on a new machine:

1. Start the Data Flow Probe installation wizard by using the following method:

- On Windows, double-click **HPUCMDB_DataFlowProbe_10.31.exe**.
- On Linux, run the following command:

```
sh <path to the installer>/HPUCMDB_DataFlowProbe_10.31.bin
```

2. Choose the locale language, and then click **OK**.
3. The Introduction page opens. Click **Next**.

Note: If an existing Data Flow Probe is detected, a prompt pops up asking you if you would like to install a second Data Flow Probe. Click **Yes** to proceed, or click **Cancel** to cancel the installation.

4. In the **License Agreement** page, accept the terms of the end-user license agreement, and then click **Next**.
5. (Windows only) The **Setup Type** page opens.

Select **Full Data Flow Probe Installation**. This installs the Data Flow Probe with all its components, including the Inventory Tools (Analysis Workbench, Viewer, SAI Editor, and MSI Scanner) required for application teaching.

Note: The **Inventory Tools** option is used to install only the Inventory Tools. For details about application teaching, see the *HPE Universal CMDB Data Flow Management Guide*.

Click **Next**.

6. In the **Select Installation Folder** page, accept the default installation folder, or click **Choose** to select a different installation folder, and then click **Next**.

If you install a second Data Flow Probe on the same Windows machine, specify a different installation folder or click **Choose** to select a different installation folder for the second probe, instead of using the one for the existing probe.

Note:

- The installation folder that you select must be empty.
- To restore the default installation folder, after selecting a different folder, click **Restore Default Folder**.
- On Linux, you can change the location of the installation, but the folder must be located under **/opt/**.

7. In the **Data Flow Probe Configuration** page, configure the details of the application server to

which the Data Flow Probe will report and then click **Next**.

Note: If you do not enter the address of the application server, or if there is no TCP connection to the application server via default ports (8443,80) (possibly because the application server has not fully started yet), a message is displayed. You can choose to continue to install the Probe without entering the address, or return to the previous page to add the address.

- Under **Application to report to** select **HP Universal CMDB** and in the **Application Server address** box, enter the name or the IP address of the HP Universal CMDB server with which the Probe is to connect.

Note:

- Two Probes installed on the same Windows machine should report to two different UCMDB servers respectively. For the second Probe you install, in the **Application Server address** box, make sure you enter the name or the IP address of a different UCMDB server.
 - In a High Availability environment, use the Writer virtual IP address of the load balancer.
- In the **Data Flow Probe address** box, enter the IP address or DNS name of the machine on which you are currently installing the Probe, or accept the default.

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

8. In the second **Data Flow Probe Configuration** page, configure an identifier for the Probe.

- In the **Data Flow Probe identifier** box, enter a name for the Probe that is used to identify it in your environment and then click **Next**.

Note:

- The Probe identifier is case sensitive, must be unique for each Probe in your deployment, and it must not exceed 50 characters.
- (Second Probe only) Make sure you enter a unique identifier for the second Probe.
- On Windows, when installing the Probe in separate mode (that is, the Probe Gateway and Probe Manager are installed on separate machines), you must give the same name to the Probe Gateway and all its Probe Managers. This name appears in UCMDB as a single Probe node. Failure to give the same name may prevent jobs from running.

- To use the default UCMDB IP address or machine name, as defined in the UCMDB Server installation, select **Use Default CMDB Domain**.

The Default UCMDB Domain is also configurable in UCMDB's Infrastructure Settings module. For details, see the *HPE Universal CMDB Administration Guide*.

9. If you cleared the **Use Default CMDB Domain** box in the previous step, specify the following information in the **HP UCMDB Data Flow Probe Domain Configuration** page, and then click **Next**.

- **Data Flow Probe domain type.** Select the type of domain on which the Probe is to run:
 - **Customer.** Select if you are installing one or more Probes in your deployment.

Note: Always use this option for new installations.

- **External.** Select this option for upgraded 6.x systems.
- **Data Flow Probe domain.** If you are not using the default domain defined in UCMDB enter the name of the domain here.

Note: For external domains, this value must be identical to the **Data Flow Probe identifier** defined in the previous step.

10. (Windows only) In the **Data Flow Probe Working Mode** page, specify if the Probe Gateway and Probe Manager are run as one Java process or as separate processes and then click **Next**.

Note:

- When installing the second Probe, this step is skipped.
- The Probe can be configured in separate mode in IPv4 environments, and in IPv4/IPv6 environments, but not in pure IPv6 environments.

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

Select **Yes** to run the Probe Gateway and Probe Manager as two processes on separate machines.

Note: When running the Probe Gateway and Probe Manager as two processes ensure the following:

- At least one Probe Gateway component must be installed. The Probe Gateway is connected to the UCMDB Server. It receives tasks from the Server and communicates with the collectors (Probe Managers).
- Several Probe Managers can be installed. The Probe Managers run jobs and gather

information from networks.

- The Probe Gateway should contain a list of attached Probe Managers.
- The Probe Managers must know to which Probe Gateway they are attached.

11. In the **Data Flow Probe Memory Size** page, define the minimum and maximum memory (in MB) to be allocated to the Probe, and then click **Next**.

Note: For information about changing the maximum heap size value at a later point in time, see the *HPE Universal CMDB Data Flow Management Guide*.

12. In the **PostgreSQL Account Configuration** page, set the password for the PostgreSQL Data Flow Probe account, and then click **Next**.

The PostgreSQL Data Flow Probe account is used by the Data Flow Probe to connect to the PostgreSQL database. This account is less privileged compared to the PostgreSQL root account. Its password is encrypted in the **DataFlowProbeOverride.properties** configuration file.

13. In the second **PostgreSQL Account Configuration** page, set the password for the PostgreSQL root account, and then click **Next**.

The PostgreSQL root account is the account used to administer the PostgreSQL database. When set, it may need to be provided while executing scripts under the Probe's installation.

Note: Changing the root account password does not affect operation of the Probe.

14. In the **Configuration for System Administrator Password** page, set the password for the system administrator (**sysadmin**), who has the ability to log into the JMX console.

Click **Next**.

15. In the **Account Configuration for Uploading Scan Files** page, configure the user name and password for the account, and then click **Next**.

This account is used for Manual Scanner Deployment mode, which enables uploading scan files directly to the XML Enricher's **incoming** directory on the Data Flow Probe using HTTP or HTTPS. The default user name is **UploadScanFile**.

16. In the **Pre-Installation Summary** page, review the selections you have made, and then click **Install**.

17. Click **Done** in the **Install Complete** page when the installation is complete.

Note:

- Any errors occurring during installation are written to the following file:

<DataFlowProbe_InstallDir>\UninstallerData\Logs\HP_UCMDB_Data_Flow_Probe_Install_<install date and time>.log

For example, **C:\hp\UCMDB\DataFlowProbe\UninstallerData\Logs\HP_UCMDB_Data_Flow_Probe_Install_<install date and time>.log** for the first Probe on the Windows machine.

- Any database-related errors occurring during installation are written to the following log:

<DataFlowProbe_InstallDir>\runtime\log\postgresql.log

For example, **C:\hp\UCMDB\DataFlowProbe\runtime\log\postgresql.log** for the first Probe on the Windows machine.

- Start the Probe by using one of the following methods:

On Windows:

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

Note: To start the second Probe: Select **Start > All Programs > HP UCMDB (2) > Start Data Flow Probe**.

To start the Probe from the console, at the command prompt execute the following script:

```
C:\hp\UCMDB\DataFlowProbe\bin\gateway.bat console
```

On Linux:

Execute the following command:

```
/opt/hp/UCMDB/DataFlowProbe/bin/ProbeGateway.sh start
```

To activate the Probe in a console, execute the following command:

```
/opt/hp/UCMDB/DataFlowProbe/bin/ProbeGateway.sh console
```

Note:

- In order for the Probe to connect to the application server, the application server must be fully started.
- On Linux, the user running the Probe service must be a member of the Administrators group.
- The Probe installed on Windows is displayed in UCMDB in the **Data Flow Management** module, under **Data Flow Probe Setup > <Domain> > Probes**.

- A Probe installed on Linux is displayed when creating a new integration point in the Data Flow Management Integration Studio. For details, see the section describing how to create integration points in the *HPE Universal CMDB Data Flow Management Guide*.
 - A Probe installed on Linux does not appear in the list of Data Flow Probes in the **Data Flow Probe Setup** window.
19. (Applicable for the first Probe only, Windows only) If you selected to run the Probe Gateway and Probe Manager as two processes on separate machines, you must configure the Probe Gateway and Probe Manager components. For details, refer to the **Data Flow Probe - Configure the Gateway and Manager Components** section in the *HPE Universal CMDB Deployment Guide* for version 10.30.

Universal CMDB 10.31 Uninstall Procedure

The following procedure rolls back the 10.31 version of Universal CMDB and Data Flow Probe to your previous version.

This procedure must be performed for both the UCMDB Server and the Data Flow probes.

1. Stop the Universal CMDB server, and all running Data Flow Probes before uninstalling version 10.31.
2. Uninstall version 10.31 of the Universal CMDB server as follows:
 - **Windows**

Go to **<CMDB installation folder>\UninstallerCUP**, delete all the content of **<CMDB installation folder>/UCMDBServer/lib** and double-click **Uninstall HP Universal CMDB Server**.

After version 10.31 is successfully uninstalled,

 - i. Go to **<CMDB installation folder>/runtime** and delete the **jsp** and **jetty-cache** folders.
 - ii. Replace the **<CMDB installation folder>/UCMDBServer/lib** folder with the one you backed up in [step 4](#) of the **Pre-requisites** stage.
 - **Linux**

Go to **<CMDB installation folder>/UninstallerCUP**, delete all the content of **<CMDB installation folder>/UCMDBServer/lib** and run **Uninstall HP Universal CMDB Server**.

After version 10.31 is successfully uninstalled,

- i. Go to **<CMDB installation folder>/runtime** and delete the **jsp** and **jetty-cache** folders.
- ii. Replace the **<CMDB installation folder>/UCMDBServer/lib** folder with the one you backed up in [step 4](#) of the **Pre-requisites** stage.

Note: The uninstaller verifies the status of the UCMDB settings and if any settings are marked sensitive and encrypted (as part of the sensitive settings work), it pops out a warning message asking you to follow the instructions in the UCMDB document to roll back all sensitive settings.

If you see such a warning message, start the server and manually decrypt those encrypted settings by invoking the **markSettingAsNonsensitive** JMX method before proceeding with the uninstall procedure.


Only proceed with the uninstall procedure when the result returned by the **listSensitiveSettings** JMX method is empty. Be aware of the fact that two new OOTB settings are already marked as sensitive. In order to proceed with the uninstall procedure, you should mark them as non-sensitive by invoking the **markSettingAsNonsensitive** JMX method.

For detailed instructions, see the *HPE Universal CMDB JMX Reference Guide*.

3. Uninstall all existing Probes by going to **Start > All Programs > HP UCMDB > Uninstall Data Flow Probe**.

If you have a second probe on the same machine, go to **Start > All Programs > HP UCMDB (2) > Uninstall Data Flow Probe**.

4. Undeploy the **probeUpdate** package.

From UCMDB UI, go to **Administration > Package Manager**, locate the **probeUpdate<version>_linux/windows** package, then click **Undeploy resources** , and then follow the Undeploy Package Resource wizard to undeploy the package.

5. Check if there are any 10.31 lib files that still exist in the **C:\hp\UCMDB\UCMDBServer\lib** and **C:\hp\UCMDB\UCMDBServer\integrations\lib** folders.

If yes, remove all 10.31 related lib files. (You can compare the lib files against a new clean installed 10.31 environment).

6. Reinstall the Probes of the 10.30 version with the same configuration, that is, use the same Probe IDs, domain names, and server names as for the previous Probe installations. Remember that the Probe ID is case sensitive.

Note: After performing an upgrade and installing the new Data Flow Probe, all the Discovery

jobs that were active before the upgrade are automatically run.

7. Restore the integration configuration file.

Go to the **C:\hp\UCMDB\UCMDBServer\integrations\conf** folder, copy the parameters in **DataFlowProbeOverride.properties** back to **DataFlowProbe.properties**, and save the file.

8. Start the UCMDB server.

Re-Enable the FIPS Mode for Configuration Manager

Re-Enable the FIPS Mode for Configuration Manager after Upgrade to 10.22

After upgrading Configuration Manager to version 10.22, some FIPS related files and folders are overwritten. You need to re-enable the FIPS mode for Configuration Manager by following the instructions below.

1. Copy the JCE Unlimited Strength Jurisdiction Policy Files for Java 8 (**local_policy.jar** and **US_export_policy.jar**) to the **<Configuration_Manager_installation_directory>\java\windows\x86_64\lib\security** directory.
2. Copy the 3 CryptoJ jars (**cryptojce-6.2.jar**, **cryptojcommon-6.2.jar**, and **jcmFIPS-6.2.jar**) to the **<Configuration_Manager_installation_directory>\java\windows\x86_64\lib\ext** directory.

You can find the jar files in the **<Configuration_Manager_installation_directory>\servers\server-0\webapps\cnc\WEB-INF\lib** folder.

3. Modify the **java.security** file (located in the **<Configuration_Manager_installation_directory>\java\windows\x86_64\lib\security** directory).
 - a. Update the **keystore.type** property value to **PKCS12** as follows:

```
keystore.type=PKCS12
```

- b. Add the following two lines:

```
com.rsa.cryptoj.fips140initialmode=FIPS140_SSL_MODE
com.rsa.cryptoj.kat.strategy=on.load
```

- c. Replace all the security providers with the following lines:

```
security.provider.1=com.rsa.jsafe.provider.JsafeJCE
security.provider.2=sun.security.provider.Sun
```

```

security.provider.3=sun.security.rsa.SunRsaSign
security.provider.4=sun.security.ec.SunEC
security.provider.5=com.sun.net.ssl.internal.ssl.Provider JsafeJCE
security.provider.6=com.sun.crypto.provider.SunJCE
security.provider.7=sun.security.jgss.SunProvider
security.provider.8=com.sun.security.sasl.Provider
security.provider.9=org.jcp.xml.dsig.internal.dom.XMLDSigRI
security.provider.10=sun.security.smartcardio.SunPCSC
security.provider.11=sun.security.mscapi.SunMSCAPI

```

- If the truststore was located in CM's **java** folder, copy the truststore from the **_sp_backup** folder back to its previous location configured in the Windows service and in the script **start-server-0.bat**.
- Replace the **crypto** tag in the **cnclwssofmconf.xml** file (located in the **servers\server-0\webapps\cnc\WEB-INF\classes** folder) with the following:

```

<crypto cryptoSource="jce" cipherType="symmetricBlockCipher"
engineName="AES" paddingModeName="CBC" keySize="256"
pbeDigestAlgorithm="SHA1"

encodingMode="Base64Url" jceProviderName="JsafeJCE"
jcePbeAlgorithmName="AES" jcePbeMacAlgorithmName="AES"

macType="hmac" macAlgorithmName="SHA1" directKeyEncoded="true"
directKeyEncoding="Base64Url" algorithmPaddingName="PKCS5Padding"

pbeCount="20" macKeySize="256" macPbeCount="20"
initString="12gHERamY1mD8LfeBp6FxE8FU6BlabS"></crypto>

```

- Add the following JVM parameter to the **start_server.bat** or **start_server.sh** file and to CM's Tomcat Windows Service (if applicable):

```
-Dcom.sun.net.ssl.enableECC=false
```

Re-Enable the FIPS Mode for Configuration Manager after Downgrade from 10.31

After downgrading Configuration Manager from version 10.31 to version 10.22, perform the steps below to re-enable the FIPS mode for Configuration Manager.

- Replace the **crypto** tag in the **cnclwssofmconf.xml** file (located in the **servers\server-0\webapps\cnc\WEB-INF\classes** folder) with the following:

```
<crypto cryptoSource="jce" cipherType="symmetricBlockCipher"
```

```
engineName="AES" paddingModeName="CBC" keySize="256"
pbeDigestAlgorithm="SHA1"

encodingMode="Base64Url" jceProviderName="JsafeJCE"
jcePbeAlgorithmName="AES" jcePbeMacAlgorithmName="AES"

macType="hmac" macAlgorithmName="SHA1" directKeyEncoded="true"
directKeyEncoding="Base64Url" algorithmPaddingName="PKCS5Padding"

pbeCount="20" macKeySize="256" macPbeCount="20"
initString="12gHERamY1mD8LfeBp6FwxE8FU6BlabS"></crypto>
```

2. Add the following JVM parameter to the **start_server.bat** or **start_server.sh** file and to CM's Tomcat Windows Service (if applicable):

```
-Dcom.sun.net.ssl.enableECC=false
```

Known Problems, Limitations, and Workarounds

The following problems and limitations are known to exist in CMS 10.31 (or later software, as indicated). The problems are categorized by the affected product area. If a problem has an assigned internal tracking number, that tracking number is provided (in parentheses) at the end of the problem descriptions.

- [DDMI - Inventory Tools](#)
- [UCMDB Browser](#)
- [Configuration Manager](#)
- [Universal CMDB - General](#)
- [UCMDB Installation](#)
- [UCMDB Upgrade](#)
- [Universal CMDB - UI](#)
- [Universal CMDB - Server](#)
- [Universal CMDB - Topology](#)
- [Universal Discovery - General](#)
- [Universal Discovery - Probe Framework](#)
- [Universal Discovery - Probe Upgrade](#)
- [Integrations](#)

DDMI - Inventory Tools

PROBLEM: Importing a custom SAI file (for example, **User.zsai**) into the Software Application Index (SAI) Editor fails with a loading error. (QCCR1H98842)

Workaround: To import the custom SAI file into the SAI Editor properly,

1. Close the Software Application Index (SAI) Editor if it is open.
 2. Navigate to the
 `..\hp\UCMDB\DataFlowProbe\runtime\probeManager\discoverySaiResources\saiRuntime`
directory, locate and remove the **auto.zsai** file.
 3. Launch the Software Application Index (SAI) Editor again.
 4. Import the customer SAI file (in this case, **User.zsai**).
-

UCMDB Browser

LIMITATION: UCMDB 10.31 requires version 4.12 of the embedded UCMDB Browser. UCMDB server version 10.30 or later does not support embedded UCMDB Browser versions older than the UCMDB Browser 4.10. (QCCR1H106107)

Workaround: None for embedded UCMDB Browser versions older than the UCMDB Browser 4.10.

LIMITATION: When a UCMDB server is reconfigured to use a new schema, the new schema has the OOTB packages deployed at the UCMDB server startup. If a standalone UCMDB Browser is already connected to the UCMDB server, the Browser's packages are not present in the new schema.

Workaround: Restart the UCMDB Browser Tomcat in order for the Browser's packages to be redeployed on the new schema.

PROBLEM: On Mozilla Firefox, the plug-in container for Firefox stops working and sometimes, when clicking **Logout**, nothing happens. This is a known issue with Mozilla Firefox ESR 38.4 ([JavaScript garbage collection crash with Java applet](#)). (QCCR1H104135)

Workaround: Use a different supported Firefox version.

PROBLEM: (Embedded UCMDB Browser only) The port number of UCMDB Browser URL changes to **8143** when Configuration Manager 10.22 is connected to UCMDB Server 10.30, resulting that the UCMDB Browser is no longer available.

After Configuration Manager is installed, UCMDB Browser URL becomes **https://<server name or IP address>.<domain name>:8143/ucmdb-browser/**, which is the URL of the UCMDB Browser embedded in CM.

Workaround: After Configuration Manager is installed, make sure you change the port number of UCMDB Browser URL from **8143** back to **8443** (go to **UCMDB UI > Administration > Infrastructure Settings Manager**, locate the **UCMDB Browser URL** setting by searching **Name** with a keyword **Browser**, and then change the port number from **8143** to **8443** and save the change.

LIMITATION: UCMDB server version 10.30 or later does not support embedded UCMDB Browser versions older than the UCMDB Browser 4.10. (QCCR1H106107)

Workaround: None for embedded UCMDB Browser versions older than the UCMDB Browser 4.10.

Configuration Manager

PROBLEM: Configuration Manager 10.22 CUP3 cannot connect to the UCMDB server 10.30.

Workaround: To resolve the issue, configure Configuration Manager by following the instructions in ["How to Configure Configuration Manager 10.22 to Connect to UCMDB Server" on page 62](#).

Universal CMDB - General

PROBLEM: The shortcut of **Uninstall HP Univesal CMDB Server** or **Uninstall Data Flow Probe** may not appear on the **Start** menu of Windows Server 2016.

Workaround: The shortcut problem is a Microsoft issue in Windows Server 2016. If you want to uninstall UCMDB server or Data Flow Probe, go to the **UninstallerData** folder to uninstall it.

PROBLEM: Displaying a specific view may crash the UCMDB server. This is because too many nodes were returned by the view that caused many more number of meta links generation and crashed the system with OutOfMemory error. (QCCR1H106088, QCCR1H100903)

Workaround: In addition to the fix provided in UCMDB 10.30, for views with huge number of nodes and relations, you may also increase the memory of the UCMDB server and the applet. For detailed

instructions, see "How to Increase the Java Heap Memory Used by the UCMDB UI Java Applet" in the *HPE Universal CMDB Administration Guide*.

PROBLEM: There is a wrapper license key support issue for certain time zones, causing UCMDB Probe service unable to start. (QCCR1H105575)

Workaround: If you encounter such an issue, contact HPE Software Support to obtain new wrapper license keys, and then manually deploy the provided License keys on probe.

PROBLEM: When LDAP is enabled, UCMDB should not require password change anymore. However, after logging into UCMDB, users receive a page with the following message requiring them to change password: "Default or expired password detected. Please change your password." (QCCR1H106754)

Workaround: When LDAP authentication is enabled, users need to set the **Passwords must use default policy** infrastructure setting to **False**.

PROBLEM: When uninstalling the UCMDB server, in the Uninstall HP Universal CMDB Server dialog box, the following items cannot be removed:

```
Unable to remove directory: C:\hp\UCMDB\UCMDBServer\solr\server\logs
Unable to remove directory: C:\hp\UCMDB\UCMDBServer\solr\server
Unable to remove directory: C:\hp\UCMDB\UCMDBServer\solr\bin
Unable to remove directory: C:\hp\UCMDB\UCMDBServer\solr
```

Workaround: Make sure that the solr process, a Java process that points to **<UCMDB_Server_Home>/bin/jre**, is stopped before uninstalling the UCMDB server.

To stop the solr process,

1. Access **http://localhost:<some_port>/solr**.
 2. Go to **<UCMDB_Server_Home>/bin**, and then run **solr.bat** on Windows and **solr.sh** on Linux to stop the solr server.
 3. If the solr process is still available, end the solr process in Task Manager.
-

PROBLEM: If the Solr index folder is empty at the UCMDB server startup, UCMDB deletes it and Solr will recreate it again with the default files, which causes server errors, such as `HttpSolrClient$RemoteSolrException` and `NoSuchFileException`.

Workaround: If the problem still appears, manually delete the index folder and restart the server.

PROBLEM: Saving or updating a perspective based view with several perspectives (for example, seven perspectives), may cause performance issues and it also may get the UCMDDB server stuck.

Workaround: In case you experience the above behavior and there is no other solution that can be used:

1. Go to the UCMDDB JMX Console, locate the **setGlobalSettingValue** JMX method in the **UCMDDB:service=Settings Services** category.
2. Provide the following parameter values:
name: **pbv.max.perspectives.to.start.use.remove.on.update**
value: Specify the number of perspectives used in the perspective based view which crashed the system.
3. Click **Invoke**.
4. Restart the UCMDDB Sever.

LIMITATION: When starting Solr manually on a Windows machine by running **solr.bat start <port>** from the command line using the script **<UCMDDB_Server_Home>\bin\solr.bat**, if the command line from which the Solr was started is closed, the Solr process is stopped. (QCCR1H109216)

Workaround: This is a Windows behavior and it has nothing to do with the Solr process or UCMDDB. However, you can restart the UCMDDB server, which will then start the Solr, and there will be no command line visible in Windows.

PROBLEM: When trying to delete an attribute from a class which is used as key attribute on a descendent class, the **Save** button from UI shows an error that the action was not able to be performed, but actually the attribute will be removed from the list of key attributes for the descendent class. Clicking **Save** again will finally delete the attribute from the class. (QCCR1H104520)

Workaround: When the attribute definition is overwritten in a descendent class, if you want to delete the attribute from the parent class, do the following:

1. Remove all attribute overriding from the descendent classes.
2. Delete the attribute from the parent class.

LIMITATION: The priority for TQL queries under the pattern-based model are changed from medium on UCMDDB 9.05 to inactive on UCMDDB 10.xx. The performance might be affected if the TQL queries under the pattern-based model are set to low/medium priority on UCMDDB 10.xx. In this case, you might

see that the locked gates and calculation for scheduled pattern-based model could take a couple of hours. (QCCR1H98275, QCCR1H95041)

Workaround: None.

LIMITATION: (High Availability environment only) Changes in Global Settings that require the server's restart to take effect may not take effect without restarting all nodes from a cluster. (QCCR1H98228)

Workaround: In order for all changes in Global Settings that require the server's restart to take effect, you must restart all nodes from the cluster (one by one or with the **restartCluster** JMX method).

PROBLEM: After upgrading UCMDB to version 10.21 (or later) successfully, some times users may encounter an internal error when trying to launch the UCMDB UI. (QCCR1H101149)

Workaround: In case you encounter an internal error when trying to launch the UCMDB UI, delete the **C:\Users\\AppData\Local\Temp\UcmdbAppletJars** folder and try to launch the UCMDB UI again.

LIMITATION: The **testDBConnection** JMX method does not support PostgreSQL. (QCCR1H98834)

Workaround: None.

UCMDB Installation

PROBLEM: The **wrapper.log** file is created in the **bin** folder when the **log** folder is missing. (QCCR1H103867)

Workaround: If the **log folder** is missing (for example, it was deleted accidentally), before starting up the UCMDB server, make sure you create the **log** folder manually.

Note: If you want to delete the logs, delete the content in the **log** folder only, and never delete the folder itself. Make sure the **C:\HP\UCMDB\UCMDBServer\runtime\log** folder always exists.

UCMDB Upgrade

PROBLEM: Opening or accessing (for example, accessing through command) any of those folders or files during the upgrade may result in upgrade failure. During the upgrade, UCMDB server folders and files will be modified or overwritten by the installer wizard.

Workaround: Close all UCMDB Server folders and files before the upgrade, and DO NOT open or access any of those folders and files during the upgrade.

In case of such upgrade failure, to restore the server, copy the entire content of the **C:\hp\UCMDB\UCMDBServer\old** folder into the **C:\hp\UCMDB\UCMDBServer** folder. Then you can continue to use the server or perform another upgrade.

PROBLEM: Resource string files added in the basic package **AutoDiscoveryInfra** are not updated during UCMDB upgrade. (QCCR1H104381)

Workaround: After upgrading UCMDB to version 10.22 (or later), manually re-deploy the **AutoDiscoveryInfra** package.

PROBLEM: Login fails after recreating a database schema after upgrading UCMDB from version 10.21 to version 10.22. (QCCR1H104015)

Workaround: After upgrading UCMDB from version 10.21 to 10.22 (or later), and you have created and changed the database schema, perform the following to align the password from the database with the one from the super integration credentials file. This requires calling two JMX methods.

1. Reset the DB password.
 - a. On the UCMDB server, go to **JMX console > UCMDB-UI:name=UCMDB Integration > setCMDBSuperIntegrationUser**.
 - b. In the **User Name** field, enter **UISysadmin**, and in the **Password** field, enter the desired password value.
 - c. Click **Invoke**
 2. Reset the super integration user credentials file.
 - a. Go to **JMX console > UCMDB:service=Authorization Services > resetPassword**.
 - b. In the **Value** box for **customerID** enter **1**, in **User Name** field enter **UISysadmin**, and in the **Password** field, enter the password value to match the one you entered in [step 1](#).
 - c. Click **Invoke**
-

LIMITATION: After upgrading from earlier versions to 10.20 or later, instances of the **Tags** business service attribute and element may not be searchable. (QCCR1H91974)

Workaround: In order to find instances of the **Tags** business service attribute when searching, you must change the indexer and ranking configuration in the JMX console.

- In **UCMDB:Service=Topology Search Services. Method: editIndexerConfiguration**, for the **business_element** class, the **Tags** attribute must be lower case in order to be searchable.
- In **UCMDB:Service=Topology Search Services. Method: editRankingConfiguration**, the **Tags** element should be **tags** in order to be searchable.

PROBLEM: When upgrading from UCMDB version 10.11 with a CP15 update to UCMDB 10.20 (or later), the UCMDB server cannot start after upgrade. This is caused by the fact that the current CP version deployed on top of version 10.11 is higher than the CP version bundled in the 10.20 install media. (QCCR1H100431)

Workaround: You can fix this upgrade issue by changing the CP version in the JMX Console manually during the upgrade, and after the upgrade, redeploy the existing CP.

For example, if you are upgrading UCMDB from version 10.11 with CP15 Update 1 to version 10.20, do the following,

1. Perform the minor upgrade from UCMDB 10.11 with CP15.01.142 to UCMDB10.20.
2. Check status and wait for the CP deployment to fail with error in **error.log**:

```
[ErrorCode [105005] Content pack downgrade is not allowed]
```

```
Trying to install CP version [15.00.123] which is older than the one already installed [15.01.143] is not support.
```

3. Log in to the JMX Console and access **UCMDB:service=Settings Services**.
4. Locate the **getInternalSettings** method.
5. Enter customer ID and **cp.version** in the **key** value field, and then click **Invoke**.

The returned value should be **15.01.142**.

6. Replace the value with **15.00.123** and click **Set**.
7. After that the CP deployment should finish successfully. You can check the status in **mam.packaging.log**.
8. Access UCMDB UI and redeploy CP 15.01.142.
9. Check the CP version from menu **Help > About**. It should be **15.01.142**.

You may also refer to [KM01581489](#) for details.

PROBLEM: When upgrading both UCMDB and Content Pack from previous versions to the latest versions, from example, upgrade UCMDB from 10.11 to 10.20 and Content Pack from CP14 to CP15,

if you have customized any Content Pack files, deployment of some Content Pack class model files may fail during the upgrade. (QCCR1H96681)

Workaround: Reinstall the latest Content Pack manually after the upgrade.

PROBLEM: If you have created custom class models on UCMDB version 9.05, after upgrading UCMDB from version 9.05 to 10.20 or later, you might find that your custom class models are not available. For example, when you create a new activity for a management zone, you might find that the Protocol pane in the Define Credentials tab page is empty. (QCCR1H97159)

Workaround: Invoke the JMX method **updateClassModel** to upgrade custom class models. To do so,

1. 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.

2. In the Search field, type **updateClassModel** and press **Enter**.
 3. Locate the **updateClassModel** method, in the customerID **Value** field, type **1**, and click **Invoke**.
-

PROBLEM: After upgrading UCMDB to version 10.20 or later, you may encounter some credentials related issues. (97159)

Workaround: To resolve the credentials related issues, do the following:

- **key.bin file.** Check and make sure that the new probe uses the same **key.bin** file as the UCMDB server.
- **Time.** Check and make sure that the probe time is the same as the UCMDB server time. If the probe time is different, it may cause credentials error.
- **Credentials fail on the upgraded environment.**

Workaround: Install a new probe and copy specified files to override problematic files. To do so,

- a. Install a clean probe on the same machine of UCMDB server, connect it to UCMDB server. Make sure that the new probe can get credentials normally.
- b. Go to the clean probe, copy the **Cmcache.bin** and **secured_storage.bin** files from **C:\hp\UCMDB\DataFlowProbe\conf\security** directory.
- c. Go to the probe that has get credentials errors, override the two files with yours.
- d. Restart the probe and try to get credentials again.

- **Export credentials from the upgraded environment and import them to the fresh install environment, the JMX operation fails.** When the exported credential xml file contains customized class models, or the customized class models are not defined on the UCMDB server that you upgraded, you may encounter credentials import issue.

Workaround:

- Remove the customized protocol from the exported credential xml file.
- Add the customized class models on the UCMDB server manually via CIT.

Note: Make sure that the export CIT or import CIT works well. Otherwise it may cause the workaround not working.

Note: To upgrade customized class models, invoke the JMX method **updateClassModel**. For details, see [Invoke JMX Method updateClassModel](#) (workaround for QCCR1H97159).

PROBLEM: A user with “create user” permissions loses permission after upgrading the UCMDB from version 9.0x. (QCCR1H93868)

Workaround: None.

PROBLEM: When upgrading from a previous version to 10.20 or later, the user preferences of a deleted user are not deleted. Warnings appear in the log and the upgrade completes successfully. (QCCR1H75574)

Workaround: None.

PROBLEM: After upgrading UCMDB to a newer version (including CUP), the Normalization rules does not work. (QCCR1H99001)

Workaround: To fix the issue, perform either of the following:

- Deploy a new Content Pack package.
- Manually delete the **<Data Flow Probe Installation>\runtime\probeGateway\maxupdatetime.txt** file and then restart the Data Flow Probe.

PROBLEM: (Automated Service Modeling only) When performing ASM service discovery from the UCMDB Browser, all the errors from the ASM service discovery are not assigned to the correct categories. They are assigned to the **Other** category.

Workaround: If you use ASM, to workaround this issue, make sure you upgrade both your UCMDB Server and Content Pack to the latest versions, that is to upgrade UCMDB Server to version 10.21 (or later) and Content Pack to version 16.00 (or later).

Universal CMDB - UI

LIMITATION: If LDAP is configured and specified, the direct login using URL parameters (**userName** and **password**) for LDAP users is not working.

Workaround: None for this release.

LIMITATION: Only HTTP protocol is supported when launching UCMDB UI from any web browser running on Mac OS X with JNLP enabled.

Workaround: None.

PROBLEM: UCMDB UI loads properly with HTTP, but it may not load with Safari on Mac OS when HTTPS is enabled.

Workaround: Switch the UCMDB Server back to HTTP protocol by changing the following setting in the `\UCMDBServer\conf\settings.override.properties` file to **true** and then restart the UCMDB server:

```
jetty.connections.http.enabled=true
```

LIMITATION: (Chrome only) UCMDB UI applet cannot work in Chrome version 42 or later, because starting from Chrome 42, NPAPI plugins are disabled by default. Chrome displays a gray screen with the following error message when users try to access the UCMDB UI: This site uses a plugin (Java (TM)) that is unsupported.

Workaround: To resolve the issue, you need to enable NPAPI manually and keep Chrome below version 45 to make UCMDB UI client applet work properly. For details, see [KM01656540](#).

To launch UCMDB UI from Chrome version 45 (or later), follow the instructions in "How to Launch UCMDB UI from Chrome 43+, Firefox 48+, IE 12+, Microsoft Edge, or Safari 10+" in the *HPE Universal CMDB Administration Guide* for version 10.30.

LIMITATION: Cannot upload a zip package if the zip file size exceeds the applet available memory. (QCCR1H99579)

Workaround: You can deploy larger packages using the **deployPackages** JMX method (go to the **JMX Console > UCMDB:service=Packaging Services > deployPackages**).

You can also control the maximum size of the packages to be uploaded by setting the value of the infrastructure setting **File upload maximum file size for archive type** to a larger value (default value: 200 MB).

PROBLEM: When clicking **Help > UCMDB Class Model** from the UCMDB UI or clicking **UCMDB Class Model** on the UCMDB login page, the page is not loading. (QCCR1H101882)

Workaround: None for this release.

Universal CMDB - Server

PROBLEM: When importing data packages into UCMDB through Package Manager, some data packages may fail to be imported.

Workaround: Check and make sure that the files you import into UCMDB are using the same encoding as defined in the XML. For example, if you export the XML files in UTF-8 encoding, then you should import files encoded in UTF-8 as well. The problem would occur if you import files encoded in UTF-8 BOM and the XML content specifies it is UTF-8.

PROBLEM: If the Solr search functionality is not enabled, even when **https://localhost:8983/solr** can be accessed or started from command line, any search activity from UCMDB Browser or JMX console may fail.

Workaround: If UCMDB server cannot start Solr for some reason after the server starts, just stop the UCMDB server, start Solr manually and start the UCMDB server again.

PROBLEM: (Linux only) OpenJDK may create a wrong server name on the status page if the machine hosting UCMDB Server is in a certain domain environment. (QCCR1H102136)

Workaround: If the problem appears, modify the **wrapper.conf** file as follows:

1. Open the **<UCMDB_Server_Home>\bin\wrapper.conf** file using a text editor.
2. Uncomment the line with **wrapper.java.additional.46**, and specify a server name or simply use the localhost name.

To find the localhost name in console, simply enter **hostname**.

PROBLEM: (Linux only) Statistics data collection does not work for Linux (program "ps" cannot run due to too many open files and failed to fetch statistics), which would create a lot of threaddump.txt files, and then failed to run other applications, like applying a content pack or running license utility.

Workaround: In order to change the Linux Max Open files, you will have to increase the maximum number of open files system-wide and per process of a specific user:

- **System-wide:**

Set system-wide file descriptors (FD) limits by editing the `/etc/sysctl.conf` file, so that after reboot the setting will remain as it is:

- Locate and open the `/etc/sysctl.conf` file.
- Append a config directive as follows:

```
fs.file-max = 100000
```

- Save and close the file.
- Users need to log out and log back in again for the changes take effect, or just type the following command: `# sysctl -p`

- **User Level FD Limits:**

After setting system-wide FD limits, you can still limit `httpd` user (or any other users) to specific limits by editing the `/etc/security/limits.conf` file.

- Set `httpd` user soft and hard limits as follows:

```
httpd soft nofile 4096
httpd hard nofile 10240
```

- Save and close the file.

To view limits, enter:

```
# su - httpd
$ ulimit -Hn
$ ulimit -Sn
```

To check the limits of a process:

- Get the PID number by entering:

```
- #ps aux | grep <process-name> #
```


2. Check the limits of a process:

```
- cat /proc/<PID>/limits`
```

PROBLEM: After adding a new UCMDB server to an High Availability (HA) cluster that has been reinstalled on a fresh operating system, the new server does not register as a cluster node. (QCCR1H106209)

Workaround: Manually set the network interface in the **wrapper.conf** file when you have more than 1 network interface. To do so,

1. On a UCMDB server instance in the HA cluster, open the **c:\hp\UCMDB\UCMDBServer\bin\wrapper.conf** file in a text editor.
2. Add a **wrapper.java.additional.nn** entry into the file, which looks similar to the following:

```
#wrapper.java.additional.27=-Djava.compiler=NONE
#wrapper.java.additional.28=-Xrunjdp:transport=dt_
socket,server=y,suspend=n,address=5005
wrapper.java.additional.30=-Djgroups.bind_addr=<ip-address>
```

where *<ip-address>* is the IP of the right interface to be used.

3. Save the file.
4. Repeat the above steps on each of the remaining UCMDB servers in the cluster, and use for each the right IP/Interface assigned for that server.
5. Restart all UCMDB servers.

PROBLEM: The Writer server becomes unresponsive which schedules a restart of the entire HA infrastructure. This impacts the load balancing URL, causing all probes to disconnect. This is caused by the existing Garbage Collector algorithm used in UCMDB. (QCCR1H100329)

Workaround: The problem can be resolved by improving the performance of the Garbage Collector by using G1 algorithm for the Garbage Collector. For enterprise environments where you have more than 16 GB of RAM allocated just for UCMDB (see the **wrapper.java.maxmemory** property value in the **..\UCMDB\UCMDBServer\bin\wrapper-platform.conf** file), check and make sure you add the following settings to the **wrapper-custom.conf** file if they are not present:

```
#Enable the following parameters for JVM G1 garbage collector in enterprise
environments
wrapper.java.additional.54=-XX:+ParallelRefProcEnabled
wrapper.java.additional.55=-XX:G1HeapRegionSize=32
```

```
wrapper.java.additional.56=-XX:InitiatingHeapOccupancyPercent=70
```

LIMITATION: You cannot not use the status page when the URM resources are not deployed at the first time a schema is created or modified.

Workaround: None.

PROBLEM: Can not save the enrichment rule when adding the customer relationship. This is caused by the fact that the TQL query behind the enrichment is not connected. When there is no existing relation between two CI types, it is not possible to create an enrichment which will add the relation just by entering enrichment manager and by adding the relation that is needed. (QCCR1H104733)

Workaround: Create a **joinf** link in the TQL query between the concerning two CI Types by joining them on an attribute value. This way the enrichment manager will know how to perform correctly the enrichment actions.

Universal CMDB - Topology

PROBLEM: After updating a non-key attribute of a CI with enrichment rule, an unexpected new CI instance is created. This is only happening when populating attributes having a constant part and a dynamic part, in this case **CDoc+<node:name>**.

Workaround: The first time the enrichment is executed, it will have a full TQL query layout. If the enrichment rule is active and it is notified of a change, it will run on a partially TQL query layout. This is designed so for performance reasons.

To workaround the issue, you may take either of the following:

- Run enrichments on a scheduled notice. Nowadays it is not recommended to have many active enrichments.
 - Split the enrichment into two parts, one does the CREATE of new CIs which will run periodically, one does the UPDATE which is active.
-

PROBLEM: Currently the Perspective views are not displayed in the Reports module in UCMDB. (QCCR1H99954)

Workaround: None.

PROBLEM: The priority for TQL queries under the pattern-based model are changed from medium on UCMDB 9.05 to inactive on UCMDB 10.xx. The performance may be affected if the TQL queries under the pattern-based model are set to low or medium priority on UCMDB 10.xx. In this case, you can see that the locked gates and calculation for scheduled pattern-based model can take a couple of hours. (QCCR1H95041)

Workaround: None.

PROBLEM: The priority for TQL queries under the pattern-based model are changed from medium on UCMDB 9.05 to inactive on UCMDB 10.xx. The performance may be affected if the TQL queries under the pattern-based model are set to low or medium priority on UCMDB 10.xx. In this case, you can see that the locked gates and calculation for scheduled pattern-based model can take a couple of hours. (QCCR1H95041)

Workaround: None.

Universal Discovery - General

LIMITATION: If there is a Linux probe connected to the UCMDB server, when running ASM, it would try to detect an available probe. If it finds the Linux probe, an ASM dispatch issue could occur, because Linux probe is capable of running integration jobs only.

Workaround: Right-click an adapter and select **Go to Adapter**, then go to the **Adapter Configuration** tab, in the Trigger Dispatch Options section, select the check box for **Override default probe selection**, and in the value field specify the target probe you want to use.

LIMITATION: After upgrading UCMDB server to version 10.31, and setting the **setDomainEncrypt** JMX method to **true**, if you start some old version 10.30 probes which were not upgraded to the latest version because they were down before the server upgrade, when they connect to the UCMDB server and you run discovery jobs, the discovery jobs would fail with error. This is because these old probes do not have the updated **domainScopeDocument.xml** and **domainRangesDocument.xml** (DSD/DRD) files that contain the new **domain_encrypt** attribute. The DSD/DRD files were downloaded to probes before server upgrade. After server upgrade, probes would not download the DSD/DRD files again.

Workaround: To resolve this issue, the easiest way to modify any IP range or credentials (such as a protocol) from UCMDB server, which will trigger the automatic upgrade process for the probes. As a result, the updated DSD/DRD files as well as the upgrade packages are downloaded to the probes, then the probes are upgraded to the latest version automatically.

PROBLEM: Universal Discovery JMX is fully accessible without providing any credentials. (QCCR1H112324)

Workaround: To fix this issue, do the following:

1. Stop Data Flow Probe.
2. Add `wrapper.java.additional.58=-XX:+DisableAttachMechanism` into `<DataFlowProbe_Home>\bin\WrapperGateway.conf` and `<DataFlowProbe_Home>\bin\WrapperManager.conf`.
3. Restart Data Flow Probe.

LIMITATION: (Probe installation) Probe cannot be started after installation if any of the following special characters are included in the PostgreSQL user account password: `? | &) %`

Workaround: During probe installation, do not use these special characters for PostgreSQL user account password as they are regarded as sensitive characters: `? | &) %`

Note: Available special characters include the following: `\ / . _ = + - , : [] (`

LIMITATION: After upgrading UCMDB to version 10.30 without deploying the latest Content Pack (CP21), when the Content Pack version is CP17 (or earlier), and you upgraded your CP to version CP18, CP19, or CP20 manually, SNMP discovery jobs may fail to run due to the missing of a Sun library.

Workaround: If you manually upgrade an older CP to CP18, CP19, or CP20 when UCMDB is already on version 10.30, to enable SNMP discovery jobs to work properly, make sure you deploy an additional package corresponding to your target CP version.

The packages can be found in the `<UCMDB_Server_Home>\tools\compatibility_patch` folder:

CP version	Package
CP18	snmp-fix-for-10.30-installer-18.01.92.zip
CP19	snmp-fix-for-10.30-installer-19.01.97.zip
CP20	snmp-fix-for-10.30-installer-20.01.92.zip

For detailed instructions, see "How to Deploy a Package" in the *HPE Universal CMDB Administration Guide*.

LIMITATION: On a Windows machine where two Data Flow Probes are installed, both with Inventory Tools, after uninstalling one probe, the following three file types (.xsf, .aws, and .awcs files) lose their default opening programs and cannot be opened.

Workaround: Manually re-associate default opening programs for the three file types: Inventory Tools Viewer for .xsf files, and Inventory Tools Analysis Workbench for .aws files and .awcs files.

PROBLEM: (FIPS mode only) Failed to run Amazon Cloud discovery if setting JAVA_TOOL_OPTIONS for FIPS in the Environment Variables.

Workaround: None.

PROBLEM: When more than 1500 IP ranges are configured on each Data Flow Probe, the following performance issues might occur:

- Memory usage is huge on the UCMDB server side, which may cause OutOfMemoryError and the writer server restart.
- Modifying the IP ranges could take a while.

Workaround: Do not configure too many IP ranges and always keep the total number of IP ranges below 1500 per probe.

PROBLEM: When application names of existing records are changed in **master.zsai**, the records in **auto.zsai** are not updated automatically.

Workaround: Delete the **auto.zsai** file on all remote servers directly so that it will be automatically regenerated:

1. Delete the **auto.zsai** file on all of the remote servers.
 2. Restart the XML Enricher.
-

PROBLEM: (Universal Discovery protocol only) When running a discovery job that uses the Universal Discovery protocol to push a large amount of CIs into another UCMDB server, the job fails with timeout errors, which causes data inconsistency issue and performance impact. (QCCR1H107794)

Workaround: The default connection timeout value of the Universal Discovery protocol is 20 seconds. If the command execution in your organization's discovery job takes some time, to ensure that the job runs successfully, increase the timeout value in both of the following places, for example, to 45 seconds:

- The **Connection Timeout** parameter value in the Universal Discovery Protocol Parameters dialog (go to **UCMDB UI > Data Flow Management > Data Flow Probe Setup > Domains and Probes > DefaultDomain(Default) > Credentials > Universal Discovery Protocol**)
- The **shellGlobalCommandTimeout** property value in the **globalSettings.xml** file (go to **UCMDB UI > Data Flow Management > Adapter Management** module, under **Resources > Packages > AutoDiscoveryContent > Configuration Files**)

PROBLEM: Version 10.10 probes appear to corrupt the PostgreSQL database under normal discovery loads. The root cause is that when Anti-Virus is scanning the PostgreSQL data folder, it could cause PostgreSQL tables to corrupt. (QCCR1H105604, QCCR1H105110)

Workaround: To resolve the issue, perform the following:

- Always make sure that the PostgreSQL install directory is added into the anti-virus software exclusion list. The exclusion of data files will not introduce any potential security risk.
- If you need to run weekly-based scan, monitor the **probeerror.log** file, and if a database error shows up (for example, a database error related to the **Discovery_result** table), do the following:
 - a. Clean the probe log folder.
 - b. Run **Clear Probe Results Cache** from **UCMDB UI > Data Flow Management > Universal Discovery > Discovery Modules/Jobs** to clean the problematic table.

This should resolve the issue.

PROBLEM: After upgrading from UCMDB from version 10.11 CUP5 + CP15 to version 10.21 CUP1 + CP17 on Windows Server 2008 R2, users are unable to run any discovery job or integration job that uses an external process on the probe. For example,

- VMware discovery
 - VMware vCenter Connection by VIM
 - VMware vCenter Toplogy by VIM
 - VMware vMotion Monitor by VIM
- XLS Import
- NNMi Integration


The discovery or integration job fails with an "Failed to execute remote process" error. This is because version 10.11 **dataflowprobe.properties** file was used in 10.21 probe and the incorrect class path value caused the error. (QCCR1H105538)

Workaround: To resolve the issue, append the missing `../lib/discovery-content-api.jar` to the value for the `remoteJVMClasspath` adapter parameter.

Note: When upgrade a probe by reinstall, do not copy the old `dataflowprobe.properties` file from the old probe to the upgraded probe directly, because the values of the properties might have been changed during the upgrade.

PROBLEM: After upgrading UCMDB from version 10.21 + CP15 to version 10.22 (or later)+ CP18 (or later), the ASM for BSM functionality does not work anymore. (QCCR1H104758)

Workaround: Re-deploy the `ASM_Enhanced.zip` package after upgrade as follows:

1. Unzip the CP18 package and locate the `ASM_Enhanced.zip` package in the `packages` folder.
2. In UCMDB UI, navigate to **Administration > Package Manager**, and click the **Deploy packages to server**  button.
3. Select the `ASM_Enhanced.zip` package and import it.

PROBLEM: (PostgreSQL only) Some SQL statements are observed running more than 30 minutes, which causes Probe database to crash. The root cause is that the default value of the `statement_timeout` setting in the `postgresql.conf` file is `0`. (QCCR1H101769)

Workaround: To workaround the issue, locate and open the `hp\UCMDB\DataFlowProbe\pgsql\data\postgresql.conf` file in a text editor, and then modify the default value of the `statement_timeout` setting from `0` to `3600000`.

PROBLEM: (Service Discovery) The modified `IsopPath` parameter value in the ASM template fails to load properly. (QCCR1H104012)

Workaround: To modify the parameters in the service discovery activity template successfully, select a different row or click **Enter** to complete the change you made in the **Value** field of parameters. After that, click **OK** to save the changes. This ensures that the parameters values are saved successfully and the communication log reflects the change properly, then the new parameter value can be used in discovery jobs correctly.

LIMITATION: When you have many environments, note that it is not supported to update the `domainScopeDocument.xml` and `domainRangesDocument.xml` files on all environments by building a package and importing it to all other environments. (QCCR1H100855)

Workaround: The only way to update these files is to call the `editResource` JMX method (from the `UCMDB:service=Packaging Services` or `UCMDB:service=URM Services` category).

If you want to update IP Ranges and Credentials, you can also use the **importCredentialsAndRangesInformation** and **exportCredentialsAndRangesInformation** JMX methods. For details, see *HPE Universal CMDB Hardening Guide* or *HPE Universal CMDB JMX Reference Guide*.

LIMITATION: When changing the LW-SSO **initString** from UCMDB UI or via JMX, the probe side fails to synchronize the credentials from Configuration Manager. (QCCR1H100746)

Workaround: To resolve the issue, do the following:

- If the value of **initString** is changed from UCMDB UI, regardless whether the probe is connected to or disconnected from the UCMDB server, you can use the **setLWSSOInitString** JMX method on the probe side to keep the same **initString** value as on the UCMDB server side, then credentials from CM can be successfully synchronized.

To do so,

- a. On the Probe machine, launch the Web browser and enter the following address:
https://localhost:8453.

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: **https://localhost:8454.**

- b. Click **type=CMClient** to open the JMX MBEAN View page.
 - c. Locate the **setLWSSOInitString** method and provide the same init string that was provided for UCMDB's LW-SSO configuration.
 - d. Click the **setLWSSOInitString** button.
- If the value of **initString** is changed from JMX on the UCMDB server side, and
 - the probe is disconnected from the UCMDB server, use the **setLWSSOInitString** JMX method on the probe side to resolve the issue. For detailed instructions, see steps above.
 - the probe is connected to the UCMDB server, invoke the **setInitString** JMX method on the UCMDB server side to enable automatic synchronization of the **initString** value.

For instructions on how to invoke the **setInitString** JMX method, see the *HPE Universal CMDB JMX Reference Guide*.

LIMITATION: Probe discovery will result in duplicate node CIs (Windows/Unix) if re-imaging the Virtual Machine system with the same template, IP address, and hostname. This is because the unique calculation logic for the node is different between the UCMDB server and the probe. (QCCR1H104153)

Workaround: Before re-imaging your Virtual Machine system, remove the CI instance of the old Windows/Unix system from UCMDDB manually.

PROBLEM: If a Management Zone inherits the IP range from a bound probe, after the probe is added to or removed from a probe cluster, the Management Zone loses the IP range setting and the following operations have unexpected results:

- Move this Management Zone from one folder to another folder.
This operation results in an error message and the Management Zone remains in the original folder.
- Move the folder that contains this Management Zone to another folder.
This operation moves the folder to the target folder successfully. However, an error message appears and this Management Zone is moved to the Root folder. If there are other Management Zones after this Management Zone in the tree, these Management Zones are also moved to the Root folder.
- Rename the folder that contains this Management Zone.
This operation renames the folder successfully. However, an error message appears and this Management Zone is moved to the Root folder.

Workaround: To work around this issue, manually set the IP range for the problematic Management Zone, and then move the Management Zone(s) to the target folder.

PROBLEM: The **WebSphere to Web Server Dependencies** job is causing `OutOfMemoryError` on the probe side. (QCCR1H97710)

Workaround: The probe requires at least 4G memory to run the WebSphere to Web Server Dependencies job. Therefore, allocate at least 4G memory for the probe.

LIMITATION: When the probe is in Separate Mode, the default credentials for basic authentication are not updated automatically. (QCCR1H98271)

Workaround: Update the default credentials for basic authentication manually. To do so,

1. Open the JMX Console of the UCMDDB Server side, enter **changeBasicAuthenticationCredential** in the quick search field and click the link that appears.

- Specify the **userName** and **password** that you want. For example:

changeBasicAuthenticationCredential

Change basic authentication credential.

Name	Type	Value	Description
customerId	int	<input type="text" value="1"/>	Customer Id
userName	java.lang.String	<input type="text" value="test"/>	new user name for basic authentication.
password	java.lang.String	<input type="text" value="123456"/>	new password for basic authentication.

Invoke

Note: Password must contain at least six characters.

- Click **Invoke**.
- Encrypt the password by using the JMX Console of the probe side as follows:
 - Open the JMX Console of the probe side, enter **getEncryptedKeyPassword** in the quick search field and click the link that appears.
 - Enter the password that you specified.
 - Click **Invoke** and then the encrypted password is generated.
- Copy the encrypted password.
- Edit the **DataFlowProbe.properties** file as follows:

```
appilog.agent.Probe.BasicAuth.User = <the user name that you specified>
appilog.agent.Probe.BasicAuth.Pwd = <the encrypted password that you just copied>
```

- Save the change and then restart the probe.

LIMITATION: When working in a High Availability environment, if there is a failover to the other UCMDB Cluster, you must first clear the data of the HP Integration Service before running it.

Workaround: To clear the data, run

```
..\UCMDB\UCMDBServer\integrations\tools\clearProbeData.bat.
```


PROBLEM: When using the network ping options available in the new **Check Network Availability** dialog box to troubleshoot network connection issues and/or credential related issues against a **node** type inventory CI in IT Universe Manager, you selected a different credential in the Choose Credential

dialog box but changed your mind and clicked the **Cancel** button, **All credentials** show up in the **Credential** field, instead of keeping the original value in the **Credential** field unchanged.

Workaround: None.

PROBLEM: After upgrading UCMDB to version 10.21 and deploying the Content Pack 16.00, the new **Check Network Availability** permission is not available for the out-of-the-box role **Discovery And Integrations Admin**. This is caused by the fact that version 10.21 installer does not run in silent mode, therefore the **Basic_Authorization.zip** package is not deployed. (QCCR1H101124)

Workaround: To make the **Check Network Availability** permission available for the out-of-the-box role **Discovery And Integrations Admin**, you need to manually deploy the **Basic_Authorization.zip** package. To do so,

1. Copy the **Basic_Authorization.zip** package from the **<UCMDB_Server_Home>\content\basic_packages** directory to the machine from where you will deploy the package.
2. Launch UCMDB UI and navigate to **Administration > Package Manager**, and click the **Deploy packages to server**  button.

In the popup dialog, select **Basic_Authorization.zip**, and then click **Deploy**.

3. After the deployment is completed, go to **Security > Roles Manager**, select **Discovery and Integration Admin > CIT Menu Items**, then select **Node CI** type, the **Check Network Availability** action should show up in the Selected Actions pane.
-

LIMITATION: After upgrading to version 10.21, some jobs cannot run in JVM 8 because the driver JAR files of these jobs only support JVM 7.

Workaround: To work around this issue, you can use a remote process of JVM 7 to run these jobs. For detailed instructions, see [KM01746334](#).

LIMITATION: When the UD probe compiles a list of CIs to be scanned, it does not add CIs that are connected through VPN. This happens when there are two UCMDB servers available handling the discovery of the client environments, but there is only one agent package with the same call home configured. (QCCR1H101777)

Workaround: Set up a DNS alias, such as **UDCallHome**, that in each network resolves to a local (for that region) UD probe to receive the agent call home event. This way the same initial agent call home configuration could be used throughout.

Universal Discovery - Probe Framework

PROBLEM: Probe database (PostgreSQL) size grows quite big (36 GB). Clearing probe cache resolves the issue, but it reoccurs at regular intervals. This issue is caused by the biggest table **ddm_discovery_results**, which is the main table that controls the result of all CIs discovered by the probe, but the table is used by multiple features. (QCCR1H105398)

Workaround: To resolve the issue, use the

C:\hp\UCMDB\DataFlowProbe\pgsql\bin\pgAdmin3.exe GUI to perform DB dump. Just right-click the Data Flow Probe DB, and choose **backup**.

For example, from the **C:\hp\UCMDB\DataFlowProbe\pgsql\bin** directory, execute the following command:

```
pgsql.exe --username=postgres --command "VACUUM full verbose" --  
dbname=dataflowprobe
```

PROBLEM: When the **appilog.collectors.storeDomainScopeDocument** property in the **DataFlowProbe.properties** file is set to **false**, some jobs which run in the remote process mode may fail, because the remote process cannot read the probe memory, thus having no access to the **domainScopeDocument** file stored in the memory. When the setting is false, the file is only stored in the probe memory. (QCCR1H98264)

Workaround: If some jobs run in the remote process mode, make sure that you set the value of the **appilog.collectors.storeDomainScopeDocument** property in the **DataFlowProbe.properties** file to **true**.

LIMITATION: When using PostgreSQL as your database on the Windows platform, the **UCMDB_Probe_DB** service is not starting as a non-system user. This is a third-party product limitation, because PostgreSQL is able to "irrevocably give up administrative rights at startup". For details, see [this PostgreSQL wiki page](#). (QCCR1H98262)

Workaround: In order for the **UCMDB_Probe_DB** service to start properly, you may configure the **Log On** options for the **UCMDB_Probe_DB** service as follows:

1. Locate the **UCMDB_Probe_DB** service in the Services window.
2. Right-click **UCMDB_Probe_DB** and select **Properties**.
3. In the **UCMDB_Probe_DB** Properties window, go to the **Log On** tab, and do either of the following:

- (Recommended) Select the **Local System account** option.

Note: This is the recommended option, because the SYSTEM account has access to all necessary folders according to the default settings on Windows.

- Select **This account**, and specify the account name and password.

Note: This option is NOT recommended. Even if you specify an administrator account, it will be treated as a common user account by PostgreSQL, because PostgreSQL is able to "irrevocably give up administrative rights at startup".

If you DO need to specify a different account, make sure that the USERS group on your Windows platform has:

- **Read** and **Write** access to the **C:/hp/UCMDB/DataFlowProbe/pgsql** folder.
- **Read** access to the files in system library (for example, the **C:/Windows/System32** folder) that PostgreSQL needs to access.

For the list of files that PostgreSQL needs to access, see PostgreSQL documentation.

4. Click **OK**.

LIMITATION: Java API `setDiscoveryConfigurationXML` does not support cluster. (QCCR1H98897)

Workaround: None.

Universal Discovery - Probe Upgrade

LIMITATION: Linux does not support automatic upgrade of probes. (QCCR1H99342)

Workaround: To perform manual upgrade of probes on Linux, run the `<DataFlowProbe Installation Folder>/tools/upgrade/extractUpgradePackage.sh` script.

PROBLEM: Deploying probe update manually failed with an "Out of memory" error.

Workaround: When you deploy a probe update manually via UCMDB UI, the maximum package size allowed is 200 MB. If the package size is greater than 200 MB, deploy it via JMX console using the `deployProbePatch` JMX method from the **UCMDB:service=Discovery Manager** category.

Also, note that the UCMDB UI client for applet requires 1280 MB memory at least.

Integrations

LIMITATION: SiteMinder with AJP does not work any more starting from UCMDB 10.21, because Jetty does not support it. That is why after upgrading to UCMDB version 10.21, the UCMDB integration with SiteMinder with IIS as front-end will fail. (QCCR1H105818)

Workaround: None.

LIMITATION: Java adapters do not support the remote process feature. An integration job will fail with an error when the "Run as Separate JVM" option with the Java adapter is set to TRUE. (QCCR1H107699)

Workaround: None for this release.

PROBLEM: After downgrading UCMDB to an earlier version (for example, from version 10.22 to version 10.21 or 10.20), because the version of the **Cmdb10xAdapter.zip** adapter is higher than the UCMDB server version, the adapter is not recognized and all integration points based on the adapter can not be loaded from the database. (QCCR1H104825)

Workaround: After downgrading UCMDB to an earlier version, re-deploy the **Cmdb10xAdapter.zip** adapter package from the **<UCMDBServer_install_dir>\content\adapters** folder and restart the UCMDB server.

PROBLEM: (UCMDB version 10.20 and later) UCMDB to BSM push integration does not work if attributes sizes is different. In UCMDB version 10.20 and later, the size for some OOTB attributes is 250, but in RTSM or BSM 9.05, the size is 100. Therefore, when trying to push CIs with large value from UCMDB to BSM, the integration does not work. (QCCR1H101184)

Workaround: Check and make sure that the sizes of attributes between UCMDB and RTSM/BSM are synchronized before pushing CIs with large values.

LIMITATION: When creating an integration point using the Cmdb 9.x Adapter, the integration point does not work on HTTPS protocol. (QCCR1H104603)

Workaround: To make the connection work, add the certificate of the remote machine into the cacert file in the **\DataFlowProbe\bin\jre\lib\security\cacert** directory.

LIMITATION: After upgrading from 10.20 to 10.21, manually redeploy the UCMDB 9.x integration adapter package located in the **C:\hp\UCMDB\UCMDBServer\content\adapters** directory. (QCCR1H98251)

If the package is not redeployed, the integration adapter still works, but the reconciliation issue fixed in QCCR1H92320 will re-occur.

Workaround: None.


PROBLEM: When creating an integration point using the Cmdb 9.x Adapter, after clicking the **OK** button to save the integration point, the saving operation may fail after working for some time. This is caused by the long-running task `DataAccessAdapterQueryGetSupportedClassConfigs`. (QCCR1H91379)

Workaround: Whenever you encounter a similar timeout issue and see `DataAccessAdapterQueryGetSupportedClassConfigs` in the log, you can go to the JMX console and increase the values for the following two settings:

- **task.DataAccess.Manager.getAdapterClassesConfig.timeOut.** Default value for the setting is 20000.
 - **configuration.remote.action.timeout.** Default value for the setting is 35000.
-

LIMITATION: You cannot create one integration point for both data push and population. (QCCR1H98068)

Workaround: To create an integration point for both data push and population, do the following:

1. Update the value for **Object Root** from **managed_object** to **root**.
 - a. Log in to UCMDB with an administrator account and go to **Administration > Infrastructure Settings Manager**.
 - b. From the **Filter by column** drop-down list, click **Name**, type **Object Root** in the text box and double-click the **Object Root** entry that is displayed.
 - c. In the Properties dialog box, go to the **Current Value** field, change **managed_object** to **root**, and then click **Save**.
 - d. Log out of UCMDB and log in to UCMDB again for the change to take effect.
2. Add the **discoverypattern_mdr_type** attribute to **Auto Discovery Pattern definition**.
 - a. Go to **Modeling > CI Type Manager > CI Types** pane > **Root tree > Data > Object > Configuration**, and click **Auto Discovery Pattern definition**.
 - b. In the right pane, click the **Attributes** tab and click the **Add**  button.
 - c. In the Add Attribute dialog box, type **discoverypattern_mdr_type** in the **Attribute Name** and **Display Name** fields, and click **OK**.

3. If you already create an integration point, delete it and create it again.
4. Open the Adapter Source Editor dialog box and click **Save**.
 - a. Go to **Data Flow Management > Adapter Management > Resources** pane, select the adapter that is related to your integration point.
 - b. Right-click the adapter, select **Edit adapter source**.
 - c. In the Adapter Source Editor dialog box, click **Save**.

LIMITATION: When creating a new inherited CI Type in which the parent has identification based on key attributes, it will be by default inherited by the child CI Type, without the possibility of changing it. For example, creating an inherited CI Type from Person will inherit its **identification by key** attribute by default. So if you choose to change the identification with reconciliation rule, the whole identification will be the Person identification by key + identification by rule. (QCCR1H92081)

Workaround: When creating the new CI Type inherited from Person, change first the identification of Person by removing all attributes conditions, so the new identification of the newly created CI Type will be empty.

PROBLEM: When trying to run a remote process using the Integration Service, the following error is returned: Failed to connect to remote process. (QCCR1H101639)

Workaround: If you want to use the Integration Service to run a remote process, add the following jars to the **basic_discovery_minimal_classpath** setting in the **<UCMDB_Server_Home>\integrations\conf\DataFlowProbe.properties** file manually:

```
../lib/cryptojce.jar;../lib/cryptojcommon.jar;../lib/jcmFIPS.jar;
```

Problem: The Integration Service cannot start due to a failure to connect to the database after you change the master key on the UCMDB server. (QCCR1H102098)

Workaround: None.

Tenant Owner Related Known Issues, Problems, and Workaround

- **PROBLEM:** After switching to Tenant aware reconciliation, the **OwnerTenant** attribute becomes read-only in the Configuration Item Properties dialog.

Workaround: Use **Assign Tenants** functionality from the CI's context menu.

- **PROBLEM:** After removing the Key Attributes qualifier from the **OwnerTenant** attribute of the Managed Object, sometime no properties are displayed for the CIs in UI.

Workaround: If you want to switch back (to disable Tenant aware reconciliation), do the following:

- a. Remove the **ID_ATTRIBUTE** qualifier for the **TenantOwner** attribute on the **managed_object** CIT.
 - b. Remove the value of the **reconciliation.tenantaware.citypes** setting.
 - c. Reload the class model from persistency (go to the **JMX console > UCMDB:service=Class Model Services**, and invoke the **reloadClassModelFromPersistency** method).
 - d. Go to **JMX console > UCMDB:service=Model Services**, invoke the **recalculateID** method with **classname** field empty.
 - e. Go to **JMX console > UCMDB:service=Model Services**, invoke the **updateClasModel** method.
- **LIMITATION:** Enrichment is not invoking the Reconciliation on Update **OwnerTenant** via **Associate Tenant Rule**. As a result, you may have duplicated data in the system in case if you update the **OwnerTenant**'s CI to a tenant that already has this CI.

Workaround: None.

- **LIMITATION:** CIs with Identification rule would be duplicated in case if the user is updating the **OwnerTenant** CI to a tenant that already has this CI from **Update OwnerTenant** in the **Assign Tenants** module.

Workaround: None.

- **PROBLEM:** When adding Consumer Tenants to a CI, the System Default Tenant appears in the list of Consumers after saving, even if it was not selected. This issue occurs only when changing the Owner Tenant or the Consumer Tenant.

Workaround: None.

- **PROBLEM:** When removing all Consumer Tenants from a CI (from the IT Universe), an error is thrown and the Owner Tenant is overwritten with the System Default Tenant.

Workaround: To avoid removing the System Default Tenant from the Consumer Tenants list, make sure you set the System Default Tenant as consumer.

Only when the System Default Tenant is not set as consumer, the Owner Tenant will be overwritten with the System Default Tenant when trying to save.

- **PROBLEM:** Error message received when setting up a tenant aware environment, for the OOTB enrichments which are adding CIs. (QCCR1H104949)

Workaround: If there are enrichments which are creating new CIs, after setting the environment as tenant aware, the attribute **Owner tenant** should be set for those CI Types which are being created through enrichments.

Enhancements Requests

The following table lists the enhancement requests that were implemented in HP UCMDB, UD, and CM 10.31.

Global ID	Problem	Solution
QCCR1H101784	When importing a resource (for example, TQL query and view) in a Multi-tenancy environment in Modeling Studio, the user should only need access permission to one dedicated folder assigned via roles and not to the Root folder.	Added the following best practices to the <i>HPE Universal CMDB Modeling Guide</i> with detailed instructions as an example: When importing a resource (for example, TQL query, view) in a multi-tenancy environment in Modeling Studio, for the import to work, the TQL query used for the creation of the view needs to have as consumer or owner tenant, the tenant associated with the user that performs the import. The user who performs the import of a view has to have at least view permission on the TQL query used.
QCCR1H102438	The creation of a new package in the Package Manager fails because the wizard is getting stuck at resource selection page.	Implemented a new Package Manager module in UCMDB Browser 4.12/UCMDB 10.31.
QCCR1H104466	This is a request to encrypt IP ranges related information that can be found on the probe.	Added a new attribute domain_encrypt in the domainScopeDocument.xml file to act as a flag to tell the probe whether to encrypt or decrypt the IP ranges related information in the domainScopeDocument.xml and domainRangesDocument.xml files. You can invoke the new JMX method setDomainEncrypt to control this attribute. For detailed instructions, see "How to Encrypt/Decrypt IP Ranges Information on the Probes" in the <i>HPE Universal CMDB JMX Reference Guide</i> .
QCCR1H104826	UCMDB Service is not started when invalid tenant association resources are present.	Implemented the enhancement by adding a new validation step after loading the URM and changing resource tenant association to use the new validation timing because the URM will be initialized at that point. Now UCMDB can start properly when invalid tenant association resources are present. All invalid tenant association resources are changed to associate with the default system tenant on startup.

Global ID	Problem	Solution
QCCR1H110902	This is a request to provide documentation about how to configure the rotation of PostgreSQL log files by specific size.	Fixed the issue by providing instructions for configuring PostgreSQL log files rotation by specific size. For more information, see the "How to Configure PostgreSQL Log Files Rotation by Size" section in the <i>HPE Universal CMDB Database Guide</i> .
QCCR1H112196	On Linux, the probe can not upgrade to the latest version automatically.	Starting from version 10.31, the probe can upgrade to the latest version automatically. Note: For a probe of version 10.30 or earlier, you need to manually upgrade it to version 10.31 first.
QCCR1H77675	This is a request to implement a feature on which users can be authenticated via LDAP and UCMDB data store.	UCMDB and LDAP servers are now supported as user repositories. At login a user can choose the repository on which he or she wants to log in. For more details, see "Hybrid User Management with Multiple User Repositories" in the <i>HPE Universal CMDB Hardening Guide</i> .
QCCR1H93585	When the user inserts a tab or space trailing character after a number value in the adapter.conf file, then a sync would fail. The problem is visible on any integration using a Generic Database Adapter (GDBA) underneath.	Fixed the issue by implementing a code change. Now trailing spaces in the adapter.conf file will not cause any error.
QCCR1H94112	This is a request to protect server against performance issues that occur after UCMDB Browser search.	Implemented the enhancement by adding the fuse cmdb.search.max.query.max.results to protect against performance issues when the enriching process is done during UCMDB Browser Search. The number of results retrieved during enriching is limited by the value specified for the cmdb.search.max.query.max.results parameter. In case this setting is not present, the default is 1000. When the max number of records retrieved through enriching (cmdb.search.max.query.max.results value) is reached, the value of cmdb.search.enriching.depth is no longer taken into consideration and the enriching process is stopped.
QCCR1H97656	This is a request to	Implemented the enhancement by making the

Global ID	Problem	Solution
	secure the access to the probe JMX console.	jettyHttpsEnabled setting in the Probe configuration file DataFlowProbe.properties default to true and using the HTTPS port 8453 for the Probe server for fresh installed Data Flow Probes, with the HTTP port 1977 being disabled. For more information, see "Using HTTPS Port 8453 as Default for Data Flow Probe" in the <i>HPE Universal CMDB JMX Reference Guide</i> .
QCCR1H98691	This is a request to have the possibility to configure multiple LDAP domains, and to define several LDAP domains for authentication.	Implemented the enhancement by adding support for multiple LDAP authentication in UCMDB version 10.30. For details, see "How to Define LDAP Servers and Enable LDAP Authentication" in the <i>HPE Universal CMDB Hardening Guide</i> .

Fixed Defects for UCMDB and UD 10.31

The following table lists the defects that were fixed in HPE UCMDB and UD 10.31.

Global ID	Problem	Solution
QCCR1H102061	Atrium push adapter never gives an error in Integration Studio even when there is a failure. For example, when the password of Atrium user account is changed, or the server is not responding, the system still runs with success in Integration Studio with wrong user name or password. But if you manually edit the integration and do a test connection, it will fail. It is expected that Atrium integration job fails if it cannot connect to Atrium when JAR files do not exist.	Fixed the issue by implementing a code change. Now a test connection will fail if the JAR files of Atrium push adapter are absent.
QCCR1H103781	In Package Manager, for the VMware package, the columns are empty, displaying no package information (for example, Category, Readme, Version, Build Number, and Description).	Fixed the issue by implementing a code change. Now the related package information is displayed.
QCCR1H104103	The probe should not check the credentials that are not selected in Management Zone.	Fixed the issue by implementing a code change. Now for Management Zone jobs, the probe side provides only the selected credentials in Management Zone.
QCCR1H105774	Some custom defined adapters disappeared from the UCMDB UI after restart. The special characters angle bracket (> or <) in the adapter's description caused SAXParseException and made the adapter disappear from the UI.	Fixed the issue by implementing a code change. Now angle bracket (> or <) can be used in the adapter description.
QCCR1H106320	Several NetDevices (firewalls) are discovered as Linux Node in customer's environment.	Fixed the issue by implementing a code change. Now NetDevices (firewalls) can be discovered as Firewall properly.
QCCR1H107532	No time information in wrapperEnricher.log .	Fixed the issue by modifying the related configuration file. Now the time information is shown in wrapperEnricher.log .

Global ID	Problem	Solution
QCCR1H107620	Some large scan files crash the Universal Discovery Viewer due to the large XML file in the scan file.	Fixed the issue by modifying the Viewer to handle large scan files properly.
QCCR1H107774	Framework should support flush objects in multi-threading way.	Fixed the issue by implementing a code change. Now framework supports multi-threading flush objects.
QCCR1H108043	Duplicate CIs are created after the full synchronization from Asset Manager. Deleted CIs should be sent during the full synchronization.	Fixed the issue by implementing a code change. UCMDB now supports automatic deletion for the full population run.
QCCR1H108250	Device drivers are discovered even though they are not selected.	Fixed the issue by implementing a code change. Now device drivers will not be discovered when they are not selected.
QCCR1H108737	The Compare Snapshots option takes too much time to open.	Fixed the issue by implementing a code change to the method, so that now the Compare Snapshot option takes much less time to open.
QCCR1H109321	When running the SCCM integration with an NT account, the integration job fails when using the persistence.xml file and the value of the temp.tables.enabled setting is true .	Fixed the issue by implementing a code change. Now the SCCM integration job works properly.
QCCR1H109379	A job, for example, Databases TCP Ports runs on the IP address that belongs to a node and creates a Node CI. When it is discovered by the Host Connection by Shell job and merged, data is lost and the global ID does not exist anymore.	Fixed the issue by implementing a code change. Now data will not be lost and the global ID still exists.
QCCR1H109641	Non-existing CITs trigger errors when running Server Capacity related JMX functions.	Fixed the issue by implementing a code change. Now Class Model will be checked for existing CITs before the capacity is calculated.
QCCR1H109643	The ProbeGW_Topology_task blocks the Result processing to the UCMDB application server.	Fixed the issue by implementing a code change. Now the error will not show up when the customer views the result for ProbeGW_Topology_task .

Global ID	Problem	Solution
QCCR1H109655	The automatic deletion mechanism does not work properly when performing the delta synchronization in UCMDB UI.	Fixed the issue by implementing a code change. Now the automatic deletion mechanism can work properly when performing the delta synchronization in UCMDB UI.
QCCR1H109768	In the High Availability environment, after the customer restarts the UCMDB Server Services, the autodiscovery service gets stuck in the Starting state, making the Writer Server unavailable.	Fixed the issue by implementing a code change so that the autodiscovery service does not get stuck anymore.
QCCR1H109807	The one way SSL authentication is not able to handle retired certificates and worked as designed. However, this is not documented.	Fixed the issue by documenting the following note in the "Enable SSL with Server (One-Way) Authentication" section in the <i>Hardening Guide</i> : Note: The certificate on the Probe will not be used in the one-way authentication.
QCCR1H109815	When the customer attempts to schedule an AM push job, the following error message appears in the UCMDB UI: "Cannot add job to scheduler".	Fixed the issue by implementing a code change. Now an AM push job can be successfully scheduled in UCMDB.
QCCR1H109831	The customer adds the IP address to the Host Connection by Shell job but the IP address does not show up in the list of IP addresses for discovery.	Fixed the issue by modifying the IP address distribution mechanism: along with domain name and IP address value. The probe name is also considered for the distribution of IP addresses.
QCCR1H109881	In the Infrastructure Settings Manager, the unit of the Session Timeout option is milliseconds , which should be seconds .	In the Infrastructure Settings Manager, now the unit of the Session Timeout option is seconds .
QCCR1H110070	When running the Inventory Discovery by Scanner job, not all the existing CIs are triggered by the job. For example, from 17,000 CIs, only a few hundred CIs are triggered, and the job run for 4 hours.	Fixed the issue by implementing a code change so that now all the CIs are triggered by the Inventory Discovery by Scanner job.

Global ID	Problem	Solution
QCCR1H110270	When the customer packages a custom .zsai file with a special character, the special character loses its format.	Fixed the issue by implementing a code change so that the special character can be parsed properly.
QCCR1H110536	In version 9.05 users got a list of discovery job via the java API by using the TopologyQueryService and reading all CIs of type discoveryjob . After migrating UCMDB system to 10.21, they got nothing. After checking JMX console (Model Services, method countCIsPerType), they see that there's no instance of that type.	Starting from version 10.00, you can not get the discoveryjob CI Type instance, because it is saved in Unified Resource Manager (URM). You can use DDMConfigurationService instead. For more details, see KM02529119 .
QCCR1H110632	The last access time attribute is not updated for the CIs that have been discovered by the Host Connection by WMI and Host Applications by WMI jobs.	Fixed the issue by setting the value of the last touch time attribute to the system's current time, and save it into the Data Flow Probe Database. Now the last access time attribute is updated for the CIs that have been discovered by the Host Connection by WMI and Host Applications by WMI jobs.
QCCR1H110793	The Global IDs are not generated for the CIs that have the CMDB ID.	Fixed the issue by adding a hidden setting force.global.id.assignment (by default the value is true). Now the Global IDs are assigned for the CIs that have the CMDB ID. Note: If the value of the force.global.id.assignment setting is false , the old behavior will be used.
QCCR1H110834	Federated CIs are not retrieved by SOLR search. As an example, searching for Windows in the regular search returns 0 results, but advanced search shows 19124 results for Windows .	Fixed the issue by implementing a code change to allow only the attributes marked with the CMS_SEARCHABLE_ATTRIBUTE qualifier and of type string to be taken into consideration. Now no errors should appear in the logs when making a search like the one described.

Global ID	Problem	Solution
QCCR1H110863	The following warning message is displayed in history.log , and there is no history information for related CIs: Cant find completed event in table <table name>; will set the incomplete events as completed	Fixed the issue by changing the query condition to adopt a-sync mechanism.
QCCR1H110886	Unable to create and export meaningful error reports from UCMDB > Modeling > Reports > Custom Reports > Discovery Status > Discovery Error Reports .	Fixed the issue by changing array to arraylist. Now meaningful error reports can be created and exported from UCMDB > Modeling > Reports > Custom Reports > Discovery Status > Discovery Error Reports .
QCCR1H110964	The activemq related dependency code still remains in the server lib folder.	Fixed the issue by removing unnecessary activemq code and binary files.
QCCR1H111238	Jar files with the same names are found in the C:\hp\UCMDB\UCMDBServer\lib folder.	Fixed the issue by deleting the add action to refine the duplicated jar files. Now only one version of the jar files exist in the lib folder.
QCCR1H111261	The DMG file contains a package installer that needs to be manually opened in order to launch it. When trying to install the program, an error message is displayed: "The Installation Failed". The Installer cannot install some files in the /Library/StartupItems folder.	Fixed the issue by implementing a code change. Now the installer installs files to the /Library/LaunchDaemons folder, instead of /Library/StartupItems .
QCCR1H111378	Invoking JMX method recalculateAttribute under Model Services returns a null string.	Fixed the issue by adding meaningful return string for JMX method recalculateAttribute and adding debug log messages to track the progress of the operation.
QCCR1H111379	Async history is not working for CIs in PostgreSQL.	Fixed the issue by modifying sql for PostgreSQL. Now async history for CIs is available.

Global ID	Problem	Solution
QCCR1H111498	When monitoring the usage of UD licenses, on several occasions the License Summary count from the UI shows "0" CIs being counted. This could last for a few hours or days and then go back to a more accurate count. Also, the License Summary count does not match the count from the Licensed OSIs Report.	Fixed the issue by implementing a code change to prevent saving the license usage data for the Authorized or Actual state. License Summary data now can be calculated properly.
QCCR1H111587	The following error message appears: Insert new destinations Failed... value too large for column "CMDB"."CCM_DISCOVERY_ERRORS"."TRIGGER_CI_ID".	Fixed the insert issue so that users can perform dispatch in ASM.
QCCR1H111655	It takes more and more time for UCMDB Server to start up because of the obsolete data in the jgroupsping table.	Fixed the issue by applying a code change to use the local host name as the own_addr instead of a random UUID. Now UCMDB server starts normally as expected.
QCCR1H111810	Nodes [display name as IP address] generated by Webseal Policy Server Topology by Shell are consuming license count.	Fixed the issue by applying code change. Now a node with hostname equal to an IP address is counted as a dummy node.
QCCR1H111813	(Probe installation) Probe cannot be started after installation if any of the following special characters are included in the PostgreSQL user account password: ? &) %	Fixed the issue by updating the documentation to list special characters available for use in the PostgreSQL user account password during probe installation, also added a limitation in the Release Notes about the special characters that should not be used.
QCCR1H111974	The AM integration is updating Last Access Time even when the " Enable update 'Last Access Time' " flag on the adapter is disabled.	Fixed the issue by applying code change. Now AM integration does not update Last Access Time when this option is disabled.
QCCR1H112039	When trying to activate the asset manager integration, the following error message is returned: "failed loading supported queries for integration point", giving little information about where went wrong.	Fixed the issue by applying code change to provide proper error messages, so that users can correct the TQL queries causing problems by themselves.

Global ID	Problem	Solution
QCCR1H112043	Users are unable to disable live discovery on specified adapter from UCMDB UI, and jobs are not dispatched in a timely fashion.	Fixed the issue by implementing a code change to the live discovery logic, so that users can disable live discovery on specified adapters to improve live discovery performance.
QCCR1H112045	Users are unable to split dispatch log in order to trace dispatch performance.	Fixed the issue by implementing a code change to split the dispatch logs and to improve the dispatch performance of live discovery.
QCCR1H112048	Currently the confirm task process still triggers a series of dispatch tasks when the dispatch queue is already busy.	Fixed the issue by implementing a code change, so that the confirm task process checks the dispatch queue status first before triggering more dispatch tasks. It will be pending if the dispatch queue is busy.
QCCR1H112049	Currently the probe limit triggers are calculated repeatedly during the live discovery task. This is not helping with the improvement of dispatch performance.	Fixed the issue by implementing a code change to. Now the probe limit triggers will not be calculated repeatedly during the live discovery task.
QCCR1H112092	The CI status is updated to SUCCESS even though the discovery job fails.	Fixed the issue by applying code change. Now the CI status is updated correctly.
QCCR1H112105	For specific topologies, Merge Cluster Software Job input TQL query computes wrong data for a trigger when all triggers run concurrently.	Fixed the issue by adding a TQL query consistency check for each trigger to make sure the result is consistent.
QCCR1H112125	After running the Host Connection by Shell job, the containment links of removed IPs were not automatically deleted as expected.	Fixed the issue by applying a code change. Now the containment links can be deleted automatically.
QCCR1H112126	No Merge CI permission when it is not admin.	Fixed the issue by applying a code change. Now the Merge CIs menu item works properly.
QCCR1H112209	The short message is too long to insert into CCM_DISCOVERY_ERRORS.	The issue is fixed. Now the system can insert the short message into CCM_DISCOVERY_ERRORS.

Global ID	Problem	Solution
QCCR1H112275	UCMDB Rerun Discovery dispatch performance is inefficient and poor.	Fixed the issue by removing some unnecessary dispatch tasks to improve dispatch performance.
QCCR1H112336	When clicking the Rerun button on UI for one job or all jobs, the system is re-dispatching inactivate triggers.	Fixed the issue by applying code change. Now the system would not re-dispatch inactive triggers when users click the Rerun button on UI for one job or all jobs.
QCCR1H112377	XML Enricher cannot parse the value for " FILE_SIZE " probably because of too big file size. This happened when import unrecognized files is enabled in software recognition configuration.	Fixed the issue by applying a code change so that the file size can be increased.
QCCR1H112591	License TQL query calculation is wrongfully executed on Reader Server.	The issue is fixed. License calculation operation will only be generated on the writer server.
QCCR1H112619	When normalization rule failed to update due to the use of an out of box ID in the custom normalization xml file, error message in the error log was not proper.	Fixed the issue by implementing a code change to display proper error message in the error log when normalization rule fails to update due to use of an out of box ID in the custom normalization xml file.
QCCR1H112637	The password of UCMDB server should not include blank as password. If yes, UCMDB Browser cannot resolve the blank in credentials.bin, thus unable to connect to UCMDB server.	Fixed the issue by implementing a code change to filter out blank passwords on UCMDB server and probes.
QCCR1H112667	After upgrading from UCMDB 10.22 to version 10.30, the integration between CM and UCMDB does not work.	Fixed the issue by aligning the new adapters with UCMDB 10.30.
QCCR1H112732	Probe Upgrade Package should not contain JRE and Jython files.	Fixed the issue by removing the JRE and Jython files during probe upgrade.
QCCR1H112872	The integration point with UCMDB 10.x adapter fails to push two SAP system CIs to the target UCMDB. The root cause is that the link between the running_software CI and its cluster_resource_group root container was removed when the CI was also connected to a sap_system CI.	Fixed the issue by adding an extra check for such topology so as not to delete the running_software root_container .

Global ID	Problem	Solution
QCCR1H112965	When there are more than 5 probes, there is a major database performance issue, probes are not sending their results to the UCMDB server.	Fixed the issue by updating the <code>MAX_OBJECTS_FOR_INSERT_RESULTS</code> value to 50.
QCCR1H112967	Touching queries are causing deadlocks each day.	Fixed the issue by changing the default value for the parameter <code>appilog.agent.probe.sendtoouchResultsToServer.maxObjects</code> in <code>dataflowprobe.properties</code> to 500.
QCCR1H113040	UCMDB10.x adapter logging spam in the <code>fcmdb.synchronizer</code> and <code>error.log</code> files.	The issue is fixed. Now the messages will be logged on trace loglevel.
QCCR1H93661	After defining an SCCM Integration, where the authentication is done through NTLM and not SQL credentials, users modified the <code>persistence.xml</code> file according to the guide, however, testing the connection always failed.	Fixed the issue by applying a code change. Now on an SCCM Integration, the test connection will succeed when authentication is done through NTLM.
QCCR1H95503	When deploying a Content Pack from the JMX console, users encounter Content Pack undeploy errors which should be changed to warning.	Fixed the issue by changing the Content Pack undeploy errors to warning.

How to Configure Configuration Manager 10.22 to Connect to UCMDB Server

Version 10.30 of the HPE Configuration Management System consists of Universal CMDB 10.30 (UCMDB) and Universal Discovery 10.30 (UD). It does not include a new release for Configuration Manager. The latest release of Configuration Manager is version 10.22 (it is recommended to have CM 10.22 CUP3), you can use it in tandem with version 10.30 of Universal CMDB.

In case you encounter any issue connecting Configuration Manager 10.22 CUP3 (or with a later CUP on top of version 10.22) to UCMDB server 10.30, configure CM as follows:

1. Copy `server.keystore` from the `C:\hp\UCMDB\UCMDBServer\conf\security` directory to the `C:\hp\CM_10.2.0.0\javalwindows\x86_64\lib\security\` directory.
2. Edit the `C:\hp\CM_10.2.0.0\servers\server-0\conf\server.xml` file.

Find the line with connector **8143**, replace the line with the following and save the file:

```
<Connector port="8143" protocol="HTTP/1.1" SSLEnabled="true"
maxThreads="150" scheme="https" secure="true" keystoreFile="C:/hp/CM_
10.2.0.0/java/windows/x86_64/lib/security/server.keystore"
keystorePass="hpass"/>
```

3. In a web browser, enter the URL of the UCMDB server:


https://<server name or IP address>.<domain name>:8443

where **<server name or IP address>.<domain name>** represents the fully qualified domain name (FQDN) of the HPE Universal CMDB Server.

4. Find the icon that indicates a secure connection, click it, and export the certificate with the name **hpcert.cer**.
5. Copy the just exported certificate into the **C:\hp\CM_10.2.0.0\java\windows\x86_64\bin** folder.
6. From the **C:\hp\CM_10.2.0.0\java\windows\x86_64\bin** folder, run the following:

```
keytool -import -alias hp -file hpcert.crt -keystore "C:\hp\CM_
10.2.0.0\java\windows\x86_64\lib\security\cacerts"
```

Note: The password is **changeit**.

7. Change the CM URL in the UCMDB Server for CM to work with HTTPS.
 - a. Log in to UCMDB Server.
 - b. Go to **Administration > Infrastructure Settings Manager > General Settings**.
 - c. Locate the **Configuration Manager URL** setting, and change its value to **https://<CM_SERVER>:8143/cnc**.
 - d. Click **Save** .
 - e. Log out and log in to UCMDB Server again for the change to take effect.

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 Release Notes (Universal CMDB 10.31)

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@hpe.com.

We appreciate your feedback!