



# **Configuration Management System (CMS)**

Software Version: 2018.08

## **CMS Troubleshooting Guide**

Document Release Date: August 2018  
Software Release Date: August 2018



## Legal Notices

### Disclaimer

Certain versions of software and/or documents ("Material") accessible here may contain branding from Hewlett-Packard Company (now HP Inc.) and Hewlett Packard Enterprise Company. As of September 1, 2017, the Material is now offered by Micro Focus, a separately owned and operated company. Any reference to the HP and Hewlett Packard Enterprise/HPE marks is historical in nature, and the HP and Hewlett Packard Enterprise/HPE marks are the property of their respective owners.

### Warranty

The only warranties for products and services of Micro Focus and its affiliates and licensors ("Micro Focus") are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Micro Focus 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. Except as specifically indicated otherwise, a valid license from Micro Focus is 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 - 2018 Micro Focus or one of its affiliates.

### Trademark Notices

MICRO FOCUS and the Micro Focus logo, among others, are trademarks or registered trademarks of Micro Focus (IP) Limited or its subsidiaries in the United Kingdom, United States and other countries. All other marks are the property of their respective owners.

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.softwaregrp.com>.

This site requires that you register for a Software Passport and to sign in. To register for a Software Passport ID, click **Register for Software Passport** on the Micro Focus Support website at <https://softwaresupport.softwaregrp.com>.

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

## Support

Visit the Micro Focus Support site at: <https://softwaresupport.softwaregrp.com>.

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

Micro Focus 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 Micro Focus 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 a Software Passport user and to sign in. Many also require a support contract. To register for a Software Passport ID, click **Register for Software Passport** on the Micro Focus Support website at <https://softwaresupport.softwaregrp.com>.

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

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

# Contents

Chapter 1: Introduction .....	9
Intended Audience .....	9
General Information .....	9
Micro Focus Websites .....	9
Chapter 2: About Troubleshooting Micro Focus Configuration Management System .....	10
How to Troubleshoot .....	10
General Checks .....	11
Before Calling Support .....	12
Before Calling Your Support Representative .....	12
Prepare the Generated Data to Be Sent to Micro Focus Customer Support Service .....	13
Retrieve Server Logs by Executing LogGrabber .....	13
Retrieve Probe Logs .....	14
Available Troubleshooting Resources for UCMDB .....	15
About Log Files .....	15
UCMDB Log Files .....	15
UCMDB Log Files .....	16
General Log Files .....	17
Class Model Log Files .....	20
TQL Log Files .....	20
Data-In Log Files .....	21
History Log Files .....	22
Enrichment Log Files .....	24
Dal Log Files .....	25
Authorization Log Files .....	25
UCMDB UI Log Files .....	26
SAML Authentication Log File .....	27
Data Flow Management Log Files .....	28
Log Severity Levels .....	32
Changing Log Levels .....	32
How to Download a Zip File of Log Files and Thread Dumps .....	32

How to Retrieve UCMDB Server Logs for a Specific Time Frame .....	33
How to Use the User Activity Log .....	34
Log Configuration Dialog Box .....	35
Data Flow Probe Log Files .....	36
General Logs .....	37
Probe Gateway Logs .....	39
Probe Manager Logs .....	39
Discovery Rules Engine Log Files .....	40
TQL Parameter Logs .....	41
Pattern Statistics Log .....	41
Audit Short/Detailed Log (TQL Perspective) .....	42
Incremental Statistics Log .....	42
Incremental Splitter Log .....	43
Incremental Detailed Log .....	43
How to Troubleshoot and Debug Using Generic Adapter Log Files .....	44
<b>Chapter 3: Troubleshooting Deployment .....</b>	<b>47</b>
Troubleshooting Deployment - UCMDB Server .....	47
Troubleshoot UCMDB in Non-English Locales .....	48
Troubleshooting Deployment - Keystore and Truststore .....	50
Troubleshooting Keystore and Truststore - Non-FIPS mode .....	50
Troubleshooting Keystore and Truststore - FIPS mode .....	56
Troubleshooting Deployment - Configuration Manager .....	59
Configuration Manager General Limitations and Troubleshooting .....	59
Configuration Manager Upgrade .....	60
Logging In to Configuration Manager .....	60
Configuration Manager Authentications .....	63
Troubleshooting Deployment - Data Flow Probe .....	63
Troubleshooting Probe Upgrade .....	65
Troubleshooting Probe Upgrade - Permission Check .....	65
Troubleshooting Probe Upgrade - How to check if a probe is upgraded successfully? .....	69
Troubleshooting Probe Upgrade - Known Issues, Limitations, and Other General Issues .....	70
Troubleshooting Probe Upgrade - PostgreSQL Upgrade .....	74
Troubleshooting Probe Upgrade - Customized Probe Configuration ..	76
<b>Chapter 4: Troubleshooting Administration .....</b>	<b>78</b>

Troubleshooting – Logging In to UCMDB .....	78
Troubleshooting and Limitations – UCMDB Server Administration .....	81
Troubleshooting and Limitations – Package Manager .....	82
CMS UI - Known Issues .....	83
Troubleshooting - Configure the Enhanced Search Engine .....	84
UCMDB doesn't start because of the search subsystem manager. What do I do? .....	84
The search doesn't return any results. ....	84
The search doesn't find CI types that I want. ....	85
The search presents too many unwanted results. ....	85
Problem with configuration - restore factory defaults .....	85
Logs and debugging info .....	86
Troubleshooting - High Availability Mode .....	86
Troubleshooting - Disable History for Specific Object CITs .....	87
Chapter 4: Troubleshooting UCMDB Server Performance with Thread Sampler .....	89
Example entry in slow.log .....	90
Chapter 4: Troubleshooting Purging - How to View and Delete History Partitions .....	91
Check partitions .....	91
Delete partitions .....	92
Logging .....	94
Chapter 5: Troubleshooting Data Flow Management .....	96
Troubleshooting and Limitations – Data Flow Probe Setup .....	97
Data Flow Probe Setup - Troubleshooting .....	97
Data Flow Probe Setup - Limitations .....	100
Troubleshooting Probe Auto Upgrade .....	101
Troubleshooting and Limitations – Multiple CMDB Integration .....	107
Troubleshooting .....	107
Limitations .....	109
Universal Discovery Troubleshooting and Limitations .....	110
Troubleshooting – Universal Discovery .....	110
Discovery Results Do Not Appear in the Topology Map .....	111
Triggers Running Unexpectedly in Management Zone .....	111
Job Running Triggers Not Within Probe Limit .....	111
Networks and IPs .....	112
TCP Ports .....	112

Discover Resources on a Windows XP Machine .....	113
Trigger CIs for jobs in a management zone are in continuous "Progress" status .....	113
Device attributes are not populating or contain unexpected or null values .....	113
Inventory Discovery by Scanner job fails .....	114
Data push troubleshooting .....	114
Test connection failed for UCMDB-UCMDB integration where one UCMDB uses SSL authentication for probes and the other does not .....	115
How to View the Status of AM and SM Integration Jobs .....	115
How to View the Integration Point Log .....	117
Limitations – Universal Discovery .....	118
Inventory Discovery Troubleshooting .....	118
How to view all information related to a device in a centralized view? .....	119
How to troubleshoot network availability and latency issue related to a device? .....	120
IP Ping and Agent Ping .....	121
SNMP Ping .....	124
Tracert and DNS Query .....	126
How to check the key indexes of the discovery history information for a discovered device? .....	126
How to check device related logs for a discovered device? .....	132
Agent deployment log .....	132
Scanner deployment log .....	133
Virtualization log .....	134
How to invoke discovery job relevant to the discovered device manually and check status to identify potential discovery errors? .....	134
Install UD Agent .....	135
Update UD Agent .....	137
Upgrade Scanner / Run Scanner / Download Scan File / Parse Enriched Scan File / Run Agentless Scanner .....	139
Uninstall Agent .....	141
Rerun Discovery .....	142
VMware Discovery Jobs .....	143
How to check which pattern (management zone) is used in the discovery for a discovered device? .....	144
How to check detailed discovery settings used in the discovery for a discovered device? .....	146

How to check the SNMP credentials used in the discovery for a discovered device? .....	149
How to View Discovery Status and Errors for a Selected CI from the Discovery Progress Widget .....	151
APLS Integration Troubleshooting - Error Handling Messages .....	153
<b>Chapter 6: Troubleshooting Configuration Manager .....</b>	<b>155</b>
Troubleshooting and Limitations – Content Management .....	155
Troubleshooting and Limitations – Federating Data to UCMDB .....	156
Troubleshooting – Explore Views .....	156
Troubleshooting – Review/Authorize .....	159
Troubleshooting and Limitations – Views .....	161
Troubleshooting and Limitations – Policies .....	161
<b>Chapter 7: Troubleshooting Automated Service Modeling .....</b>	<b>162</b>
Troubleshooting Automated Service Modeling (ASM) - General Guideline .....	162
Troubleshooting ASM - Host Discovery by Shell job .....	164
Troubleshooting ASM - References .....	170
Add an IP Range to the Ranges Setting .....	170
Discover Load Balancers .....	170
Add or Edit Credentials .....	170
Edit the portNumberToPortName.xml File .....	171
Add or Edit Application Signatures .....	171
<b>Chapter 8: Troubleshooting Development .....</b>	<b>172</b>
Troubleshooting Migration from Jython Version 2.1 to 2.5.3 .....	172
String Formatting .....	172
Checking String Type .....	173
Non-ASCII character in file .....	173
Import sub-packages .....	174
Iterator Changes .....	174
Raising Exceptions .....	174
Troubleshooting and Limitations – Developing Generic Database Adapters .....	175
General Limitations .....	175
JPA Limitations .....	175
Functional Limitations .....	176
Troubleshooting - Build an Adapter Package .....	176
<b>Chapter 9: Troubleshooting Hardening .....</b>	<b>178</b>

Troubleshooting and Limitations - Data Flow Credentials Management .....	178
Troubleshooting and Limitations - LW-SSO Authentication .....	178
Known Issues .....	178
Limitations .....	179
Troubleshooting Hybrid User Management - LDAP authentication .....	181
Troubleshooting - High Availability Mode .....	182
Troubleshooting - Database TLS Connection Issues .....	183
<b>Chapter 10: Troubleshooting Modeling .....</b>	<b>184</b>
Troubleshooting and Limitations – Topology Query Language .....	184
Understanding Validation Restrictions .....	185
Impact Analysis TQL Query Validation .....	186
Enrichment TQL Query Validation .....	187
Troubleshooting and Limitations – CI Selector .....	188
Unavailable Views and CIs .....	189
<b>Send documentation feedback .....</b>	<b>190</b>



# Chapter 1: Introduction

This guide describes how to troubleshoot problems you may encounter when using Micro Focus Configuration Management System components. It contains problems and proposed solutions to resolve them.

## Intended Audience

This section is intended for administrators and support engineers responsible for administering and maintaining CMS systems.

## General Information

General information about Micro Focus Configuration Management System can be found at <https://www.microfocus.com/cmdb>.

## Micro Focus Websites

For additional information, see the following Micro Focus websites:

- <http://www.microfocus.com>
- <https://softwaresupport.softwaregrp.com/group/softwaresupport>
- Micro Focus Software Support Matrices site:  
<https://softwaresupport.softwaregrp.com/group/softwaresupport/support-matrices>

# Chapter 2: About Troubleshooting Micro Focus Configuration Management System

This chapter includes:

How to Troubleshoot .....	10
General Checks .....	11
Before Calling Support .....	12
Before Calling Your Support Representative .....	12
Prepare the Generated Data to Be Sent to Micro Focus Customer Support Service .....	13
Available Troubleshooting Resources for UCMDB .....	15
About Log Files .....	15
UCMDB Log Files .....	15
Data Flow Probe Log Files .....	36
TQL Parameter Logs .....	41
How to Troubleshoot and Debug Using Generic Adapter Log Files .....	44

## How to Troubleshoot

To solve problems quickly and efficiently:

1. Make yourself familiar with the general troubleshooting information
2. Check if your problem is described in this **UCMDB Help**, for example, the Release Notes or the Troubleshoot sections:
  - a. To troubleshoot Installation and Upgrade, see the interactive [Universal CMDB Deployment Guide](#).
  - b. To troubleshoot Integrations, see the following sections of the Universal CMDB Discovery and Integrations Content Help:
    - Micro Focus Integrations
    - Third Party Integrations
  - c. To troubleshoot Discovery, see the following sections of the Content Help:

- Discovery Activities
  - Discovery Modules
  - Supported Content
- d. To troubleshoot general administration or configuration tasks, see the [Administer](#) section.
3. If you cannot find a solution to your problem, report the problem to the Micro Focus Customer Support Service. On how to prepare the required data for the support organization, see "[Prepare the Generated Data to Be Sent to Micro Focus Customer Support Service](#)" on page 13.

## General Checks

Before proceeding, ensure that:

- You are not running into known limitations that cannot currently be overcome. For specific information on Universal CMDB limitations and recommendations, as well as known Universal CMDB and non-Universal CMDB problems, see the *Support Matrix section of the UCMDB Help*, Universal CMDB Release Notes or known issues in general across UCMDB. You can also check the Knowledge Base: <https://softwaresupport.softwaregrp.com/group/softwaresupport>.
- Your problem is not related to third-party hardware or software. In this case, contact the vendor support.
- You have the latest Universal CMDB patches or hotfixes installed. Patches and hotfixes can be obtained from: <https://softwaresupport.softwaregrp.com/group/softwaresupport>
  - To check which UCMDB patches are installed on your system, go to the UCMDB Server JMX console and invoke the **UCMDB:service=Server Services > viewSystemInformation** JMX method.
- Check the if your problems is not a known issue or has a solution mentioned in the latest release notes:  
  
UCMDB Content Pack, UCMDB CUP, CMS UI, or Discovery Knowledge Pack
- You have appropriate operating system patches installed
- The system is not running low on memory – there is sufficient resource allocation on the server
- Check the respective UCMDB logs for each type:
  - Client (UI) logs: **%temp%\UcmdbLog\log\applet-errors.log** (Windows)
  - CMS UI Embedded logs: **<UCMDBServer>\runtime\log\ucmdb\_browser.log** or **warn\_log**

- CMS UI Standalone logs : **<WebAppServer>\<webappcontext>\<log\_folder>**
- Server logs: **<UCMDBServer>\runtime\log\error.log**
- Probe logs: **<DataFlowProbe>\runtime\log\probe-error.log**
- Check if your problem is not described in the troubleshooting sections of applicable user guides.

## Before Calling Support

This chapter includes:

Before Calling Your Support Representative .....	12
Prepare the Generated Data to Be Sent to Micro Focus Customer Support Service .....	13

## Before Calling Your Support Representative

If you cannot solve your problem, report it. Before contacting the Micro Focus Customer Support Service, ensure that:

- You have performed the general checks  
See ["About Troubleshooting Micro Focus Configuration Management System" on page 10.](#)
- You have collected the relevant data about the problem you will send to the Micro Focus Customer Support Service:
  - a. A description of the problem, including timestamps if applicable.
  - b. A description of your environment:
    - i. Is this productions or test environment
    - ii. Is it a new implementation – install or upgrade
    - iii. Any environment changes prior to the encountered issue
    - iv. Has the observed behavior ever functioned correctly previously
  - c. Collect the output of the **viewSystemInformation** JMX method from the UCMDB server **JMX console > UCMDB:service=Server Services > viewSystemInformation.**
  - d. Collect the relevant error logs from the General Check section
  - e. Collect the output of Run Support Handlers from the UCMDB server **JMX console >**

**UCMDB:service=Supportability Services > runSupportHandlersForSpecificCategories**,  
use empty categories.

The Micro Focus Customer Support Service will then provide you with the further instructions. You might be asked to:

1. Enable UCMDB Debugging
2. Prepare the generated data for sending to the Micro Focus Customer Support Service

## Prepare the Generated Data to Be Sent to Micro Focus Customer Support Service

The Micro Focus Customer Support Service might ask you to gather and send the data they need to resolve a technical issue. Since UCMDB operates in large network environments, the data sometimes may be difficult to gather. The UCMDB LogGrabber is a tool for collecting and packaging log data. The methods to use the LogGrabber tool are described below.

## Retrieve Server Logs by Executing LogGrabber

This task describes how to retrieve UCMDB Server log files.

- **If the UCMDB Server is operational**
  - a. Launch the Web browser and enter the following address: **https://localhost:8443/jmx-console**  
You may have to log in with a user name and password. (Default user name is **sysadmin**)
  - b. Search and click **UCMDB:service=Server Services** to open the JMX MBEAN View page.
  - c. Click **executeLogGrabber**.
  - d. Click **Invoke**.
  - e. Provide the downloaded zip package to Micro Focus Customer Support Service.
- **If the UCMDB server is not operational**
  - a. Execute the LogGrabber script: **<UCMDB\_Server\_Home>/tools/logGrabber/logGrabber.bat**
  - b. Clear the content of the following folder: **<UCMDB\_Server\_Home>/runtime/log**

Make sure NOT to remove the **log** folder itself.

- c. Restart the UCMDB Server.
- d. Allow some time for the problem to reproduce.
- e. Execute the LogGrabber script again: **<UCMDB\_Server\_Home>/tools/logGrabber/logGrabber.bat**
- f. Collect the most recent LogGrabber archive first from **<UCMDB\_Server\_Home>/runtime/logGrabber\_xxx.zip** and upload it to the Support incident.
- g. Once the upload completes in [step f](#), inform Support and upload the LogGrabber output of [Step a](#).

## Retrieve Probe Logs

- If the Probe is operational
  - a. Launch the Web browser and enter the following address: **https://localhost:8453/**  
You may have to log in with a user name and password. (Default user name is **sysadmin**)
  - b. Go to **GeneralUtils**.
  - c. Click **executeLogGrabber**.
  - d. Click **Invoke**.
  - e. Provide the downloaded zip package to Micro Focus Customer Support Service.
- If the Probe is not operational
  - a. Zip the content of the following folder: **<DataFlowProbe>/runtime/log**
  - b. Clear the content of the following folder: **<DataFlowProbe>/runtime/log**  
Make sure NOT to remove the **log** folder itself.
  - c. Restart the Data Flow Probe.
  - d. Allow some time for the problem to reproduce.
  - e. Zip again the content of the folder: **<DataFlowProbe>/runtime/log**
  - f. Collect the most recent log archive first and upload it to the Support incident.
  - g. Once the upload completes in [step f](#), inform Support and upload the log zip of [Step a](#).

# Available Troubleshooting Resources for UCMDB

- **Installation troubleshooting.** Use to troubleshoot common problems that you may encounter when installing Universal CMDB, and the solutions to those problems. See ["Troubleshooting Deployment" on page 47](#).
- **Login troubleshooting.** Use to troubleshoot possible causes of failure to log in to Universal CMDB. See ["Troubleshooting – Logging In to UCMDB" on page 78](#).
- **Micro Focus Software Self-solve knowledge base.** Use to search for specific troubleshooting information on a wide variety of topics. Located on the [Micro Focus Support](#) site, the Micro Focus Software Self-solve knowledge base can be accessed by selecting Troubleshooting & Knowledge Base from the Universal CMDB Help menu.  
  
Note that only registered customers can access the resources on the Micro Focus Support site. Customers who have not yet registered can do so from this site.
- **Universal CMDB Log files.** Use to troubleshoot CMDB runtime problems. For details, see ["UCMDB Log Files"](#).
- **Data Flow Management log files.** Use to troubleshoot DFM problems. For details, see ["Data Flow Probe Log Files"](#).
- **Query log files.** Use to view definitions for query parameter log files. For details, see ["UCMDB Log Files"](#).

## About Log Files

This section includes:

UCMDB Log Files .....	15
Data Flow Probe Log Files .....	36
TQL Parameter Logs .....	41
How to Troubleshoot and Debug Using Generic Adapter Log Files .....	44

## UCMDB Log Files

This section includes:

UCMDB Log Files .....	16
Log Severity Levels .....	32
How to Download a Zip File of Log Files and Thread Dumps .....	32
How to Retrieve UCMDB Server Logs for a Specific Time Frame .....	33
How to Use the User Activity Log .....	34
Log Configuration Dialog Box .....	35

## UCMDB Log Files

CMDB log files enable you to perform basic troubleshooting of CMDB runtime problems. Additionally, by tracking the CMDB behavior in the log files, you can examine the effects of changes made in the system. The CMDB is composed of subsystems and each subsystem records to several log files. CMDB Server logs have consistent format. The order is data and time: **(format "yyyy-MM-dd hh:mm:ss:SSS") logLevel [Thread Name]**. The wrapper log is an exception to this standard. These settings can be changed from log properties files located in the **UCMDBServer\conf\log\** folder.

Log files are located in:

- **Windows:** C:\UCMDB\UCMDBServer\runtime\log
- **Linux:** /opt/UCMDB/UCMDBServer/runtime/log

**Note:** UCMDB log levels should be set to the OOTB values. They may be increased when investigating issues. However, after obtaining the required information the log levels should be reverted. Increased log levels for a longer period of time may have an impact over performance.

If you want to delete the logs, you should delete the content in the **log** folder only, and never delete the folder itself. Make sure that the **log** folder always exists. If the **log** folder is deleted accidentally, create the **log** folder manually before starting up the UCMDB Server.

This section includes the following topics:

- ["General Log Files" on the next page](#)
- ["Class Model Log Files" on page 20](#)
- ["TQL Log Files" on page 20](#)
- ["Data-In Log Files" on page 21](#)
- ["History Log Files" on page 22](#)
- ["Enrichment Log Files" on page 24](#)



- ["Dal Log Files" on page 25](#)
- ["Authorization Log Files" on page 25](#)
- ["UCMDB UI Log Files" on page 26](#)
- ["SAML Authentication Log File" on page 27](#)
- ["Data Flow Management Log Files" on page 28](#)

## General Log Files

### Quota Log Parameters

The log name is **cmdb.quota.log**.

Log File	Description
Purpose	Quota names, quota values, and current quota levels.
Information Level	Quota names and values set in the server and customer levels during a customer load.
Error Level	CMDB operations that fail because they exceed quota limits.
Debug Level	A count collector runs every <b>n</b> minutes and gathers current counts for all quotas. Collected counts are logged.
Basic Troubleshooting	If operations fail because of quota limits, check the count growth and quota values.

### CMDB Operation Statistics Log

The log name is **cmdb.operation.statistics.log**.

The log does not appear in the log folder by default. Only when you perform some specific action, the log becomes available. For example, when you invoke the **resetOperationStatistics** JMX method from the **Framework Services** category, it resets CMDB Server Operation Statistics and writes dump to this log.

Log File	Description
Purpose	Statistics for all operations performed in the past 15 minutes including worst operation instances.
Information Level	Statistics per operation including operation class name, caller application, and customer ID.

Log File	Description
	Default of 10 worst operation instances.
Error Level	Disables the statistics feature.
Debug Level	Not available.
Basic Troubleshooting	Check when there is a performance slowdown.

## Configuration Log

The log name is **configuration.log**.

Log File	Description
Purpose	Contains basic environment details, including: <ul style="list-style-type: none"><li>• Server version and CUP version</li><li>• Database vendor and version</li><li>• Content pack version</li><li>• High Availability configuration</li><li>• Data Flow Probe version</li><li>• Changes to settings (each setting is audited in the log)</li></ul>
Information Level	Information is written to the log when the system starts up or when a setting is changed.
Error Level	Not available.
Debug Level	Not available.
Basic Troubleshooting	Used by Customer Support to help reproduce customer problems.

## Keystore and Truststore Password Save Log

The log name is **save\_store\_pass.log**.

Log File	Description
Purpose	Information about installation log: keystore password and truststore password save time and encryption type.
Information Level	Operation details.

Log File	Description
Error Level	Not available.
Debug Level	Not available.
Basic Troubleshooting	This is especially useful when installing and starting the UCMDB server. You can use this log information together with the information in <a href="#">Troubleshooting Keystore and Truststore</a> .

## Keystore and Truststore Password Verify Log

The log name is **verify\_store\_pass.log**.

Log File	Description
Purpose	Information about the installation log: whether keystore password and truststore password are saved correctly or not. If <b>server-storepass.conf</b> exists, then the UCMDB server installer will change keystore and truststore passwords with keytool.
Information Level	Operation details.
Error Level	Not available.
Debug Level	Not available.
Basic Troubleshooting	This is especially useful when installing and starting the UCMDB server. You can use this log information together with the information in <a href="#">Troubleshooting Keystore and Truststore</a> .

## Long Running Threads Troubleshooting

The log name is **slow.log**.

Log File	Description
Purpose	This log file is used to troubleshoot long running threads and operations.
Information Level	A list of slow running threads with operations will be displayed. A list of all managers and their load will also be displayed. Finally a list of open connections to the database will be displayed.
Error Level	Errors about collecting the information about the threads will be displayed. All threads interrupted due to operation timeout will be displayed.
Debug Level	No information.
Basic Troubleshooting	If an operation takes a lot of time you will see it in this log. If an operation is interrupted you will see it in this log.

## Class Model Log Files

### CI Type Model Log

The log name is **cmdb.classmodel.log**.

This log should appear when you perform operations on the UCMDB class model, like creating a new CI Type, or adding an attribute on an existing CI Type.

Log File	Description
Purpose	CI Type Model errors and debug messages.
Information Level	When a CI Type Model is loaded, incorrect definitions are logged as informational messages. An example of an incorrect definition is <code>duplicate attributes</code> .
Error Level	Not available.
Debug Level	Every CI Type update includes the following: <ul style="list-style-type: none"><li>• Original CIT in XML format</li><li>• New CIT in XML format</li><li>• Differences between the CITs</li></ul> If the CI Type Model update is rejected, the reason is logged.
Basic Troubleshooting	Compares the differences that the server finds between the original CIT and the new CIT. This is useful to understand the following scenarios: <ul style="list-style-type: none"><li>• A CIT in a package failed</li><li>• An action in the CIT browser applet failed</li><li>• An action in the CIT browser applet succeeded when it should have failed</li></ul>

## TQL Log Files

### CMDB Notification Log

The log name is **cmdb.notification.log**.

Log File	Description
Purpose	Notification messages from the time of the component's creation in the CMDB

Log File	Description
	until the client's listener receives a message.  Most components receive configuration changes from the CMDB in push mode, by the notification mechanism, rather than in pull mode.
Information Level	<ul style="list-style-type: none"><li>• Startup and shutdown of publishers</li><li>• Register and unregister remote and internal listeners</li></ul>
Error Level	<ul style="list-style-type: none"><li>• Errors when messages are published</li><li>• Errors when messages are received</li></ul>
Debug Level	<ul style="list-style-type: none"><li>• Unique message ID</li><li>• Number of changes that a message includes as well as more details according to the type of the message (for example, the TQL result version)</li><li>• JMS header properties</li></ul>
Basic Troubleshooting	If an application does not receive a notification, check the following: <ul style="list-style-type: none"><li>• a listener is registered with the appropriate notification filter</li><li>• a message is published with data that matches this filter</li><li>• a message is received by the listener (use the unique message ID to verify)</li></ul>

## Data-In Log Files

### CMDB Model Audit Short Log

The log name is **cmdb.model.audit.short.log**.

Log File	Description
Purpose	Information about a CI Type operation: type of operation, data received as input, and what happened to the data in each CIT.  Also contains information about the caller application, execution time, and persistency time.
Information Level	Operation details.
Error Level	Not available.
Debug Level	Not available.
Basic Troubleshooting	If there are no changes when there should be, check the following:

Log File	Description
	<ul style="list-style-type: none"><li>• Whether the operation exists.</li><li>• Whether the input is correct.</li><li>• What happened to the data. There may have been a false update.</li></ul> <p>This is especially useful when running DFM to trace the input.</p>

## History Log Files

### History Log

The log name is **history.log**.

Log File	Description
Purpose	Records general history events
Information Level	<ul style="list-style-type: none"><li>• Auto completion events</li><li>• Auto complete table lock/unlock messages</li><li>• Tenants bitmask column size handling</li><li>• Delete customer fuse notice</li></ul>
Debug Level	<ul style="list-style-type: none"><li>• Auto completion details</li><li>• History Root table handling messages</li></ul>

### History Audit Update Log

The log name is **history.update.audit.log**.

Log File	Description
Purpose	Tracks events saved in the History tables
Information Level	<ul style="list-style-type: none"><li>• Details all events stored in the history tables</li><li>• Event statistics</li></ul>
Debug Level	Database statistics

## History Partition Log

The log name is **history.partition.log**.

Log File	Description
Purpose	<ul style="list-style-type: none"><li>• Records history partition data.</li><li>• Records the Baseline process events.</li></ul>
Information Level	<ul style="list-style-type: none"><li>• Add/Remove partition history tables</li><li>• Baseline events</li><li>• Baseline statistics</li></ul>
Error Level	<ul style="list-style-type: none"><li>• Table partition failures</li><li>• Baseline process failures</li></ul>

## Query History Log

The log name is **history.queries.log**.

Log File	Description
Purpose	Records all the queries performed on the history tables.
Information Level	<ul style="list-style-type: none"><li>• Query condition</li><li>• Query results summary</li></ul>
Error Level	Fuse exceeded
Debug Level	<ul style="list-style-type: none"><li>• Query condition details</li><li>• Query result details</li></ul>

## History Class Model Changes Log

The log name is **history.classmodel.changes.log**.

Log File	Description
Purpose	Tracks all the class model changes that affect the history tables.
Information Level	Class aligning messages
Error Level	Errors that occurred during class aligning

## History Purging Log

The log name is **history.purge.log**.

Log File	Description
Purpose	Records the History purging process events
Information Level	Purging process information
Error Level	Errors that occurred during the purging process
Debug Level	Details about purged data

## Enrichment Log Files

### CMDB Enrichment Log

The log name is **cmdb.enrichment.log**.

Log File	Description
Purpose	<ul style="list-style-type: none"><li>• Enrichment definitions: adding, updating, removing, and calculating.</li><li>• Calculation results such as how many CIs were added, how many relationships were removed, and so forth.</li><li>• Supplies the reason for a calculation failure. Failure in a model update, however, is not included since it is an asynchronous execution.</li></ul>
Information Level	<ul style="list-style-type: none"><li>• Add, update, and remove enrichment definitions.</li><li>• Add, update, and remove CIs or relationships to or from a model.</li></ul>
Error Level	Calculation failure.
Debug Level	Traces the enrichment calculation process.
Basic Troubleshooting	<ul style="list-style-type: none"><li>• If no calculation was carried out, check the definition of <b>add enrichment</b>.</li><li>• If there are no results, check the <b>finish calculate</b> entry.</li></ul>



## Dal Log Files

### CMDB Dal Log

The log name is **cmdb.dal.log**.

Log File	Description
Purpose	Information about activity that occurred in the data access layer, the layer that works with the CMDB.
Information Level	Not available.
Error Level	<ul style="list-style-type: none"><li>• Connection pool errors</li><li>• Database errors</li><li>• Command execution errors</li></ul>
Debug Level	<ul style="list-style-type: none"><li>• All DAL commands executed</li><li>• All SQL commands executed</li></ul>
Basic Troubleshooting	<p>If you suspect that CMDB actions are taking too long, check the time spent on queries and updates in the DAL logs and operation logs.</p> <p>Exception details and ID are entered into the log. The exception ID appears in the exception itself.</p>

## Authorization Log Files

### CMDB Authorization Management Log

The log name is **security.authorization.management.log**.

Log File	Description
Purpose	Audit all modifications related to the authorization model.
Information Level	<ul style="list-style-type: none"><li>• Creation and deletion of users, user groups, tenants, roles, and resource groups.</li><li>• Addition and removal of users from user groups, changes to user passwords, and changes in users' default tenants.</li><li>• Addition and removal of permissions from roles and changes in read-only</li></ul>

Log File	Description
	status of roles. <ul style="list-style-type: none"><li>• Addition and removal of resources from resource groups.</li><li>• Changes in user role assignments.</li><li>• Changes in resource tenant associations.</li></ul>
Error Level	Failure to create or modify authorization resources, such as trying to create a user with an existing name.
Debug Level	Web services login requests.
Basic Troubleshooting	May be used to track why a user no longer has a specific permission.

## CMDB Authorization Permissions Log

The log name is **security.authorization.permissions.log**.

This log contains detailed information for authorization and out-of-the-box information. To enable the print of information, you may need to set the log level to **DEBUG**.

Log File	Description
Purpose	Debug authorization permissions queries.
Debug Level	Print all existing permissions for the user currently logged in, whenever they are queried in the server.
Basic Troubleshooting	<p>To check a specific permission issue, turn on the debug level, perform the action in the UI, turn the debug level off, and check the log for the existing permissions of the user.</p> <p>It is not recommended to keep this log at debug level, because it generates a large amount of printed output.</p>

## UCMDB UI Log Files

### Client-side Applet Logs

The following client side applet logs are also available:

- **applet-operations.log**. Tracks the operations that are executed from the CMDB UI to the UCMDB server.

- **applet-general.log**. General log for the UI.
- **applet-cacheStatistics.log**. Tracks statistics of the UI cache.
- **applet-missing\_resources.log**. Missing resources log.
- **applet-applet-tasks.log**. Logs task executions.
- **applet-timeMeasure.log**. Log for measuring performance.
- **applet-memoryTracker.log**. Tracks the memory usage of the UI.
- **applet-errors.log**. Logs the errors that occurred in the UI

**Note:** UCMDB UI log files are present in the **%Temp%/UcmdbLog/log** folder on the machine from which you access the UCMDB UI.

## SAML Authentication Log File

### **cmdb.samlAuthentication.log**

This log file contains all log information related to SAML Authentication. By default, the log level is set to **DEBUG**. You can change the log level in the **conf/log/cmdb.properties** file by updating the following line:

```
samlAuthentication= DEBUG
```

**Note:** For starters, we suggest leaving this log on **DEBUG** in order to resolve possible problems more easily.

Log File	Description
Purpose	Log the details related to SAML authentication.
Information Level	The default log level is <b>DEBUG</b> for now.
Error Level	Errors that appeared during SAML Authentication.
Debug Level	Details related to SAML Authentication, like the request send to IdP, the response received, and so on.
Basic Troubleshooting	Errors could appear if the configurations are not done correctly. If anything wrong happens, it will be logged in the file.

## Data Flow Management Log Files

Data Flow Management log files store information about data flow activity (discovery and integrations), as well as related errors, that occur on the Server side.

### **mam.AutoDiscovery.log**

Contains information about tasks running on the server. The server provides services to the user interface or the Probe Gateway, such as: activating jobs, processing results from the Probe, or creating tasks for the Probe.

Level	Description
Error	All DFM process errors on the server side.
Information	Information about requests being processed.
Debug	Logs mainly for debugging purposes.

**Basic Troubleshooting.** Check this log when you have invalid user interface responses or errors you need to explore. This log provides information to enable you to analyze the problems.

### **discoveryServlet.log**

This log receives messages from:

- **The Collectors Utilities Servlet.** The user interface connects to the server through this servlet.
- **The Collectors Servlet.** The Probe requests new tasks from the server through this servlet.
- **The Collectors Results Servlet.** The Probe sends new results through this servlet.
- **The Collectors Download Servlet.** The Probe downloads new server data through this servlet.

Level	Description
Error	All errors in the servlet.
Information	Information about user requests and Probe task requests.
Debug	<ul style="list-style-type: none"><li>• User requests</li><li>• Probe requests to read DFM tasks.</li><li>• Probe access to the servlet.</li></ul>

### **Basic Troubleshooting**

- User Interface – Server communication problems.
- Probe – Server communication problems.

Some processing problems may be written to this log instead of to **mamAutoDiscovery.log**.

### **mam.autodiscovery.results.stat.log**

Contains the statistics of the results received from the Probe.

### **mam.autodiscovery.accuratedependency.log**

(Deprecated) Contains information about accurate dependency for the Automatic Service Modeling feature. This log is related to the old ASM version (before Content Pack 18), and is no longer in use.

### **mam.dispatch.log**

Contains all the dispatch related information.

To enable this log,

1. Locate and open the **<UCMDB\_Server\_Home>/conf/log/mam.properties** file.
2. Manually add the following settings into the **mam.properties** file:

```
log4j.category.mam.dispatch=${loglevel}, mam.dispatch.appender
#####
##    mam.packaging                ##
#####

log4j.appender.mam.dispatch.appender=com.mercury.topaz.cmdb.shared.base.log.
BetterRollingFileAppender

log4j.appender.mam.dispatch.appender.File=${logs.dir}/mam.dispatch.log
log4j.appender.mam.dispatch.appender.MaxFileSize=${def.file.max.size}
log4j.appender.mam.dispatch.appender.MaxBackupIndex=${def.files.backup.coun
t}

log4j.appender.mam.dispatch.appender.layout=org.apache.log4j.PatternLayout
log4j.appender.mam.dispatch.appender.layout.ConversionPattern=${msg.layout}
```

3. Save the file.

## Autodiscovery Dal Log

The log name is **mam.autodiscovery.dal.log**.

Log File	Description
Purpose	Holds information on queries and other actions taken on the server's database tables as part of the discovery process.
Information Level	A summary of actions taken and their results on the database (such as retrieving information, deleting records, and so on).
Error Level	All critical errors that occurred during the attempt to access the database.
Debug Level	Detailed information on query parameters and/or the results that are retrieved from them
Basic Troubleshooting	If there are any database errors or failures (such as connection failed, technical error in the query, and so on), the error log is included in this log file also.

## workflow\_sizing.log

Enabling this log file helps you to collect running statistics (for example, time spent on normalization and auto delete) of each modules on a probe.

To enable this log, follow these steps:

1. On the probe, locate and open the **/conf/log/probeGWLog4j.properties** and **/conf/log/probeMgrLog4j.properties** files.
2. Manually add the following settings into each of the above files:

```
#####  
### cmdb.workflow.sizing          ##  
#####  
  
log4j.category.cmdb.workflow.sizing=INFO, cmdb_workflow_sizing  
log4j.appender.cmdb_workflow_  
sizing=com.mercury.topaz.cmdb.shared.base.log.BetterRollingFileAppender  
log4j.appender.cmdb_workflow_sizing.File=${logs.dir}/workflow_sizing.log  
log4j.appender.cmdb_workflow_sizing.Append=true  
log4j.appender.cmdb_workflow_sizing.MaxFileSize=512MB  
log4j.appender.cmdb_workflow_sizing.Threshold=INFO
```

```
log4j.appender.cmdb_workflow_sizing.MaxBackupIndex=10  
log4j.appender.cmdb_workflow_sizing.layout=org.apache.log4j.PatternLayout  
log4j.appender.cmdb_workflow_sizing.layout.ConversionPattern=<%d> [%-5p]  
[%t] (%F:%L) - %m%n  
log4j.appender.cmdb_workflow_sizing.encoding=UTF-8
```

3. Save the files.
4. Restart the probe.

### Sample log

```
<2015-11-11 13:56:51,459> [INFO ] [ProbeGW Task Results Sender]  
(TaskResultsSenderThread.java:458) -  
[TaskResultsSenderThread.handleSuccessTriggers.start][desc=update ID  
mapping,size=1]  
  
<2015-11-11 13:56:51,460> [INFO ] [ProbeGW Task Results Sender]  
(TaskResultsSenderThread.java:481) -  
[TaskResultsSenderThread.handleSuccessTriggers.stop][desc=update ID  
mapping,size=1]
```

### Probe Auto Upgrade Log

The log name is **probe\_auto\_upgrade.log**.

It shows in the **C:\UCMDB\DataFlowProbe\runtime\log\probeUpgradeLogs\<source\_version>to<target\_version>** folder. For example:

**C:\UCMDB\DataFlowProbe\runtime\log\probeUpgradeLogs\10.32to10.33.**

This log file is also sent to the UCMDB server and shows as **<domain\_name>\_probenname\_auto\_upgrade.log** in the **C:\UCMDB\UCMDBServer\runtime\log\probeUpgradeLogs\<source\_version>to<target\_version>\failed|success** folder.

Log File	Description
Purpose	Shows the related information when the probe auto upgrade agent upgrades a probe.
Information Level	Shows the console output of normal information.
Error Level	Any error that occurs when the probe auto upgrade agent upgrades a probe.
Debug Level	N/A
Basic Troubleshooting	Check this log file when the probe upgrade fails.

## Log Severity Levels

Each log is set so that the information it records corresponds to a certain severity threshold. Because the various logs are used to keep track of different information, each is pre-set to an appropriate default level. For details on changing the log level, see ["Changing Log Levels" below](#).

Typical log levels are listed below from narrowest to widest scope:

- **FATAL.** The log records only events that prevent the system from functioning.
- **ERROR.** In addition to Fatal events, the log records events that adversely affect the immediate functioning of the CMDB. When a malfunction occurs, you can check if Error messages were logged and inspect their content to trace the source of the failure.
- **WARN.** The log's scope includes, in addition to Fatal and Error-level events, problems for which the CMDB is currently able to compensate and incidents that should be noted to prevent possible future malfunctions.
- **INFO.** The log records all activity. Most of the information is normally routine and of little use and the log file quickly fills up.
- **DEBUG.** This level is used by Micro Focus Software Support when troubleshooting problems.

**Note:** The names of the different log levels may vary slightly on different servers and for different procedures. For example, **INFO** may be referred to as **Always logged** or **Flow**.

## Changing Log Levels

If requested by Micro Focus Software Support, you may have to change the severity threshold level in a log, for example, to a debug level. For details on changing the log level, see ["Log Configuration Dialog Box" on page 35](#).

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

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



Thread dumps are created periodically: Once a minute, a thread dump snapshot is taken and is saved to a new file in the **C:\UCMDB\UCMDBServer\runtime\log\threadDumps** folder. Thread dump files from the last hour are kept. This folder also holds the ad hoc Server snapshots that are generated during the **logGrabber** execution.

#### To generate the zip file from the client machine:

1. Launch the Web browser and enter the server address, as follows: **https://<UCMDB Server Host Name or IP>:8443/jmx-console**.

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

2. Under **UCMDB**, click **UCMDB:service=Server services** to open the JMX MBEAN View page.
3. Locate the **executeLogGrabber** operation.
4. Click **Invoke**.

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

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

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

#### To generate the zip file from the UCMDB Server:

1. Access the following folder on the UCMDB Server:  
**C:\UCMDB\UCMDBServer\tools\logGrabber\**.

2. Run the **logGrabber.bat** file.

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

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

## How to Retrieve UCMDB Server Logs for a Specific Time Frame

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

### To generate the zip file from the client machine:

1. Launch the Web browser and enter the server address, as follows: **https://<UCMDB Server Host Name or IP>:8443/jmx-console**.

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

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

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

### Limitations

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

## How to Use the User Activity Log

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

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

1. On the UCMDB server, launch the Web browser and enter the following address:  
**https://localhost:8443/jmx-console**

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

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

Next, change the log level to INFO:


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

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


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

## Log Configuration Dialog Box

This dialog box enables you to view Universal Cmdb logs and change the log level.

<b>To access</b>	On the Status bar, click <b>Log Level Configuration</b>  or select <b>Tools &gt; Log Configuration...</b> from the Modeling main menu.
<b>See also</b>	<a href="#">"Log Severity Levels" on page 32</a>

User interface elements are described below:

UI Element	Description
	<b>Apply.</b> Click to apply the selected log level to the log.

UI Element	Description
<b>Appender</b>	The name of the appender.
<b>Appender pane</b>	Displays details for the appender you selected in the Loggers pane.
<b>File</b>	Click the link to open the log file in an editor.
<b>Max file size</b>	Maximum appender file size.
<b>Max backup index</b>	Maximum number of backup indexes. Default: <b>5</b>
<b>Loggers pane</b>	An expandable list of Universal CMDB logs. Select the required log from the list: the details of the log appear in the lower pane.
<b>Logger pane</b>	Displays details for the logger you selected in the Loggers pane.
<b>Loggers table</b>	Displays a list of loggers (with Logger Name and Log level) for the selected log.
<b>Log level</b>	Select a log level from the drop-down list.
<b>Logger's appender</b>	A string defining the log category. For internal use only.
<b>Appender file</b>	The name of the logger's appender file.

## Data Flow Probe Log Files

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

**C:\UCMDB\DataFlowProbe\runtime\log**

**Note:** Alternatively, to access the Data Flow Probe's log files, log in to the JMX console (<https://localhost:8453>) and, from the main page, select the **GeneralUtils** mbean. Activating the **executeLogGrabber** function zips all the Data Flow Probe's log files. Save the .zip file locally on your client machine.

## General Logs

<b>WrapperProbeGw.log</b>	<p>Records all the Probe's console output in a single log file.</p> <ul style="list-style-type: none"><li>• <b>Levels:</b><ul style="list-style-type: none"><li>◦ <b>Error.</b> Any error that occurs within the Probe Gateway.</li><li>◦ <b>Information.</b> Important information messages, such as the arrival or removal of a new task.</li><li>◦ <b>Debug.</b> N/A</li></ul></li><li>• <b>Basic Troubleshooting:</b> Use this file for any Probe Gateway problems to verify what occurred with the Probe Gateway at any time as well as any important problems it encountered.</li></ul>
<b>probe-error.log</b>	<p>Summary of the errors from the Probe.</p> <ul style="list-style-type: none"><li>• <b>Levels:</b><ul style="list-style-type: none"><li>◦ <b>Error.</b> All errors in the Probe components.</li><li>◦ <b>Information.</b> N/A</li><li>◦ <b>Debug.</b> N/A</li></ul></li><li>• <b>Basic Troubleshooting:</b> Messages from the Probe's infrastructure only.</li></ul>
<b>wrapperLocal.log</b>	<p>When running the Probe in separate mode (that is, the Probe Manager and Probe Gateway are installed on separate machines), a log file is also saved to the Probe Manager.</p> <ul style="list-style-type: none"><li>• <b>Levels:</b><ul style="list-style-type: none"><li>◦ <b>Error.</b> Any error that occurs within the Probe Manager.</li><li>◦ <b>Information.</b> Important information messages such as received tasks, task activation, and the transferring of results.</li><li>◦ <b>Debug.</b> N/A</li></ul></li><li>• <b>Basic Troubleshooting:</b> Use this file for any Probe Manager problems to verify what occurred with the Probe Manager at any time as well as any important problems it encountered.</li></ul>
<b>postgresql.log</b>	<p>Displays database related error during the installation.</p> <p><b>Note:</b> If this log is empty, check in the Event Viewer logs.</p>
<b>pg_upgrade.log</b>	<p>Shows the running details of the <b>pg_upgrade.bat</b> script, including the details about PostgreSQL upgrade and table splitting.</p>

	<p>The log does not appear in the <b>log</b> folder by default. It appears only when you manually run the <b>pg_upgrade.bat</b> script or may appear when you select the upgrade option during probe installation.</p> <ul style="list-style-type: none"> <li>• <b>Levels:</b> <ul style="list-style-type: none"> <li>◦ <b>Error.</b> Any error that occurs when PostgreSQL upgrade or table splitting fails.</li> <li>◦ <b>Information.</b> Shows the console output and suggestions when it fails.</li> <li>◦ <b>Debug.</b> N/A</li> </ul> </li> <li>• <b>Basic Troubleshooting:</b> Check this log file when PostgreSQL upgrade or table splitting fails.</li> </ul>
<b>probe_upgrade_conf_merge.log</b>	<p>Shows the related information when probe upgrader merges configuration files.</p> <ul style="list-style-type: none"> <li>• <b>Levels:</b> <ul style="list-style-type: none"> <li>◦ <b>Error.</b> Any error that occurs when merging configuration files.</li> <li>◦ <b>Information.</b> Shows the console output of normal information.</li> <li>◦ <b>Debug.</b> N/A</li> </ul> </li> <li>• <b>Basic Troubleshooting:</b> Check this log file when the probe upgrade fails.</li> </ul>
<b>probe_auto_upgrade.log</b>	<p>Shows the related information when the probe auto upgrade agent upgrades a probe.</p> <p>It shows in the  <b>C:\UCMDB\DataFlowProbe</b>  <b>\runtime\log\probeUpgradeLogs\&lt;source_version&gt;to&lt;target_version&gt;</b> folder. For example:  <b>C:\UCMDB\DataFlowProbe</b>  <b>\runtime\log\probeUpgradeLogs\10.32to2018.08.</b></p> <p>This log file is also sent to the UCMDB server and shows as <b>&lt;domain_name&gt;_&lt;probe_name&gt;_auto_upgrade.log</b> in the  <b>C:\UCMDB\UCMDBServer\runtime\log\probeUpgradeLogs\&lt;source_version&gt;to&lt;target_version&gt;\failed success</b> folder.</p> <ul style="list-style-type: none"> <li>• <b>Levels:</b> <ul style="list-style-type: none"> <li>◦ <b>Error.</b> Any error that occurs when the probe auto upgrade agent upgrades a probe.</li> <li>◦ <b>Information.</b> Shows the console output of normal information.</li> <li>◦ <b>Debug.</b> N/A</li> </ul> </li> <li>• <b>Basic Troubleshooting:</b> Check this log file when the probe auto upgrade fails.</li> </ul>

## Probe Gateway Logs

<b>probeGW-taskResults.log</b>	<p>Records all the task results sent from the Probe Gateway to the server.</p> <ul style="list-style-type: none"><li>• <b>Levels:</b><ul style="list-style-type: none"><li>◦ <b>Error.</b> N/A</li><li>◦ <b>Information.</b> Result details: task ID, job ID, number of CIs to delete or update.</li><li>◦ <b>Debug.</b> The <b>ObjectStateHolderVector</b> results that are sent to the server (in an XML string).</li></ul></li><li>• <b>Basic Troubleshooting:</b><ul style="list-style-type: none"><li>◦ If there is a problem with the results that reach the server, check this log to see which results were sent to the server by the Probe Gateway.</li><li>◦ The results in this log are written only after they are sent to the server. Before that, the results can be viewed through the Probe JMX console (use the <b>ProbeGW Results Sender</b> MBean). You may have to log in to the JMX console with a user name and password.</li></ul></li></ul>
<b>probeGW-tasks.log</b>	<p>Records all the tasks received by the Probe Gateway.</p> <ul style="list-style-type: none"><li>• <b>Levels:</b><ul style="list-style-type: none"><li>◦ <b>Error.</b> N/A</li><li>◦ <b>Information.</b> N/A</li><li>◦ <b>Debug.</b> The task's XML.</li></ul></li><li>• <b>Basic Troubleshooting:</b><ul style="list-style-type: none"><li>◦ If the Probe Gateway tasks are not synchronized with the server tasks, check this log to determine which tasks the Probe Gateway received.</li><li>◦ You can view the current task's state through the JMX console (use the <b>Discovery Scheduler</b> MBean).</li></ul></li></ul>

## Probe Manager Logs

<b>probeMgr-performance.log</b>	<p>Performance statistics dump, collected every predefined period of time, which includes memory information and thread pool statuses.</p>
---------------------------------	--

	<ul style="list-style-type: none"> <li>• <b>Levels:</b> <ul style="list-style-type: none"> <li>◦ <b>Error.</b> N/A</li> <li>◦ <b>Information.</b> N/A</li> <li>◦ <b>Debug.</b> N/A</li> </ul> </li> <li>• <b>Basic Troubleshooting:</b> <ul style="list-style-type: none"> <li>◦ Check this log to investigate memory issues over time.</li> <li>◦ The statistics are logged every 1 minute, by default.</li> </ul> </li> </ul>
<b>probeMgr-adaptersDebug.log</b>	Contains messages that are created following a job execution.

## Discovery Rules Engine Log Files

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



## TQL Parameter Logs

This section contains definitions for TQL parameter log files.

This section includes the following topics:

- ["Pattern Statistics Log" below](#)
- ["Audit Short/Detailed Log \(TQL Perspective\)" on the next page](#)
- ["Incremental Statistics Log" on the next page](#)
- ["Incremental Splitter Log" on page 43](#)
- ["Incremental Detailed Log" on page 43](#)

## Pattern Statistics Log

The log name is **cmdb.pattern.statistics.log**.

Log File	Description
Purpose	General calculation data for each TQL query, updated at predefined intervals.
Information Level	The following information is given for each TQL query: <ul style="list-style-type: none"><li>• name</li><li>• average, minimum, and maximum calculation times</li><li>• number of calculations</li><li>• last calculation time</li><li>• result size</li></ul>
Error Level	Not available.
Debug Level	Not available.
Basic Troubleshooting	<ul style="list-style-type: none"><li>• Verify that a specific TQL query was updated.</li><li>• Evaluate a TQL query's calculation time.</li><li>• Evaluate a TQL query's result size.</li></ul>

## Audit Short/Detailed Log (TQL Perspective)

The log name is **cmdb.audit.short.log**.

Log File	Description
Purpose	CMDB state changes, CI Type changes, and TQL query results. You can use this log to follow the results of TQL queries.
Information Level	Not available.
Error Level	Not available.
Debug Level	<ul style="list-style-type: none"><li>Final calculation for TQL queries is logged.</li><li>If the final TQL query calculation is unchanged from the previous calculation, this is noted.</li><li>If the final TQL query calculation is changed from the previous calculation, results of the CIs and relationships are recorded in the detailed log. The number of CIs and relationships are recorded in the short log.</li></ul>
Basic Troubleshooting	<ul style="list-style-type: none"><li>Use this log to verify which notifications are published by the TQL query subsystem.</li><li>Check the section at the end of each result. This section includes added, removed, and updated CIs and relationships.</li><li>Track the CIT changes and see if the query results also change. You can thus correlate the CIT changes to the results of the query calculations.</li></ul>

## Incremental Statistics Log

The log name is **cmdb.incremental.statistics.log**.

Log File	Description
Purpose	Traces the calculation procedure, full or incremental, of every query.
Information Level	Not available.
Error Level	Not available.

Log File	Description
Debug Level	<ul style="list-style-type: none"><li>• Gives the date, time, query name, and whether an incremental statistic calculation was performed (yes/no).</li><li>• If an incremental statistic calculation was not performed, states the reason, the number of subcalculations (relevant for incremental calculations only), and the complete calculation time.</li></ul>
Basic Troubleshooting	<p>Monitors the calculation process.</p> <p>If a specific query calculation takes a long time, check if it is a full or incremental calculation:</p> <ul style="list-style-type: none"><li>• If full, check whether a full calculation is necessary.</li><li>• If incremental, check how many subcalculations have been performed.</li></ul>

## Incremental Splitter Log

The log name is **cmdb.incremental.splitter.log**.

Log File	Description
Purpose	Monitors the incremental splitter result made during an incremental calculation.
Information Level	Not available.
Error Level	Not available.
Debug Level	Gives the set of query node numbers of each query graph created by the incremental splitter.
Basic Troubleshooting	If the TQL result calculated by the incremental calculator is wrong, verify that the splitter result is correct.

## Incremental Detailed Log

The log name is **cmdb.incremental.detailed.log**.

Log File	Description
Purpose	Monitors the incremental calculation process.
Information Level	Not available.

Log File	Description
Error Level	Not available.
Debug Level	Each incremental subcalculation entry includes the following: <ul style="list-style-type: none"><li>• the trigger query node</li><li>• the number of elements classified to the trigger query node</li><li>• whether the subcalculation step is driven by new elements added to the model or by existing elements</li><li>• the calculated query graph</li></ul>
Basic Troubleshooting	Follows the basic steps of an incremental calculation.

## How to Troubleshoot and Debug Using Generic Adapter Log Files

For troubleshooting and debugging, use the following:

- Adjust logging levels in these files (set the *log/level* variable to TRACE for the most detailed results):
  - **<UCMDB\_DataFlowProbe>\conf\log\fcmdb.push.properties**  
**<UCMDB\_DataFlowProbe>** is the UCMDB Data Flow Probe installation directory.
  - **<UCMDB\_Server>\conf\log\reconciliation.properties**  
**<UCMDB\_Server>** is the UCMDB Server installation directory.
- Analyze the following Generic Adapter log files by considering the following three scenarios:
  - If **integration.log.mode=0**, that is, all the log messages are included in **fcmdb.push.all.log**, analyze the following log files:
    - **<UCMDB\_DataFlowProbe>\runtime\log\fcmdb.push.all.log**
    - **<UCMDB\_DataFlowProbe>\runtime\log\fcmdb.push.configuration.log**
    - **<UCMDB\_DataFlowProbe>\runtime\log\fcmdb.push.connector.all.log**
    - **<UCMDB\_DataFlowProbe>\runtime\log\fcmdb.push.connector.configuration.log**
    - **<UCMDB\_DataFlowProbe>\runtime\log\fcmdb.push.mapping.log**
  - If **integration.log.mode=1**, that is, both **fcmdb.push.all.log** and separate log files based on

integration point names are generated, analyze the following log files:

- <UCMDB\_DataFlowProbe>\runtime\log\fcmdb.push.all.log
  - <UCMDB\_DataFlowProbe>\runtime\log\fcmdb.push.configuration.log
  - <UCMDB\_DataFlowProbe>\runtime\log\fcmdb.push.connector.all.log
  - <UCMDB\_DataFlowProbe>\runtime\log\fcmdb.push.connector.configuration.log
  - <UCMDB\_DataFlowProbe>\runtime\log\fcmdb.push.mapping.log
  - <UCMDB\_DataFlowProbe>\runtime\log\fcmdb.push.<integrationPointName>.log
  - <UCMDB\_DataFlowProbe>\runtime\log\fcmdb.push.<integrationPointName>.configuration.log
  - <UCMDB\_DataFlowProbe>\runtime\log\fcmdb.push.<integrationPointName>.connector.all.log
  - <UCMDB\_DataFlowProbe>\runtime\log\fcmdb.push.<integrationPointName>.connector.configuration.log
  - <UCMDB\_DataFlowProbe>\runtime\log\fcmdb.push.<integrationPointName>.mapping.log
- If **integration.log.mode=2**, that is, only separate log files based on integration point names are generated, analyze the following log files:
    - <UCMDB\_DataFlowProbe>\runtime\log\fcmdb.<integrationPointName>.log
    - <UCMDB\_DataFlowProbe>\runtime\log\fcmdb.<integrationPointName>.configuration.log
    - <UCMDB\_DataFlowProbe>\runtime\log\fcmdb.<integrationPointName>.connector.all.log
    - <UCMDB\_DataFlowProbe>\runtime\log\fcmdb.<integrationPointName>.connector.configuration.log
    - <UCMDB\_DataFlowProbe>\runtime\log\fcmdb.<integrationPointName>.mapping.log
- Analyze the following generic log files:
    - <UCMDB\_DataFlowProbe>\runtime\log\probe-error.log
    - <UCMDB\_DataFlowProbe>\runtime\log\WrapperProbeGw.log
    - <UCMDB\_Server>\runtime\log\error.log
    - <UCMDB\_Server>\runtime\log\cmdb.reconciliation.log

**Related information:**

["How to Generate Separate Generic Adapter Log Files" on page 1](#)

## Chapter 3: Troubleshooting Deployment

This chapter includes:

Troubleshooting Deployment - UCMDB Server .....	47
Troubleshoot UCMDB in Non-English Locales .....	48
Troubleshooting Deployment - Keystore and Truststore .....	50
Troubleshooting Keystore and Truststore - Non-FIPS mode .....	50
Troubleshooting Keystore and Truststore - FIPS mode .....	56
Troubleshooting Deployment - Configuration Manager .....	59
Configuration Manager General Limitations and Troubleshooting .....	59
Configuration Manager Upgrade .....	60
Logging In to Configuration Manager .....	60
Configuration Manager Authentications .....	63
Troubleshooting Deployment - Data Flow Probe .....	63
Troubleshooting Probe Upgrade .....	65

### Troubleshooting Deployment - UCMDB Server

**Problem:** The UCMDB Server does not start automatically upon system restart.

**Solution:**

1. Open the Windows Services dialog box and select the **UCMDB\_Server** service.
2. Open the UCMDB\_Server Properties (Local Computer) dialog box.
3. In the **General** tab, ensure that:
  - **The Path to executable** field points to the correct executable location.
  - The service is configured to automatically start (Startup type is **Automatic**).
4. In the **Log On** tab, ensure that the service uses the correct user for logon. For details on changing the service user, see the [HardeningHardening](#) section of the UCMDB Help.
5. In the **Dependencies** tab, ensure that the service is configured to have no dependencies (**<No Dependencies>**).

# Troubleshoot UCMDB in Non-English Locales

## Installation and Deployment Issues

- If you use the Japanese, Chinese, or Korean language in your browser, you must ensure that the Universal CMDB server has East Asian languages installed. On the machine on which the Universal CMDB server is installed, you must select **Control Panel > Regional and Language Options > Languages > Install files for East Asian languages**.
- Universal CMDB in an I18N environment is supported for Universal CMDB installed on a Windows or Linux platform.
- The installation path for all Universal CMDB components must not contain non-English language characters.
- The Upgrade Wizard for version 2018.08 does not support the non-English user interface. (The upgrade itself works properly.)

## Database Environment Issues

- To work in a non-English language Universal CMDB environment, you can use either an Oracle Server database, Microsoft SQL Server database, or PostgreSQL Server database. The OS Windows regional settings language of the database should be the same as that of the UCMDB Server. When using an Oracle Server database, the encoding of the database can also be UTF-8 or AL32UTF-8, which supports both non-English languages as well as multiple languages.
- When you create a new Oracle instance in an Oracle database, you must specify the character set for the instance. All character data, including data in the data dictionary, is stored in the instance's character set. For details, see the section describing the Oracle Summary Checklist in the [DatabaseDatabase](#) section of the UCMDB Help.
- The Database Query Monitor can connect to an Oracle database, but the Oracle user names and passwords must contain only English characters.

## Multi-Lingual User (MLU) Interface Support

Use the language preference option in your browser to select how to view Universal CMDB. The language preference chosen affects only your local machine (the client machine) and not the Universal CMDB Server machine or any other user accessing the same Universal CMDB machine.



The Universal CMDB user interface can be viewed in the following languages in your Web browser:

✓	English	✓	Korean
✓	French	✓	Brazilian Portuguese
✓	German	✓	Russian
✓	Italian	✓	Simplified Chinese
✓	Japanese	✓	Spanish

**To set up and view Universal CMDB in a specific language:**

1. Install the appropriate language's fonts on your local machine if they are not yet installed. If you choose a language in your Web browser whose fonts have not been installed, Universal CMDB displays the characters as squares.
2. If you are logged in to Universal CMDB, you must log out. Click **LOGOUT** at the top of the Universal CMDB window.

Close every open browser window or, alternatively, clear the cache.

3. If Universal CMDB is running on Internet Explorer, configure the Web browser on your local machine to select the language in which you want to view Universal CMDB (**Tools > Internet Options**).
  - a. Click the **Languages** button and in the Language Preference dialog box, highlight the language in which you want to view Universal CMDB.
  - b. If the language you want is not listed in the dialog box, click **Add** to display the list of languages. Select the language you want to add and click **OK**.
  - c. Click **Move Up** to move the selected language to the first row.
  - d. Click **OK** to save the settings.
  - e. Display the Universal CMDB login window.
  - f. From the Internet Explorer menu, select **View > Refresh**. Universal CMDB immediately refreshes and the user interface is displayed in the selected language.

**Note:** For details on viewing Web pages in Internet Explorer that are written in a different language, see <http://support.microsoft.com/kb/306872/en-us>.

# Troubleshooting Deployment - Keystore and Truststore

## Troubleshooting Keystore and Truststore - Non-FIPS mode

**Problem:** UCMDB server startup failed, and the **startup.log** shows message similar to the following:

```
2017-05-04 08:32:17,074 ERROR [WrapperSimpleAppMain] (JettyManager.java:247) -
Failure starting jetty server
MultiException[java.io.IOException: Keystore was tampered with, or password was
incorrect, java.io.IOException: Keystore was tampered with, or password was
incorrect]
    at org.eclipse.jetty.server.Server.doStart(Server.java:329)
    at org.eclipse.jetty.util.component.AbstractLifeCycle.start
(AbstractLifeCycle.java:68)
    at com.mercury.topaz.cmdb.server.manage.servlet.JettyManager.startServer
(JettyManager.java:243)
    at com.mercury.topaz.cmdb.server.manage.Framework.doStart0(Framework.java:242)
    at com.mercury.topaz.cmdb.server.manage.Framework.access$100
(Framework.java:102)
    at com.mercury.topaz.cmdb.server.manage.Framework$2.executeInContext
(Framework.java:221)
    at com.mercury.topaz.cmdb.server.manage.Framework$2.executeInContext
(Framework.java:218)
    at
com.mercury.topaz.cmdb.shared.manage.AuthorizationContextUtils.executeInSystemAu
thorizationContext(AuthorizationContextUtils.java:24)
    at com.mercury.topaz.cmdb.server.manage.Framework.start0(Framework.java:218)
    at com.mercury.topaz.cmdb.server.manage.Framework.doStartUp(Framework.java:204)
    at com.mercury.topaz.cmdb.server.manage.Framework.access$000
(Framework.java:102)
    at com.mercury.topaz.cmdb.server.manage.Framework$1.executeInContext
(Framework.java:186)
    at com.mercury.topaz.cmdb.server.manage.Framework$1.executeInContext
(Framework.java:183)
    at
com.mercury.topaz.cmdb.shared.manage.AuthorizationContextUtils.executeInSystemAu
thorizationContext(AuthorizationContextUtils.java:24)
    at com.mercury.topaz.cmdb.server.manage.Framework.startUp(Framework.java:183)
```

```
at com.hp.ucmdb.server.Main.startFramework(Main.java:34)
at com.hp.ucmdb.server.Main.main(Main.java:23)
at sun.reflect.NativeMethodAccessorImpl.invoke0(Native Method)
at sun.reflect.NativeMethodAccessorImpl.invoke
(NativeMethodAccessorImpl.java:62)
at sun.reflect.DelegatingMethodAccessorImpl.invoke
(DelegatingMethodAccessorImpl.java:43)
at java.lang.reflect.Method.invoke(Method.java:498)
at org.tanukisoftware.wrapper.WrapperSimpleApp.run(WrapperSimpleApp.java:325)
at java.lang.Thread.run(Thread.java:745)
```

### **Solution A:**

Check the **verify\_store\_pass.log** (in the **C:\UCMDB\UCMDBServer\runtime\log** folder), if you see the following message:

INFO: server-storepass.conf file exists and it contains keystore and truststore.

Do the following:

1. Stop the UCMDB Server.
2. Run commands.
  - a. Check keystore password.

#### **Windows:**

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

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

#### **Linux:**

From **/opt/UCMDB/UCMDBServer/bin/jre/bin**, run the following commands:

```
./keytool -list -keystore
/opt/UCMDB/UCMDBServer/conf/security/server.keystore
```

Enter the password that you set up during the installation of UCMDB server. If you see the following message:

```
keytool error: java.io.IOException:Keystore was tampered with, or password
was incorrect.
```

Then the password was not properly set, and you need to change keystore and truststore passwords using keytool.

- b. Change the store password:

**Windows:**

```
keytool -storepasswd -new <new_keystore_pass> -keystore  
C:\UCMDB\UCMDBServer\conf\security\server.keystore -storepass <current_  
keystore_pass>
```

**Linux:**

```
./keytool -storepasswd -new <new_keystore_pass> -keystore  
/opt/UCMDB/UCMDBServer/conf/security/server.keystore -storepass  
<current_keystore_pass>
```

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

**Windows:**

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

**Linux:**

```
./keytool -keypasswd -alias <alias> -keypass <currentPass> -new  
<newPass> -keystore /opt/UCMDB/UCMDBServer/conf/security/server.keystore
```

- d. Change the trust store password:

**Windows:**

```
keytool -storepasswd -new <new_truststore_pass> -keystore  
C:\UCMDB\UCMDBServer\conf\security\server.truststore -storepass  
<current_truststore_pass>
```

**Linux:**

```
./keytool -storepasswd -new <new_truststore_pass> -keystore  
/opt/UCMDB/UCMDBServer/conf/security/server.truststore -storepass  
<current_truststore_pass>
```

3. Start the UCMDB Server service.

**Solution B:**

Check the **verify\_store\_pass.log**, if you see the following message:

INFO: keystore password and truststore password don't exist.

Or the following:

INFO: server-storepass.conf file doesn't exist.

Do the following:

1. Generate the **server-storepass.conf** file.

**Windows:**

From the **C:\UCMDB\UCMDBServer\bin** folder, run the following command:

```
key-truststore.bat <fips_mode> <new_keystore_pass> <new_truststore_pass>
```

**Linux:**

From the **/opt/UCMDB/UCMDBServer/bin** folder, run the following command:

```
./key-truststore.sh <fips_mode> <new_keystore_pass> <new_truststore_pass>
```

where <fips\_mode> can be only set to **true** or **false**. For non-FIPS mode UCMDB server, **false** for <fips\_mode>.

2. Stop the UCMDB Server.
3. Change keystore password and truststore password with keytool.

From the **C:\UCMDB\UCMDBServer\bin\jre\bin** (Windows) or **/opt/UCMDB/UCMDBServer/bin/jre/bin** (Linux) folder, run the following commands:

- a. Change the store password:

**Windows:**

```
keytool -storepasswd -new <new_keystore_pass> -keystore  
C:\UCMDB\UCMDBServer\conf\security\server.keystore -storepass <current_  
keystore_pass>
```

**Linux:**

```
./keytool -storepasswd -new <new_keystore_pass> -keystore  
/opt/UCMDB/UCMDBServer/conf/security/server.keystore -storepass  
<current_keystore_pass>
```

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

**Windows:**

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

**Linux:**

```
./keytool -keypasswd -alias <alias> -keypass <currentPass> -new  
<newPass> -keystore /opt/UCMDB/UCMDBServer/conf/security/server.keystore
```

- c. Change the trust store password:

**Windows:**

```
keytool -storepasswd -new <new_truststore_pass> -keystore  
C:\UCMDB\UCMDBServer\conf\security\server.truststore -storepass  
<current_truststore_pass>
```

**Linux:**

```
./keytool -storepasswd -new <new_truststore_pass> -keystore  
/opt/UCMDB/UCMDBServer/conf/security/server.truststore -storepass  
<current_truststore_pass>
```

4. Start the UCMDB Server service.

**Solution C:**

If you only changed keystore password or truststore password during UCMDB server installation, and then server startup failed and the **startup.log** shows similar error messages as shown above. You can follow the instructions provided in Solution A or Solution B, but you need to change the keystore password or truststore password that you set during installation.

For example, if you only changed truststore password during installation and you need to generate **server-storepass.conf**, run the following command:

**Windows:** key-truststore.bat <fips\_mode> null <new\_truststore\_pass>

**Linux:** ./key-truststore.sh <fips\_mode> null <new\_truststore\_pass>

**Problem:** You have changed schema in UCMDB Server. The server startup failed and the **startup.log** shows the following message:

```
2017-05-04 08:32:17,074 ERROR [WrapperSimpleAppMain] (JettyManager.java:247) -  
Failure starting jetty server  
MultiException[java.io.IOException: Keystore was tampered with, or password was  
incorrect, java.io.IOException: Keystore was tampered with, or password was  
incorrect]  
    at org.eclipse.jetty.server.Server.doStart(Server.java:329)  
    at org.eclipse.jetty.util.component.AbstractLifeCycle.start  
(AbstractLifeCycle.java:68)  
    at com.mercury.topaz.cmdb.server.manage.servlet.JettyManager.startServer
```

```
(JettyManager.java:243)
    at com.mercury.topaz.cmdb.server.manage.Framework.doStart0(Framework.java:242)
    at com.mercury.topaz.cmdb.server.manage.Framework.access$100
(Framework.java:102)
    at com.mercury.topaz.cmdb.server.manage.Framework$2.executeInContext
(Framework.java:221)
    at com.mercury.topaz.cmdb.server.manage.Framework$2.executeInContext
(Framework.java:218)
    at
com.mercury.topaz.cmdb.shared.manage.AuthorizationContextUtils.executeInSystemAu
thorizationContext(AuthorizationContextUtils.java:24)
    at com.mercury.topaz.cmdb.server.manage.Framework.start0(Framework.java:218)
    at com.mercury.topaz.cmdb.server.manage.Framework.doStartUp(Framework.java:204)
    at com.mercury.topaz.cmdb.server.manage.Framework.access$000
(Framework.java:102)
    at com.mercury.topaz.cmdb.server.manage.Framework$1.executeInContext
(Framework.java:186)
    at com.mercury.topaz.cmdb.server.manage.Framework$1.executeInContext
(Framework.java:183)
    at
com.mercury.topaz.cmdb.shared.manage.AuthorizationContextUtils.executeInSystemAu
thorizationContext(AuthorizationContextUtils.java:24)
    at com.mercury.topaz.cmdb.server.manage.Framework.startUp(Framework.java:183)
    at com.hp.ucmdb.server.Main.startFramework(Main.java:34)
    at com.hp.ucmdb.server.Main.main(Main.java:23)
    at sun.reflect.NativeMethodAccessorImpl.invoke0(Native Method)
    at sun.reflect.NativeMethodAccessorImpl.invoke
(NativeMethodAccessorImpl.java:62)
    at sun.reflect.DelegatingMethodAccessorImpl.invoke
(DelegatingMethodAccessorImpl.java:43)
    at java.lang.reflect.Method.invoke(Method.java:498)
    at org.tanukisoftware.wrapper.WrapperSimpleApp.run(WrapperSimpleApp.java:325)
    at java.lang.Thread.run(Thread.java:745)
```

**Solution:** You need to re-generate **server-storepass.conf**, because the new schema does not store any keystore and truststore passwords.

- If you remember what passwords were specified previously, you can generate the **server-storepass.conf** file with the following command:

```
Windows: key-truststore.bat <fips_mode> <new_keystore_pass> <new_truststore_
pass>

Linux: ./key-truststore.sh <fips_mode> <new_keystore_pass> <new_truststore_
pass>
```

where `<fips_mode>` can be only set to **true** or **false**. For non-FIPS mode UCMDb server, **false** for `<fips_mode>`.

- If you don't remember the passwords, follow the instructions in [Solution B](#) to regenerate the passwords.

## Troubleshooting Keystore and Truststore - FIPS mode

**Problem:** If starting the UCMDb server failed, and the **startup.log** shows message similar to the following:

```
2017-05-04 08:32:17,074 ERROR [WrapperSimpleAppMain] (JettyManager.java:247) -
Failure starting jetty server
MultiException[java.io.IOException: Keystore was tampered with, or password was
incorrect, java.io.IOException: Keystore was tampered with, or password was
incorrect]
    at org.eclipse.jetty.server.Server.doStart(Server.java:329)
    at org.eclipse.jetty.util.component.AbstractLifeCycle.start
(AbstractLifeCycle.java:68)
    at com.mercury.topaz.cmdb.server.manage.servlet.JettyManager.startServer
(JettyManager.java:243)
    at com.mercury.topaz.cmdb.server.manage.Framework.doStart0(Framework.java:242)
    at com.mercury.topaz.cmdb.server.manage.Framework.access$100
(Framework.java:102)
    at com.mercury.topaz.cmdb.server.manage.Framework$2.executeInContext
(Framework.java:221)
    at com.mercury.topaz.cmdb.server.manage.Framework$2.executeInContext
(Framework.java:218)
    at
com.mercury.topaz.cmdb.shared.manage.AuthorizationContextUtils.executeInSystemAu
thorizationContext(AuthorizationContextUtils.java:24)
    at com.mercury.topaz.cmdb.server.manage.Framework.start0(Framework.java:218)
    at com.mercury.topaz.cmdb.server.manage.Framework.doStartUp(Framework.java:204)
    at com.mercury.topaz.cmdb.server.manage.Framework.access$000
(Framework.java:102)
    at com.mercury.topaz.cmdb.server.manage.Framework$1.executeInContext
(Framework.java:186)
    at com.mercury.topaz.cmdb.server.manage.Framework$1.executeInContext
(Framework.java:183)
    at
```



```
com.mercury.topaz.cmdb.shared.manage.AuthorizationContextUtils.executeInSystemAu  
thorizationContext(AuthorizationContextUtils.java:24)  
    at com.mercury.topaz.cmdb.server.manage.Framework.startUp(Framework.java:183)  
    at com.hp.ucmdb.server.Main.startFramework(Main.java:34)  
    at com.hp.ucmdb.server.Main.main(Main.java:23)  
    at sun.reflect.NativeMethodAccessorImpl.invoke0(Native Method)  
    at sun.reflect.NativeMethodAccessorImpl.invoke  
(NativeMethodAccessorImpl.java:62)  
    at sun.reflect.DelegatingMethodAccessorImpl.invoke  
(DelegatingMethodAccessorImpl.java:43)  
    at java.lang.reflect.Method.invoke(Method.java:498)  
    at org.tanukisoftware.wrapper.WrapperSimpleApp.run(WrapperSimpleApp.java:325)  
    at java.lang.Thread.run(Thread.java:745)
```

#### **Solution A:**

Check the **verify\_store\_pass.log**, if you see the following message:

INFO: server-storepass.conf file exists and it contains keystore and truststore.

Do the following:

1. Change the keystore and truststore passwords using keytool.

For detailed instructions, see the "Generate a new self-signed certificate (hpcert) and sign it with the default UCMDB root certificate (hproot)" "Generate a new self-signed certificate (hpcert) and sign it with the default UCMDB root certificate (hproot)" section in the [Universal CMDB FIPS Deployment Guide](#) (page 19).

2. Start the UCMDB Server service.

#### **Solution B:**

Check the **verify\_store\_pass.log**, if you see the following message:

INFO: keystore password and truststore password don't exist.

Or the following:

INFO: server-storepass.conf file doesn't exist.

Do the following:

1. Make sure you have stopped the UCMDB Server.
2. Generate the **server-storepass.conf** file.

#### **Windows:**

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

```
key-truststore.bat <fips_mode> <new_keystore_pass> <new_truststore_pass>
```

**Linux:**

From **opt/UCMDB/UCMDBServer/bin/jre/bin**, run the following command:

```
./key-truststore.sh <fips_mode> <new_keystore_pass> <new_truststore_pass>
```

where <fips\_mode> can be only set to **true** or **false**. For FIPS mode UCMDB server, **true** for <fips\_mode>.

3. Change the keystore and truststore passwords using keytool.

For detailed instructions, see the "Generate a new self-signed certificate (hpcert) and sign it with the default UCMDB root certificate (hproot)" "Generate a new self-signed certificate (hpcert) and sign it with the default UCMDB root certificate (hproot)" section in the [Universal CMDB FIPS Deployment Guide](#) (page 19).

4. Start the UCMDB Server service.

**Solution C:**

If you only changed keystore password or truststore password during UCMDB server installation, and then server startup failed and the **startup.log** shows similar error messages as shown above. You can follow the instructions provided in Solution A or Solution B, but you need to change the keystore password or truststore password that you set during installation.

For example, if you only changed truststore password during installation and you need to generate **server-storepass.conf**, run the following command:

**Windows:** key-truststore.bat <fips\_mode> null <new\_truststore\_pass>

**Linux:** ./key-truststore.sh <fips\_mode> null <new\_truststore\_pass>

# Troubleshooting Deployment - Configuration Manager

## Configuration Manager General Limitations and Troubleshooting

### Limitations

- The time settings on the UCMDB and Configuration Manager servers must be synchronized, down to the seconds.
- The time zone and time format on the UCMDB and Service Manager servers must be synchronized.
- You will not see a new CI type that you created in UCMDB until you log out of Configuration Manager and then log on again.
- Whenever the time is changed on the Configuration Manager Tomcat server, the server must be restarted to update the time on the server.

### Troubleshooting

**Problem.** When you start the Configuration Manager service, you receive the following error message:

Windows could not start the Universal CMDB Configuration Manager on Local Computer. For more information, review the System Manager Event log. If this is a non-Microsoft service, contact the service vendor, and refer to service-specific error code 0.

**Solution.** Do the following:

1. Go to the **<Configuration\_Manager\_installation\_directory>\cnc\bin** folder and execute the following command:  
  
`edit-server-0.bat`
2. Select the Startup tab. In the Mode drop-down list (at the bottom), select **jvm** instead of **exe**.
3. Click **OK**.
4. Run your service.

## Configuration Manager Upgrade

**Problem.** The upgrade to version 2018.08 fails.

**Solution:** To restore to the previous version, perform the following steps:

- Uninstall Configuration Manager version 2018.08.
- Restore the installation folder for the previous version of Configuration Manager (that you backed up before upgrading) to its original location.
- Restore the database (that you backed up before upgrading).
- Import the Windows registry entry (that you backed up before upgrading).

## Logging In to Configuration Manager

**Problem.** You have been assigned the appropriate permissions for Configuration Manager but you are not able to log in.

**Solution.** Verify that the following parameters are configured correctly in UCMDB:

- LW-SSO init string: This string must not be empty.
- LW-SSO domain: Must be set to the same domain as UCMDB.
- LW-SSO trusted DNS domains: The Configuration Manager domain must be listed here, even if it is the same as the UCMDB domain.

**Problem.** There is an error in the UCMDB connection.

**Solution.** One of the following may be the cause:

- The UCMDB server is down. Restart Configuration Manager after UCMDB is fully up (verify that the UCMDB server status is **Up**).
- The UCMDB server is up but the Configuration Manager connection credentials or URL is wrong.

**Problem.** After changing UCMDB connection settings (such as changes to: host/port/protocol/SRP), the Configuration Manager server fails to start.

**Solution.** Reconfigure Configuration Manager and specify the UCMDB connection settings that reflect your latest changes. The reconfiguration wizard (**CM\_2018.08.exe**) is located in the **<Configuration\_Manager\_installation\_directory>\\_installation** folder.

**Problem.** Changes to the UCMDB class model are not detected in Configuration Manager.

**Solution.** Restart the Configuration Manager server.

**Problem.** The Configuration Manager log contains a **UCMDBExecution timeout expired** error.

**Solution.** This occurs when the UCMDB database is overloaded. To correct this, increase the connection timeout as follows:

1. Create a **jdbc.properties** file in the **UCMDBServer\conf** folder.
2. Enter the following text: `QueryTimeout=<number in seconds>`.
3. Restart the UCMDB server.

**Problem.** Configuration Manager does not allow you to add a view to be managed.

**Solution.** When a view is added to be managed, a new TQL is created in UCMDB. If the maximum limit of active TQLs is reached, the view cannot be added. Increase the limit of active TQLs in UCMDB by changing the following settings in the Infrastructure Settings Manager:

- Max Number Of Active TQLs In Server
- Max Number Of Customer Active TQLs

**Problem.** The HTTPS Server certificate is not valid.

**Solution.** One of the following may be the cause:

- The validation date of the certificate has passed. You need to get a new certificate.
- The certification authority on the certificate is not a trusted authority. Add the certification authority to your Trusted Root Certification Authority list.

**Problem.** When logging in from the Configuration Manager login page, you get a login error or access denied page.

**Solution.** Check that the LW-SSO settings are correct. For details, see the general LW-SSO reference in the [HardeningHardening](#) section of the UCMDB Help.

**Problem.** The Configuration Manager server does not start due to entering incorrect database credentials.

**Solution.** If you made a change to the database credentials and the server fails to start, the credentials may be wrong. You need to re-encrypt the database password and enter new credentials in the configuration file. Proceed as follows:

1. From a command line, run the following command to encrypt the updated database password:

```
<Configuration_Manager_installation_directory>\bin\encrypt-password.bat -p  
<password>
```

which returns an encrypted password.

2. Copy the encrypted password (including the {ENCRYPTED} prefix), into the **db.password** parameter in the **<Configuration\_Manager\_installation\_directory>\conf\database.properties** file.

**Problem.** The Configuration Manager Tomcat server does not start due to a bind port issue.

**Solution.** Try one of the following:

- Run the Post install wizard and replace the Configuration Manager server ports.
- Abort the other process that occupies the Configuration Manager ports.
- Manually change the ports in Configuration Manager configuration files by editing the following file:  
**<Configuration Manager installation directory>\servers\server-0\conf\server.xml** and updating the relevant ports:
  - HTTP (8180): line 69
  - HTTPS (8143): lines 71, 90

**Problem.** You receive an "out of memory" message.

**Solution.** Do the following to change the server startup parameters:

1. Run the following batch file:

```
<Configuration Manager installation directory>/bin/edit-server-0.bat
```

2. Change the following settings:

```
-Dapplication.ms=<initial memory pool size>
```

```
-Dapplication.mx=<maximum memory pool size>
```

**Problem.** Changes in CIs in UCMDB are not reflected in Configuration Manager.

**Solution.** Configuration Manager runs an offline asynchronous analysis process. The process may not yet have processed the latest changes in UCMDB. To resolve this, try one of the following:

- Wait a few minutes. The default interval between analysis process executions is 10 minutes. It is configurable in **Administration > Settings**.
- Execute a JMX call to run the offline analysis calculation on the relevant view.
- In **Policies**, click the **Recalculate Policy Analysis** button. This invokes the offline analysis process for all views (which may take some time). You may also need to make an artificial change to one policy and save it.

## Configuration Manager Authentications

**Problem.** During authentication of Configuration Manager after redirection to the UCMDB login page, you are not redirected back to Configuration Manager but UCMDB opens instead.

**Solution.** The Configuration Manager authentication session cookie is blocked or denied when using Internet Explorer browser. Add the Configuration Manager server to the Intranet/Trusted zone in the Internet Explorer security zones on your computer (**Tools > Internet Options > Security > Local Intranet > Sites > Advanced**). This allows all cookies to be accepted.

**Solution.** Make sure that the LW-SSO configuration in UCMDB settings is correct. For details, see the section about LW-SSO in the [HardeningHardening](#) section of the UCMDB Help.

**Possible solution.** Make sure that you access the application with the Fully Qualified Domain Name (FQDN) in the login URL (for example: **http://myserver.companydomain.com/WebApp**).

## Troubleshooting Deployment - Data Flow Probe

### Probe Downgrade or Rollback

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

### Probe Restart

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

## How to Change the PostgreSQL Database Default Port

To change the port for the PostgreSQL database, that is defined by default in the Data Flow Probe installation:

1. Stop the Probe (if already started).
2. Stop the UCMDB Probe DB Service.
3. Modify the port in the following file:

The following shows how to change the port from **5432** to **5433**:

**Note:** If two probes coexist on the same machine, plan the port usage carefully so that the ports used by the two probes do not conflict.

```
#port = 5432 # (change requires restart) < Old line  
port = 5433 # (change requires restart) < New line
```

4. Make the following changes in the **DataFlowProbe.properties** file (in **C:\UCMDB\DataFlowProbe\conf** on Windows, and **/opt/UCMDB/DataFlowProbe/conf** on Linux):

- Change:

```
jdbc:postgresql://localhost/dataflowprobe
```

to

```
jdbc:postgresql://localhost:5433/dataflowprobe
```

- Change:

```
appilog.agent.local.jdbc.uri = jdbc:postgresql://localhost/dataflowprobe
```

to

```
appilog.agent.local.jdbc.uri =  
jdbc:postgresql://localhost:5433/dataflowprobe
```

- Change:

```
appilog.agent.normalization.jdbc.uri =  
jdbc:postgresql://localhost/dataflowprobe
```

to



```
appilog.agent.normalization.jdbc.uri =  
jdbc:postgresql://localhost:5433/dataflowprobe
```

- Change:

```
appilog.agent.netflow.jdbc.uri =  
jdbc:postgresql://localhost/dataflowprobe
```

to

```
appilog.agent.netflow.jdbc.uri =  
jdbc:postgresql://localhost:5433/dataflowprobe
```

## Troubleshooting Probe Upgrade

- [Troubleshooting Probe Upgrade - Permission Check](#)
- [Troubleshooting Probe Upgrade - How to check if a probe is upgraded successfully?](#)
- [Troubleshooting Probe Upgrade - General Known Issues, Limitations, and Others](#)
- [Troubleshooting Probe Upgrade - PostgreSQL Upgrade](#)
- [Troubleshooting Probe Upgrade - Customized Probe Configuration](#)

## Troubleshooting Probe Upgrade - Permission Check

**Problem:** When logged in using a different user, the probe auto upgrade fails. (From the **probe\_auto\_upgrade.log**, you may see a message "Failed to start probe service".)

**Solution:** Check your environment to make sure it meets the following requirements:

- If you are using a system default user account (for example, **administrator** or **admin**), make sure you grant the user the full control the **<DataFlowProbe>** folder permissions. For details, see ["Grant the <DataFlowProbe> folder permissions " on page 67](#).
- if you are using a custom account, make sure the custom account meet the following requirements:
  - a. The user running the Probe service must be a member of the **Administrators** group.

- b. If the **UCMDB\_Probe** and the **UCMDB\_Probe\_DB** services run under a custom account, make sure you grant the user the full control the **<DataFlowProbe>** folder permissions before the probe auto upgrade starts, and revert the control after the upgrade.
- c. Run one of the following commands using the custom account:

- `net stop UCMDB_Probe`
- `net stop UCMDB_Probe_DB`
- `net start UCMDB_Probe`
- `net start UCMDB_Probe_DB`

If any of the above commands fails, you need to do the following to grant the custom account the required permissions:

- Grant the custom users the permission to start/stop the probe services.

**Note:** The steps below use the **UCMDB\_Probe** service as an example. You should also apply the same steps for the **UCMDB\_Probe\_DB** and **UCMDB\_Probe\_XmlEnricher** services.

- A. Locate the Command Prompt tool (**cmd.exe**), right-click and select **Run as administrator**.
- B. Get the current permission for the **UCMDB\_Probe** service by running the following command:

```
sc sdshow UCMDB_Probe
```

The returned result is as follows: (You may want to note down this string)

```
D: (A;;CCLCSWRPWPDTLOCRRC;;;SY) (A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)
(A;;CCLCSWLOCRRC;;;IU) (A;;CCLCSWLOCRRC;;;SU) S:
(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)
```

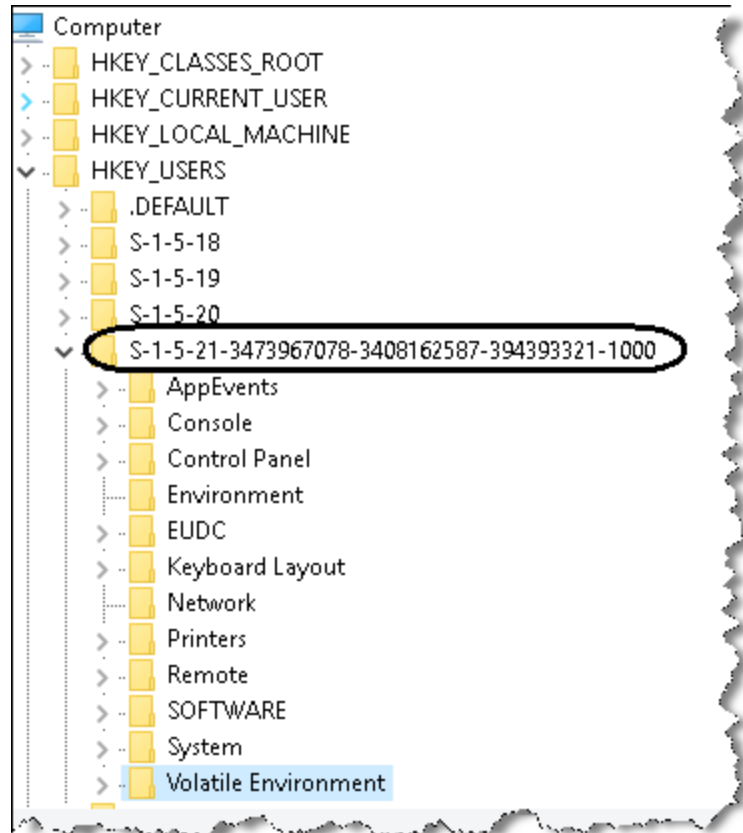
- C. Get the SID for the custom user account by running **whoami /all** from the custom user command-prompt.

The SID example for admin is **S-1-5-21-3473967078-3408162587-394393321-1000**.

If you cannot log in with the custom user account, do the following to get the user ID:

- A. Run **regedit** to launch the registry.
- B. Go to **HKEY\_USERS** to find the user ID. You can locate the problematic custom

user account by the **Volatile Environment** tag.



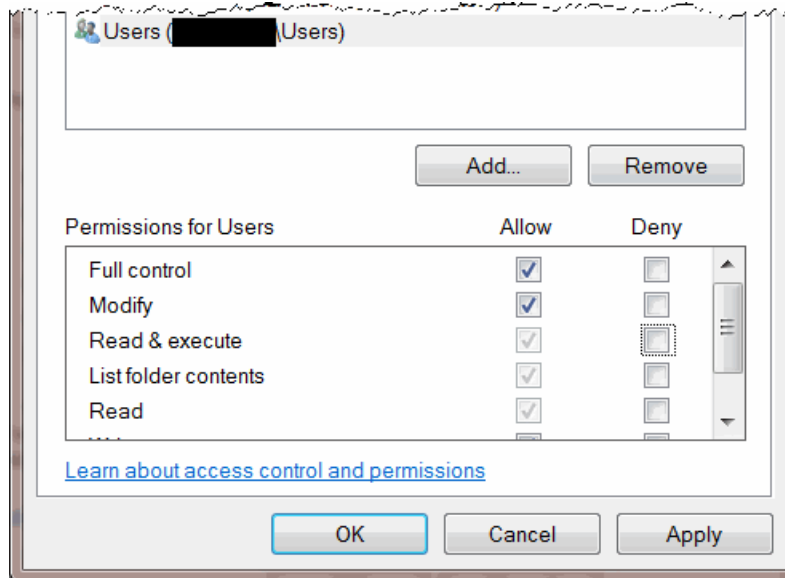
- D. Set the start/stop permission for the custom user account (for example, the admin user) on the **UCMDB\_Probe** service.

From your regular administrator command-prompt, run the following:

```
sc sdset UCMDB_Probe D:(A;;CCLCSWRPWPDTLOCRRC;;;SY)
(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRRC;;;IU)
(A;;CCLCSWLOCRRRC;;;SU)(A;;RPWPD;;;S-1-5-21-3473967078-3408162587-
394393321-1000)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)
```

The highlighted part means to grant the custom user's SID the permission to stop, start, and pause the **UCMDB\_Probe** service (RP, WP, and DT respectively).

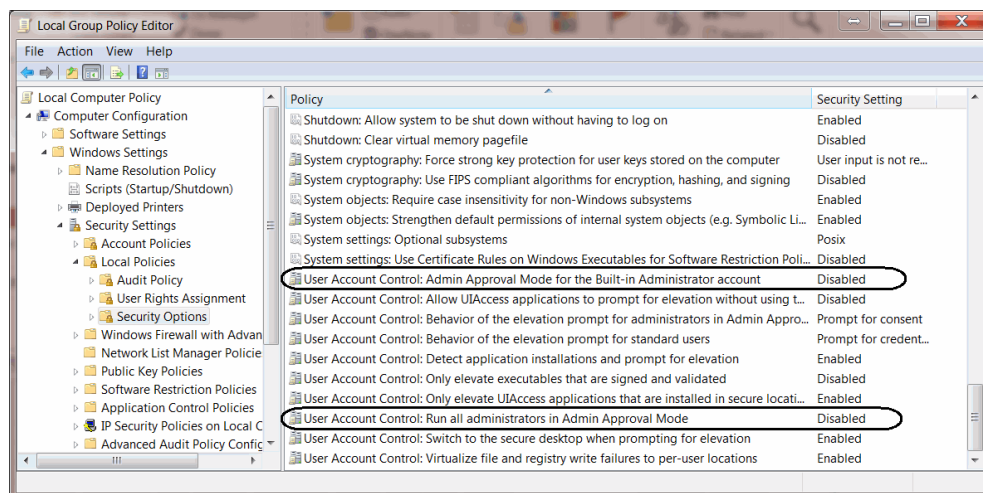
- Grant the **<DataFlowProbe>** folder permissions
  - A. Right-click the **<DataFlowProbe>** folder and select **Properties > Security**.
  - B. Edit the **Users** group permission by selecting the **Allow** checkbox for the **Full Control** permission.



C. Click **Apply** and **OK**.

**Important:** Make sure you revert the control after the probe auto upgrade.

- (Not recommended) Change the group policy in the Local Group Policy Editor window.
  - A. Open the Local Group Policy Editor by clicking **Start** and type **gpedit.msc** in the Start Search box, and then press ENTER.
  - B. In the navigation pane, expand **Computer Configuration > Windows Settings > Security Settings > Local Policies > Security Options**.
  - C. Make sure the two highlighted UAC entries are both **Disabled**.



- **User Account Control: Admin Approval Mode for the Build-in Administrator account** (Disabled) – This means UAC is disabled for the built-in Administrator account.
- **User Account Control: Run all Administrators in Admin Approval Mode** (Disabled) – This means for other administrator users, the UAC is disabled.

If this entry is **Enabled**, change it to **Disabled** and restart the operating system. The UAC would be disabled for all the administrator users in the Administrators group, which means that they have the same permission as the build-in administrator user.

**Important:** Make sure you change it back to **Enabled** after the upgrade.

## Troubleshooting Probe Upgrade - How to check if a probe is upgraded successfully?

Before upgrading a probe, the probe auto upgrader checks the environment and the probe status:

1. **Check probe version.** Only a probe of version 10.22 (with or without a CUP) or later could be upgraded. For details about supported probe versions, see [Data Flow Probe Auto Upgrade Overview](#) in the [Data Flow Management](#) section.
2. **Check probe status.** Only union mode probe in non-FIPS mode could be upgraded.
3. **Check available disk space.** At least 10 GB disk space is required to perform the probe auto upgrade.

If a probe does not satisfy the requirements, it will be restored and back on running.

### Important:

- A probe has only one chance for auto upgrade. If the auto upgrade process fails, and the probe was not broken during the process, it would be restored and you will need to manually upgrade it.
- The probe auto upgrade does not support to upgrade a probe started in console mode.

To check if a probe has been upgraded successfully, you can check the **probe\_auto\_upgrade.log** file (in the **C:\UCMDB\DataFlowProbe\runtime\log\probeUpgradeLogs** folder).

- If the probe is upgraded successfully, you should be able to see the following message in the log file:

```
Finished probe upgrade. Probe has been upgraded to [version] [Build]. Probe auto upgrade agent will exit.
```

- If your probe environment is still intact because the probe upgrader exits directly without taking any action when auto upgrade pre-check fails.

In this case, the probe is still on previous version, probe service and probe DB service are still up. You can try to run probe upgrader to perform auto upgrade again.

- a. Modify **<DataFlowProbe>/version.dat** file. So that the **version.dat** file content looks like the following:

```
version=2018.08  
build=<Release build number in the probe installer filename>  
installedVersion=<Current probe version, for example, 10.22>  
installedBuild=<Current probe build, for example, 196>
```

- b. Go to the **<DataFlowProbe>\tools\upgrade** directory, and run **post-upgrade.bat** with administrator privileges.

The probe upgrader will perform auto upgrade again.

- If the probe upgrade failed, and there is no upgrade related error message in the **probe\_auto\_upgrade.log** file.

For further information about the upgrade failure, check the following log files:

- **probe\_upgrade\_conf\_merge.log**
- **pg\_upgrade.log**
- **probe\_post\_upgrade.log**

For information about the probe log files, see "[Data Flow Probe Log Files](#)" "Data Flow Probe Log Files" in the [Data Flow Management](#) section.

## Troubleshooting Probe Upgrade - Known Issues, Limitations, and Other General Issues

### General issues

- **Probe Downgrade or Rollback**

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

- **Probe Restart**

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

- **How to Change the PostgreSQL Database Default Port**

To change the port for the PostgreSQL database, that is defined by default in the Data Flow Probe installation:

- a. Stop the Probe (if already started).
- b. Stop the UCMDB Probe DB Service.
- c. Modify the port in the following file:
  - Windows: **C:\UCMDB\DataFlowProbe\pgsql\data\postgresql.conf**
  - Linux: **/opt/UCMDB/DataFlowProbe/pgsql/data/postgresql.conf**

The following shows how to change the port from **5432** to **5433**:

**Note:** If two probes coexist on the same machine, plan the port usage carefully so that the ports used by the two probes do not conflict.

```
#port = 5432 # (change requires restart) < Old line  
port = 5433 # (change requires restart) < New line
```

- d. Make the following changes in the **DataFlowProbe.properties** file (in **C:\UCMDB\DataFlowProbe\conf** on Windows, and **/opt/UCMDB/DataFlowProbe/conf** on Linux):
  - Change:

```
jdbc:postgresql://localhost/dataflowprobe
```

to

```
jdbc:postgresql://localhost:5433/dataflowprobe
```

- Change:

```
appilog.agent.local.jdbc.uri =  
jdbc:postgresql://localhost/dataflowprobe
```

to

```
appilog.agent.local.jdbc.uri =  
jdbc:postgresql://localhost:5433/dataflowprobe
```

- Change:

```
appilog.agent.normalization.jdbc.uri =  
jdbc:postgresql://localhost/dataflowprobe
```

to

```
appilog.agent.normalization.jdbc.uri =  
jdbc:postgresql://localhost:5433/dataflowprobe
```

- Change:

```
appilog.agent.netflow.jdbc.uri =  
jdbc:postgresql://localhost/dataflowprobe
```

to

```
appilog.agent.netflow.jdbc.uri =  
jdbc:postgresql://localhost:5433/dataflowprobe
```

- **Probe auto upgrade limitation**

If the probe auto upgrade fails, retry will not resolve the issue. You need to access the corresponding probe server and perform manual deployment of the probe.

- **Probe auto upgrade known issue**



The **C:\UCMDB\temp** folder was created and used by the probe auto upgrader during the upgrade process. If you see this folder on your probe server, you can just ignore it, or safely remove it. It has no functional impact.

- **Problem:** Sometimes due to the environment, the probe installer may be in hung state and cannot finish the upgrade. If this happens, the probe upgrader will abort the probe upgrade process and restore the probe.

**Solution:** Manually upgrade the probe.

- **Problem:** Log shows that “errors occurred installing probe”, and probe service, probe DB service, or XML Enricher service could not be started. It may happen when errors occur launching the probe installer.

**Solution:** You need to manually upgrade the probe.

Most likely it is caused by the missing of some properties in the configuration file. If not, you may need to check the probe auto upgrade log files for further information. For details, see [Probe auto upgrade log files](#).

#### How to check if resources are placed under the right place after UCMDB server is upgraded to version 2018.08

1. Check if the Data Flow Probe installer is placed under the right place

Go to the **<UCMDB\_Server>\content\probe\_installer** directory. This directory should contain the probe installer **UCMDB\_DataFlowProbe\_2018.08.exe**.

2. Check if the probe auto upgrader package is placed under the right place

Go to the **<UCMDB\_Server>\runtime\probe\_upgrade** directory. This directory should contain the probe upgrade package **probe-patch-windows.zip**.

If the **probe-patch-windows.zip** package does not exist,

- a. Go to **<UCMDB\_Server>\content\probe\_patch**.
- b. Copy the **probe-patch-2018.08-windows.zip** package to the **<UCMDB\_Server>\runtime\probe\_upgrade** directory.
- c. Restart the UCMDB server. UCMDB server will then perform probe auto upgrade.

### Probe auto upgrade log files

The following probe auto upgrade log files (in the **<DataFlowProbe>\runtime\log** directory) contains details if the probe auto upgrade fails:

- **pg\_upgrade.log**. Shows the running details of the **pg\_upgrade.bat** script, including the details about PostgreSQL upgrade and table splitting.
- **probe\_upgrade\_conf\_merge.log**. Shows the related information when probe installer merger configuration files.
- **probe\_auto\_upgrade.log**. In the **probeUpgradeLogs** subfolder, shows the related information when the probe auto upgrader upgrades a probe.

For more details about the log files, see ["Data Flow Probe Log Files"](#) in the [Data Flow Management](#) section of the UCMDB Help.

### XML Enricher service port conflict issue

**Problem:** The XML Enricher service may fail to start after the probe upgrade due to port conflict. In that case, the **probe\_auto\_upgrade.log** is placed under the **failed** folder, for example, **<UCMDB\_Server>\runtime\log\probeUpgradeLogs\10.22to2018.08\failed**. You should find the following message in **probe\_auto\_upgrade.log**:

```
2018-07-14 11:27:11 INFO ServiceControl:106 - Starting XML Enricher service...
2018-07-14 11:27:11 INFO ServiceControl:328 - XML EnricherStatus status: STOPPED
2018-07-14 11:27:11 INFO ServiceControl:381 - Waiting for execution...
2018-07-14 11:27:46 ERROR ServiceControl:394 - Problems occurred during execution.
```

**Solution:** Check **<DataFlowProbe>\runtime\logWrapperEnricher.log**, if you find "Port already in use: 34545", you can change the port for XMLEnricher by editing the **<DataFlowProbe>\bin\xmlenricher\WrapperEnricher.conf** file, or free the port **34545**.

## Troubleshooting Probe Upgrade - PostgreSQL Upgrade

### Check the PostgreSQL version to verify if the upgrade is successful or not.

When PostgreSQL finishes upgrade, you can check the PostgreSQL version to verify if the probe upgrade is successful or not.

Or, you can check the **pg\_upgrade.log** in the **<DataFlowProbe>\runtime\log** folder for more details.

If PostgreSQL upgrade is completed successfully, you can find "The new PostgreSQL will be used" message in the **pg\_upgrade.log** file, and you can also see two folders:

<DataFlowProbe>\pgsql and <DataFlowProbe>\pgsql.old . The <DataFlowProbe>\pgsql.new folder was removed when the upgrade is completed successfully. If you manually run the script from the <DataFlowProbe>/tools/dbscripts folder to upgrade the database again, the log will tell you that **pgsql.new** does not exist, and running the script again has no functional impact to the PostgreSQL installation.

### How to read log messages when the PostgreSQL upgrade fails?

In some cases the PostgreSQL upgrade may fail. Then you can find three subfolders under <DataFlowProbe>: **pgsql**, **pgsql.old**, and **pgsql.new**. You can also find more details in the **pg\_upgrade.log** file, which displays messages that may indicate why the upgrade failed. You may follow the solutions for different log messages.

1. **Log message:** Folder `pgsql.new` doesn't exist.
  - **Possible Cause:** Something unexpected happened when installing the probe, and the probe failed to generate the **pgsql.new** folder.  
**Solution:** Download PostgreSQL resources for the same version from the official PostgreSQL website and extract the resources to the **pgsql.new** folder, then rerun the **pg\_upgrade.bat** script.
  - **Possible Cause:** You have already run the script more than once, and the script already deleted the **pgsql.new** folder previously.  
**Solution:** The PostgreSQL upgrade is completed successfully previously. Just check for the PostgreSQL version.
2. **Log message:** The new PostgreSQL database initialization failed.  
**Possible Cause:** The conditions for **initdb** were not met.  
**Solution:** Check if the password is correct, or there is no **data** folder in **pgsql.new**.
3. **Log message:** The precheck of the old and new PostgreSQL failed.  
**Possible Cause:** The script did not run in the local system account or has no full control of the files.  
**Solution:** Switch to the local system account, or add full control to the whole folder for users, then rerun the script.
4. **Log message:** PostgreSQL upgrade failed, the old PostgreSQL will still be used.  
**Possible Cause:** The conditions for **pg\_upgrade.exe** were not met.

**Solution:** Check the conditions for both the old PostgreSQL and the new PostgreSQL, make sure both are fine. You can manually run the following command to find more details:

```
"%DB_PATH%\pg_upgrade.exe" -b "%BASE_DIR%\pgsql\bin" -B "%BASE_DIR%\pgsql.new\bin" -d "%BASE_DIR%\pgsql\data" -D "%BASE_DIR%\pgsql.new\data" -p 5436 -P 5437 -U postgres
```

5. **Log message:** Table splitting failed, the old PostgreSQL will still be used.

**Possible Cause:** There is no **ddm\_discovery\_results** table in the database, or the upgrade failed when creating the **ddm\_discovery\_touch\_results** table.

**Solution:** Check the log details to find out where the problems happened, then check the script **tools\dbscripts\migrateData.cmd**.

After resolving [issue a](#) ~ [issue e](#) above, you can follow the steps below to upgrade PostgreSQL manually:

1. Stop the **UCMDB\_Probe\_DB** service.
2. Remove the content of the **pgsql** folder and copy the content of the **pgsql.old** folder into the **pgsql** folder.
3. Give full control to the user of the **DataFlowProbe** folder, and then from the **<DataFlowProbe>/tools/dbscripts** folder run the following command:

```
pg_upgrade.bat %DB_Password%
```

4. Once the command is successful run, revert the full control you granted to the user.

**Note:** During the upgrade, we do not keep the configuration files for **<DataFlowProbe>\pgsql\data\postgresql.conf**, so make sure you reconfigure it after the upgrade (if necessary).

## Troubleshooting Probe Upgrade - Customized Probe Configuration

When the probe installer is launched, it will merge the following configuration files:

- **DataFlowProbe.properties**
- **DataFlowProbeOverride.properties** (If exists)

The result is that all the custom configuration settings will be written into the **DataFlowProbeOverride.properties** file.

**Note:** The recommended value of the **appilog.agent.probe.sendtouchResultsToServer.maxObjects** setting in **DataFlowProbe.properties** for version 10.33 (and later) is **500**. So if your value is greater than 500, it will be reset back to **500**.

The following files will be replaced with the ones from your environment:

- <DataFlowProbe>\conf\postgresql.conf
- <DataFlowProbe>\conf\probeMgrList.xml
- <DataFlowProbe>\conf\WrapperGatewayCustom.conf
- <DataFlowProbe>\conf\WrapperManagerCustom.conf
- <DataFlowProbe>\conf\security\ssl.properties
- <DataFlowProbe>\conf\security\ProbeKeyStore.jks
- <DataFlowProbe>\conf\security\ProbeTrustStore.jks
- <DataFlowProbe>\conf\enricher.properties
- <DataFlowProbe>\conf\EnricherServiceSettings.ini
- <DataFlowProbe>\bin\WrapperEnv.conf
- <DataFlowProbe>\bin\wrapper-platform.conf
- <DataFlowProbe>\bin\WrapperManager.conf
- <DataFlowProbe>\bin\WrapperGateway.conf
- <DataFlowProbe>\bin\xmlenricher\WrapperEnricher.conf

**Problem:** After finishing probe auto upgrade, the probe cannot not be started, and many properties in **DataFlowProbe.properties** are empty. This happens when probe backing up configuration files failed.

**Solution:** You need to manually upgrade the probe. That is to say, uninstall the probe and install version 10.33 (or later) probe manually.

# Chapter 4: Troubleshooting Administration

This chapter includes:

Troubleshooting – Logging In to UCMDB .....	78
Troubleshooting and Limitations – UCMDB Server Administration .....	81
Troubleshooting and Limitations – Package Manager .....	82
CMS UI - Known Issues .....	83
Troubleshooting - Configure the Enhanced Search Engine .....	84
UCMDB doesn't start because of the search subsystem manager. What do I do? .....	84
The search doesn't return any results. ....	84
The search doesn't find CI types that I want. ....	85
The search presents too many unwanted results. ....	85
Problem with configuration - restore factory defaults .....	85
Logs and debugging info .....	86
Troubleshooting - High Availability Mode .....	86
Troubleshooting - Disable History for Specific Object CITs .....	87
Chapter 4: Troubleshooting UCMDB Server Performance with Thread Sampler .....	89
Example entry in slow.log .....	90
Chapter 4: Troubleshooting Purging - How to View and Delete History Partitions .....	91
Check partitions .....	91
Delete partitions .....	92
Logging .....	94

## Troubleshooting – Logging In to UCMDB

Use the following information to troubleshoot possible causes of failure to log in to UCMDB.

This section includes the following:

- ["Possible Causes for Failure to Log In to UCMDB" on the next page](#)
- ["Java Not Installed on Client Machine" on page 80](#)

## Possible Causes for Failure to Log In to UCMDB

Use the following information to troubleshoot possible causes of failure to log into Universal CMDB.

Problem/Possible Causes	Solutions
<p>Universal CMDB is not started successfully.</p> <p><b>Indication:</b> The <b>startup.log</b> file does not include the following line:</p> <p>**** All components started ****</p>	<p><b>Solution 1:</b> Verify that the Universal CMDB Server is up and running by accessing the Web console <b>https://&lt;Server name&gt;:8443/web-console</b> where <b>&lt;server name&gt;</b> is the name of the Universal CMDB Server to which you are connecting.</p> <p><b>Solution 2:</b> Check the database connection:</p> <p>To check that the database server is up and running:</p> <ol style="list-style-type: none"> <li>1. Launch the Web browser and navigate to: <b>https://localhost:8443/jmx-console.</b></li> <li>2. Under <b>UCMDB</b>, click <b>UCMDB:service=Dal Services</b> to open the JMX MBean View.</li> <li>3. Invoke the function <b>getDbContext</b> with a <b>customerID</b> parameter value of <b>1</b>.</li> <li>4. Check that the operation result shows no problems.</li> </ol> <p><b>Solution 3:</b> Check that the database connection parameters are correct. Ensure that you can log into the database server using the credentials you provided during the configuration procedure.</p> <p><b>Solution 4:</b> Use the <b>cmdb.dal.log</b> file to verify the database connections. The <b>cmdb.dal.log</b> file can be found in the following directory:</p> <ul style="list-style-type: none"> <li>• Windows: <b>C:\UCMDB\UCMDBServer\runtime\log</b></li> <li>• Linux: <b>/opt/UCMDB/UCMDBServer/runtime/log</b></li> </ul> <p><b>Solution 5:</b> To verify that the database connection is valid, in the Windows command interpreter (<b>cmd.exe</b>), type <b>sqlplus cmdb/cmdb@skazal</b>.</p>
<p>The CMDB is corrupted (for example, a user record may have been deleted accidentally from the CMDB).</p>	<p>Import a previously backed up database file. For details, see the <i>Database section of UCMDB Help</i>.</p> <p><b>Important:</b> The Universal CMDB server must be down while importing the database.</p> <p><b>Note:</b> When you import a previously backed up database file, you lose all data previously existing in the system.</p>
<p>The Universal CMDB login fails. This may be due to an incorrect</p>	<p><b>Solution 1:</b> Ensure that you enter a correct login user name/password combination.</p>

Problem/Possible Causes	Solutions
login name/password combination.	<b>Solution 2:</b> Restore the default
Universal CMDB login fails due to unexpected errors.	<p><b>Solution 1:</b> Select <b>Start &gt; All Programs &gt; UCMDB &gt; Universal CMDB Server Status</b> and ensure that the service is running.</p> <p><b>Solution 2:</b> Look for errors in the following log files:</p> <ul style="list-style-type: none"> <li>• <b>C:\UCMDB\UCMDBServer\runtime\log\error.log</b></li> <li>• <b>C:\UCMDB\UCMDBServer\runtime\log\ui-server.log</b></li> </ul> <p>If you find errors that are unfamiliar to you, contact Micro Focus Software Support.</p>
Universal CMDB fails to start, even though the password was successfully changed.	<p>Restore the default passwords:</p> <ol style="list-style-type: none"> <li>1. Overwrite the existing file by copying the <b>Basic_Authorization.zip</b> file from the following folder:             <ul style="list-style-type: none"> <li>◦ Windows: <b>C:\UCMDB\UCMDBServer\content\backup</b></li> <li>◦ Linux: <b>/opt/UCMDB/UCMDBServer/content/backup</b></li> </ul>             to the following folder:             <ul style="list-style-type: none"> <li>◦ Windows: <b>C:\UCMDB\UCMDBServer\content/basic_packages</b></li> <li>◦ Linux: <b>/opt/UCMDB/UCMDBServer/content/basic_packages</b></li> </ul> </li> <li>2. Log into the the JMX Console and locate the <b>UCMDB-UI:name=UCMDB Integration</b> service.</li> <li>3. Run <b>setCMDBSuperIntegrationUser</b> by using the credentials of UISysadmin.</li> <li>4. Stop the UCMDB Server.</li> <li>5. Create a new schema.</li> <li>6. Restart the UCMDB Server.</li> </ol>
After upgrading UCMDB from version 10.30 (or earlier) to 10.31 (or later), LDAP authentication fails and users cannot log in to UCMDB.	For more details about the problematic scenario, possible cause and solutions, see " <a href="#">Troubleshooting Hybrid User Management - LDAP authentication</a> " on page 181.

#### Java Not Installed on Client Machine



If Java is not installed on your machine or you have a version older than Java 8, during login a message is displayed asking you to install the correct Java Runtime Environment version. JRE is needed to view Universal CMDB applets.

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

## Troubleshooting and Limitations – UCMDb Server Administration

This section describes troubleshooting and limitations for UCMDb.

- If the **wrapper.java.additional.10=-XX:+HeapDumpOnOutOfMemoryError** parameter is set (it is enabled by default) in the **wrapper.conf** file, then every time the server fails with an Out of Memory error, it dumps the full memory to the disk. Since the memory contents could be very large, you should delete these files to avoid disk space problems.

- **Problem:** When working in a Firefox browser using Linux, you get an **OutOfMemoryError: PermGen space** error.

**Solution:** Follow these steps:

- a. Go to the **bin** directory of the Java installation directory and open the Control Panel.
- b. In the **Java** tab, select **View**.
- c. In the Java runtime environment settings, under Runtime parameters, increase the -**XX:MaxPermSize**.

- **Limitation: Unsupported characters in password when UCMDb is used in integrations**

When UCMDb is used in integrations, the following characters should not be used in the password:

- All non-ASCII characters (valid ISO 8859/1 characters that are not also ASCII characters)
- The following special characters: the tab character, the space character, and `[ \ ] ^ ` { | } ~ " # % & + , / : < = > ? @`

- **Problem:** The **"User {0} has exceeded the maximum number of login sessions"** message is displayed.

**Solution:** Ensure that you are properly logged out from other sessions on other computers. For example, closing a tab or closing the browser does not immediately close a user session on the server.

# Troubleshooting and Limitations – Package Manager

This section describes some of the troubleshooting issues that might arise when deploying and undeploying packages.

This section includes the following topics:

- ["Gold Master Reports Cannot be Deployed by Package Manager" below](#)
- ["Datamodel Resources Cannot Be Undeployed" below](#)
- ["Additional Information on Package Deployment Failure" below](#)
- ["Package Creation and Deployment in a Non-English Locale" below](#)

- **Gold Master Reports Cannot be Deployed by Package Manager**

If you export a package's resources from Package Manager that includes a Gold Master report definition, and then export those resources again to another system, the Gold Master report definition is not deployed.

- **Datamodel Resources Cannot Be Undeployed**

For a list of the package resources, see [Package Resources](#).

- **Additional Information on Package Deployment Failure**

If package deployment fails, you can check the Package Manager log files for additional information on why the deployment failure occurred.

Log files are located in the **C:\UCMDB\UCMDBServer\runtime\log** folder.

- **Package Creation and Deployment in a Non-English Locale**

This section describes the limitations when working in a non-English locale.

- You cannot deploy a package if the server locale is different than the client locale and the package name contains non-English characters.
- You cannot create a package that contains resources (for example, views and TQL queries) having non-English characters in their names, if the server locale is different from the client locale.

## CMS UI - Known Issues

**Problem:** "There is no data available for this report" message is displayed for individual default report widgets (such as Installed Software) on the Home module

- **Cause:** It could be one of the following:
  - It is true that there is no data available for the reports. Or,
  - The reports are querying over a large amount of data from the UCMDB server which exceeds the maximum number of elements allowed in view, and you may find "server view query over limit" error in log.
- **Solution:** In case of the second scenario, to resolve the display issue, go to **UCMDB UI > Administration > Infrastructure Settings Manager**, locate the **Maximum number of elements (nodes) in TQL result for view** setting (default value: 30000) and increase its value to meet your need.

**Problem:** Performance for the CMS UI is slow.

- **Possible Solution:** Add the variable **CATALINA\_OPTS** to the Operating Systems environment variables with values:  
  
-Xms512M -Xmx4096M

**Problem:** The Tomcat log that contains requests to the CMS UI and their HTTPS codes becomes too large and is unreadable.

- **Solution:** Comment out the following lines in the **server.xml** file, located in **<CMS\_UI\_installation\_directory>\webapps\release\conf**:  
  

```
<Valve className="org.apache.catalina.valves.AccessLogValve" directory="logs"
prefix="localhost_access_log." suffix=".txt"
pattern="%h %l %u %t &quot;%r&quot; %s %b" />
```

**Problem:** Icons are not displayed when the Turn Off Data URI support setting is not disabled.

- **Solution:** Disable the **Turn Off Data URI support** setting on Windows as follows:
  - a. Click **Start**, type **gpedit.msc** in the **Start Search** box, and then press **ENTER**.
  - b. In the navigation pane of the Local Group Policy Editor window, expand **Computer Configuration > Administrative Templates > Windows Components > Internet Explorer > Security Features**.
  - c. In the right pane, double-click **Turn Off Data URI support**.
  - d. Select **Enabled**, click **Apply**, and then click **OK**.
  - e. Go back to the navigation pane of the Local Group Policy Editor window, expand **User Configuration > Administrative Templates > Windows Components > Internet Explorer > Security Features**.
  - f. Repeat step 3 and step 4.

## Troubleshooting - Configure the Enhanced Search Engine

### UCMDB doesn't start because of the search subsystem manager. What do I do?

Stop UCMDB, delete the folder **<UCMDB installation folder>/search**, then restart UCMDB.

If the search still does not start, disable it, as explained in "[Troubleshooting - Configure the Enhanced Search Engine](#)" above and revert to the legacy search engine.

### The search doesn't return any results.

In the Topology Search JMX, invoke the following methods:

- **restoreFactoryDefaults:** This restores factory configuration for the search.
- **reindex:** This recreates a search index for CIs in the UCMDB model. Note, this can take up to several hours for large databases (approx 1M CIs/hour).

You can also invoke the **reindexCiType** method to re-index all the CIs of a given CI type from the CMDB model database.

## The search doesn't find CI types that I want.

There are several different possible causes for this. Check the following:

- Check that the attribute and CI type are indexable according to the indexing configuration. If they are not, add the class attributes configuration item as explained ["Troubleshooting - Configure the Enhanced Search Engine" on the previous page](#).
- Check that you have correct synonyms defined for the class in Class synonyms.
- Check that **rating** and **pageItemCount** for this CI are non-zero. Check for **rating** in the Attribute ranking and for **pageItemCount** in Presentable CI types.

Cardinality conditions don't work or return incorrect results.

In addition to checking attribute synonyms, check that the attribute type is defined as numeric in Indexing Configuration and that units configuration matches attribute units in **Search\_Parser\_Configuration\_XML**.

## The search presents too many unwanted results.

- Check if you are using queries with natural language. This can limit results of the "best guess" of what the user intended.
- If you need to be 100% certain that your query returns results only of one specific CI type, use type: **ci-type** filter in the query.
- If the two suggestions above don't help, contact the R&D team with your use case and status report from JMX.

## Problem with configuration - restore factory defaults

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

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

## Logs and debugging info

### Logs

**search.log** logs everything related to searches. Default log level is INFO, only statistics are printed. The log level and number of logs are configured with the **search.loglevel** variable in **conf/log/cmdm.properties**.

### Status Report

The topology search JMX status report displays all current configuration tables and statistics for the search engine component. It is useful to include it when reporting issues to R&D.

### Content of Solr Database

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

Example queries:

- empty query returns all CIs
- "id:a6693cd46cfd1b4fab0c3551bac9289e" returns a CI with cmdbld a6693cd46cfd1b4fab0c3551bac9289e. This uses Solr/Lucene syntax.

## Troubleshooting - High Availability Mode

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

Some examples of wrong cluster encryption configuration are:

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

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

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

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

## Troubleshooting - Disable History for Specific Object CITs

In case of investigation, if history was disabled for specific CITs, the logs can provide useful information if the operation finished successfully or why it failed. The logs to check are history logs (mainly **history.classmodel.changes.log**), **error.log** and **cmdb.dal.log**.

For example, if you successfully disabled the history for the **installed\_software** CIT, you should see the following log messages:

```
----- Starting alignment for class installed_software -----
--
    Align will be done for all descendant classes of class [installed_software]
    Class [installed_software] should not store history events anymore, going to
remove history tables
    About to remove partition registry for class [installed_software].
    Done removing partition registry for class [installed_software].
    About to remove history table [HDM_L_170910INSTALL_182931014].
    Done removing history table [HDM_L_170910INSTALL_182931014].
    About to remove history table [HDM_RL_INSTALLED_SOFTWARE_1].
    Done removing history table [HDM_RL_INSTALLED_SOFTWARE_1].
    About to remove history table [HDM_170910INSTALL_182931014].
    Done removing history table [HDM_170910INSTALL_182931014].
    About to remove history table [HDMR_INSTALLED_SOFTWARE_1].
    Done removing history table [HDMR_INSTALLED_SOFTWARE_1].
    About to remove class [installed_software] from HDM_ROOT table
    Done removing class [installed_software] from HDM_ROOT table
    About to remove related history links for class [installed_software].
    Retrieved 2,671,197 objects from memory took 452 ms
    Retrieved 3,382,173 related links from memory took 36,850 ms
    About to delete from root link table
    deleted 565,119 rows
    Entries from root link table deleted successfully
    About to delete from links history tables
    deleted 419,028 rows
    deleted 146,091 rows
    Entries from links history tables deleted successfully
    Done removing related history links for class [installed_software].
----- Finished alignment for class installed_software -----
--
```

To double check that the CITs have been deleted from history tables, you can use the following SQL statements. The count should match with the ones in the logs or should show 0 when running against **HDM\_ROOT\_1** and **HDM\_Root\_Link\_1** tables.

- Check that CITs were deleted from HDM\_ROOT\_1 table

```
select count(*) from HDM_ROOT_1 where OBJECT_CLASS='installed_software'
```

- Check the links that were deleted

Taking **installed\_software** as an example (the related links history tables may vary (usage, composition)).

Check the number of related links to instances of the CIT that was disabled history

```
select count(*) from link_1 l where l.end2_id in (select cmdb_id from CDM_
INSTALLED_SOFTWARE_1)

select count(*) from link_1 l where l.end1_id in (select cmdb_id from CDM_
INSTALLED_SOFTWARE_1)
```

- Check the number of related links that will be removed from HDM\_Root\_Link\_1 table

```
SELECT count(*) from HDM_root_link_1 where CMDB_ID IN (select l.CMDB_ID from
link_1 l , cdm_root_1 r where l.END1_ID=r.CMDB_ID and r.A_ROOT_
CLASS='installed_software')
SELECT count(*) from HDM_root_link_1 where CMDB_ID IN (select l.CMDB_ID from
link_1 l , cdm_root_1 r where l.END2_ID=r.CMDB_ID and r.A_ROOT_
CLASS='installed_software')
```

- Check the number of related link that will be removed from links history tables (the links history tables may vary (usage, composition))

```
SELECT count(*) from HDM_170910CONTAINMENT_1 where CMDB_ID IN ( select
l.CMDB_ID from link_1 l , cdm_root_1 r where l.END2_ID=r.CMDB_ID and r.A_
ROOT_CLASS='installed_software')
SELECT count(*) from HDM_170910CONTAINMENT_1 where CMDB_ID IN ( select
l.CMDB_ID from link_1 l , cdm_root_1 r where l.END1_ID=r.CMDB_ID and r.A_
ROOT_CLASS='installed_software')
```

The following logs should be seen when removing the qualifier from UI(enabling history for the selected CIT):

```
INFO [qtp1197761641-589] - ----- Starting alignment for class
installed_software -----
INFO [qtp1197761641-589] - Align will be done for all descendant classes of class
[installed_software]
INFO [qtp1197761641-589] - Start align for Class [installed_software]
INFO [qtp1197761641-589] - Class installed_software is new (has no registry of
```



```

current table name). Going to create history tables for it.
INFO [qtp1197761641-589] - Going to create history tables for class installed_
software
INFO [qtp1197761641-589] - Table name for class installed_software: HDM_
170510INSTALL_867021642
INFO [qtp1197761641-589] - Created table HDM_170510INSTALL_867021642 for class
[installed_software]
INFO [qtp1197761641-589] - Created table for removed CIs HDMR_INSTALLED_SOFTWARE_
1 for class [installed_software]
INFO [qtp1197761641-589] - Created table for removed CIs HDMR_INSTALLED_SOFTWARE_
1 for class [installed_software]
INFO [qtp1197761641-589] - Created list attributes table HDML_170510INSTALL_
867021642 for for class [installed_software]
INFO [qtp1197761641-589] - Created list attributes table for removed CIs HDML_
INSTALLED_SOFTWARE_1 for for class [installed_software]
INFO [qtp1197761641-589] - Created list attributes table for removed CIs HDML_
INSTALLED_SOFTWARE_1 for for class [installed_software]
INFO [qtp1197761641-589] - Finished to create history tables for class installed_
software

```

For large environments, adding the CIT\_NOT\_TRACKED\_FOR\_HISTORY qualifier may take longer depending on the environment activity and its performance as well as UCMDB Database performance. If the operation fails with an operation timeout or sql query timeout increase the timeout specified and add the qualifier again after a server restart.

If the operation fails with an error, the CIT\_NOT\_TRACKED\_FOR\_HISTORY qualifier should be added to the CIT, and it should work as expected. However, not all history instances were deleted from history tables. You can check these instances directly in the database using similar SQL queries like the ones presented above. (Only the tables names and class name should match the required CIT). Same queries can be converted to delete statements to clean the history tables from CI instances that should be removed.

## Chapter 4: Troubleshooting UCMDB Server Performance with Thread Sampler

UCMDB Server includes a thread sampler that can be used to troubleshoot performance related problems without the use of an external tool like VisualVM or YourKit. This will sample all threads and include the collected information in the **slow.log** as part of the logged threads.

After enabling the thread sampler, when a new entry is created in **slow.log**, a list of top 10 methods in which the most time was spent will be logged with the thread. By default the sampling is done at a rate of 100 milliseconds.

**To enable the thread sampler,**

1. On the UCMDB server, launch the Web browser and access JMX console by providing the following address: **https://localhost:8443/jmx-console**.

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

2. Locate the **setGlobalSettingValue** operation in the **UCMDB:service=Settings Services** category.
3. Provide the following parameter values:  
**name:** thread.sampling.enabled  
**value:** true
4. Click **Invoke**.
5. Restart the UCMDB server.

#### To change the sampling rate value,

1. On the UCMDB server, launch the Web browser and access JMX console by providing the following address: **https://localhost:8443/jmx-console**.

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

2. Locate the **setGlobalSettingValue** operation in the **UCMDB:service=Settings Services** category
3. Provide the following parameter values:  
**name:** thread.sampling.frequency  
**value:** <specify a value in milliseconds>
4. Click **Invoke**.
5. Restart the UCMDB server.

## Example entry in **slow.log**

Top 10 sampled methods (name, own time, total time) ordered by own time:

```
java.net.SocketInputStream.socketRead0(Native Method), 34400ms, 34400ms
java.util.zip.Inflater.inflateBytes(Native Method), 17400ms, 17400ms
java.io.FileInputStream.readBytes(Native Method), 9900ms, 9900ms
java.lang.Object.wait(Native Method), 4200ms, 4200ms
java.util.Arrays.copyOf(Arrays.java:3332), 1100ms, 1100ms
java.util.Arrays.copyOf(Arrays.java:3236), 1000ms, 1000ms
```

```
java.util.zip.ZipFile.getEntry(Native Method), 900ms, 900ms
java.net.SocketOutputStream.socketWrite0(Native Method), 900ms, 900ms
java.lang.Class.forName0(Native Method), 800ms, 900ms
appilog.common.utils.packaging.PackagesFileUtils.inputStreamToBytes
(PackagesFileUtils.java:350), 800ms, 1500ms
```

## Chapter 4: Troubleshooting Purging - How to View and Delete History Partitions

The **PurgeHistoryTroubleshooting** JMX method in the **UCMDB:service=History DB Services** category allows users to view history partitions and generate SQL statements for deleting the history partitions.

### Check partitions

To check all partitions from DB and UCMDB, do the following:

1. On the UCMDB server, launch the Web browser and access JMX console by providing the following address: **https://localhost:8443/jmx-console**.  
  
You may have to log in with a user name and password.
2. Locate the **PurgeHistoryTroubleshooting** JMX method in the **UCMDB:service=History DB Services** category.
3. Select **False**.
4. Click **Invoke**.

The result page displays the partitions corresponding to the values from the infrastructure settings **History Months To Save Back** and **History purging extra months to save back removed**

**data.**

**Mbean: UCMDB:service=History DB Services. Method: purgeHistoryTroubleshooting**

UCMDB_HIST_PARTITIONS (hist_YYMM)	Rows_count
hist_1804	1
hist_1805	1
hist_1806	763
DB_HIST_PARTITIONS (hist_YYMM)	Rows_count
hist_1804	1
hist_1805	1
hist_1806	1470
other_tables	2541

## Delete partitions

You can view all partitions from UCMDB (records in the URM\_RESOURCES table) and DB (physical tables in DB), and also generate the delete statements.

To delete partitions, do the following:

1. View partitions and generate delete statements
  - a. On the UCMDB server, launch the Web browser and access JMX console by providing the following address: **https://localhost:8443/jmx-console**.  
  
You may have to log in with a user name and password.
  - b. Locate the **PurgeHistoryTroubleshooting** JMX method in the **UCMDB:service=History DB Services** category.
  - c. Select **True**.
  - d. Click **Invoke**.

The returned result page displays all partitions from UCMDB (records in the URM\_RESOURCES table) and DB (physical tables in DB), and also the delete statements generated.

The delete statements are generated depending on the values from the infrastructure settings **History Months To Save Back** and **History purging extra months to save back removed data**.

**Mbean: UCMDB:service=History DB Services. Method: purgeHistoryTroubleshooting**

UCMDB_HIST_PARTITIONS (hist_YYMM)	Rows_count
hist_17	1
hist_1801	1
hist_1802	1
hist_1803	1
hist_1804	1
hist_1805	1
hist_1806	763
DB_HIST_PARTITIONS (hist_YYMM)	Rows_count
hist_17	1
hist_1801	1
hist_1802	1
hist_1803	1
hist_1804	1
hist_1805	1
hist_1806	1470
other_tables	2541

Copy this statement and then run it in the DB context in order to delete old UCMDB history partitions from URM\_RESOURCES.

```
DELETE FROM URM_RESOURCES WHERE TYPE = 'History_HIST_PARTITIONS' AND ( 1 = 2
or TEXT_DATA like '%HDM_16%' or TEXT_DATA like '%HDML_16%'
or TEXT_DATA like '%HDM_17%' or TEXT_DATA like '%HDML_17%'
or TEXT_DATA like '%HDM_1801%' or TEXT_DATA like '%HDML_1801%'
or TEXT_DATA like '%HDM_1802%' or TEXT_DATA like '%HDML_1802%'
or TEXT_DATA like '%HDM_1803%' or TEXT_DATA like '%HDML_1803%');
GO
```

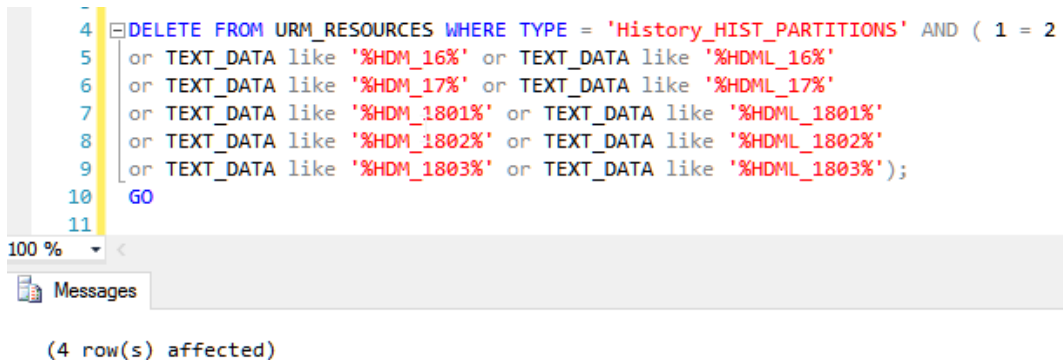
Copy this statement, and then run it in the DB context. The output will be a set of DROP TABLES statements which needs to be run in the DB context for the actions to take place.

```
select 'DROP TABLE ' + name + ';' + CHAR(10) + 'GO' from sys.tables WHERE (1 = 2
or name like '%HDM_16%' or name like '%HDML_16%'
or name like '%HDM_17%' or name like '%HDML_17%'
or name like '%HDM_1801%' or name like '%HDML_1801%'
or name like '%HDM_1802%' or name like '%HDML_1802%'
or name like '%HDM_1803%' or name like '%HDML_1803%');
```

In the screenshot above, you can see that there exists partitions from last year ( 2017 - “hist\_17” ) until June 2018 ( “hist\_1806” ).

## 2. Delete partitions

- a. To delete old **UCMDB history partitions** (from the URM\_RESOURCES table), copy the first statement from the result page and then run it in the DB context.



- b. To delete old **DB history partitions**, copy the second statement from the result page and then run it in the DB context.

```

15 select 'DROP TABLE ' + name + ';' + CHAR(10) + 'GO' from sys.tables WHERE (1 = 2
16 or name like '%HDM_16%' or name like '%HDML_16%'
17 or name like '%HDM_17%' or name like '%HDML_17%'
18 or name like '%HDM_1801%' or name like '%HDML_1801%'
19 or name like '%HDM_1802%' or name like '%HDML_1802%'
20 or name like '%HDM_1803%' or name like '%HDML_1803%');

```

00 %

Results Messages

	(No column name)
1	DROP TABLE HDM_171210INTERFACE_1; GO
2	DROP TABLE HDM_180110INTERFACE_1; GO
3	DROP TABLE HDM_180210INTERFACE_1; GO
4	DROP TABLE HDM_180310INTERFACE_1; GO

- c. The output will be a set of DROP TABLE statements which needs to be run in the DB context for the actions to take place.

```

23 DROP TABLE HDM_171210INTERFACE_1;
24 GO
25 DROP TABLE HDM_180110INTERFACE_1;
26 GO
27 DROP TABLE HDM_180210INTERFACE_1;
28 GO
29 DROP TABLE HDM_180310INTERFACE_1;
30 GO

```

100 %

Messages

Command(s) completed successfully.

3. After running the scripts on DB, check if all old history partitions were cleaned, by invoking the same **PurgeHistoryTroubleshooting** JMX method with the flag setting to **False**.

## Logging

The calls of the **PurgeHistoryTroubleshooting** JMX method are logged in the **history.purge.log** file (<UCMDBServer>\runtime\log) along with the timestamp, DB stored procedure used, value of parameters (settings).

When invoking **PurgeHistoryTroubleshooting** with the flag setting to **true**, both DB stored procedures (SPU\_SHOW\_HIST\_PARTITIONS and SPU\_DELETE\_HIST\_PARTITIONS) will be executed; whereas invoking it with the flag setting to **false**, only the SPU\_SHOW\_HIST\_PARTITIONS procedure will be executed.

```
2018-07-09 11:52:14,374 INFO [qtp1403217169-6441] - (purgeHistoryTroubleshooting JMX method) -  
Calling stored procedure SPU_SHOW_HIST_PARTITIONS with the following parameters: monthsToSaveBack= 3  
and extraMonthsToSaveOldRemovedData= 1  
2018-07-09 11:52:15,511 INFO [qtp1403217169-6441] - (purgeHistoryTroubleshooting JMX method) -  
Calling stored procedure SPU_DELETE_HIST_PARTITIONS with the following parameters: monthsToSaveBack= 3  
and extraMonthsToSaveOldRemovedData= 1
```

# Chapter 5: Troubleshooting Data Flow Management

This chapter includes:

Troubleshooting and Limitations – Data Flow Probe Setup .....	97
Data Flow Probe Setup - Troubleshooting .....	97
Data Flow Probe Setup - Limitations .....	100
Troubleshooting Probe Auto Upgrade .....	101
Troubleshooting and Limitations – Multiple CMDB Integration .....	107
Troubleshooting .....	107
Limitations .....	109
Universal Discovery Troubleshooting and Limitations .....	110
Troubleshooting – Universal Discovery .....	110
Limitations – Universal Discovery .....	118
Inventory Discovery Troubleshooting .....	118
How to view all information related to a device in a centralized view? .....	119
How to troubleshoot network availability and latency issue related to a device? .....	120
How to check the key indexes of the discovery history information for a discovered device? ..	126
How to check device related logs for a discovered device? .....	132
How to invoke discovery job relevant to the discovered device manually and check status to identify potential discovery errors? .....	134
How to check which pattern (management zone) is used in the discovery for a discovered device? .....	144
How to check detailed discovery settings used in the discovery for a discovered device? .....	146
How to check the SNMP credentials used in the discovery for a discovered device? .....	149
How to View Discovery Status and Errors for a Selected CI from the Discovery Progress Widget .....	151
APLS Integration Troubleshooting - Error Handling Messages .....	153



# Troubleshooting and Limitations – Data Flow Probe Setup

## Data Flow Probe Setup - Troubleshooting

**Problem:** You cannot transfer a Data Flow Probe from one domain to another.

**Reason:** Once you have defined the domain of a Probe, you can change its ranges, but not the domain.

**Solution:** Install the Probe again:

1. (Optional) If you are going to use the same ranges for the Probe in the new domain, export the ranges before removing the Probe. For details, see [Ranges Pane](#).
2. Remove the existing Probe from UCMDDB. For details, see the **Remove Domain or Probe** button in [Data Flow Probe Setup Window](#).
3. Install the Probe. For details, see the section about installing the Data Flow Probe in the interactive *Universal CMDB Deployment Guide*.
4. During installation, make sure to give the new Probe a different name to the name given to the old Probe, or make sure you delete the reference to Probe from the original domain.

**Problem:** Discovery shows a disconnected status for a Probe.

**Solution:** Check the following on the Probe machine:

- That the Probe is running
- That there are no network problems

**Solution:** The probe status is **Disconnected** or **Disconnected (being restarted)**.

- Search for restart messages in the **wrapperProbeGW** logs.
- If the probe does not restart, try to take probe thread dump from the disconnected time and search for the **ProbeGW Tasks Downloader** thread.
- If there is no probe thread dump, investigate the problematic timeframe in the **wrapperProbeGw log**. In particular:

- Check if the probe tasks confirmer has been running for more than 5 minutes.
- Check if some of the resources are being downloaded for more than 5 minutes.

**Problem:** The connection between the Universal CMDB server and the Probe fails due to an HTTP exception.

**Solution:** Ensure that none of the Probe ports are in use by another process.

**Problem:** A Data Flow Probe node name cannot be resolved to its IP address. If this happens, the host cannot be discovered, and the Probe does not function correctly.

**Solution:** Add the host machine name to the Windows HOSTS file on the Data Flow Probe machine.

**Problem:** After uninstalling the Data Flow Probe, mysqld.exe and associated files are not deleted.

**Solution:** To delete all files, restart the machine on which the Data Flow Probe was installed.

**Problem:** After the UCMDB Server CUP is updated, the Probe fails to start or fails to connect to server

**Solution:** The Probe's CUP version must be the same as UCMDB Server's CUP version. If the CUP versions are not aligned, you must update the Probe's CUP version. To do this, see [How to Deploy a Data Flow Probe CUP](#).

In some cases, the CUP may need to be deployed manually on a Probe. For details, see [How to Deploy a Data Flow Probe CUP Manually](#).

**Problem:** I want to check if my integration probe is connected, but I can't see it listed in the Data Flow Probe Setup module tree.

**Reason:** The Data Flow Probe Setup module displays only Data Flow Probes for discovery. Integration Probes—that is, Probes on Linux machines, and Windows Probes configured for integration only—are not displayed in the Data Flow Probe Setup module.

**Workaround:** To see if an integration Probe is connected, create a dummy integration point and verify that the Probe is listed among the Probes that can be selected for the integration point (in the **Data Flow Probe** field). For details, see [How to Set Up an Integration Point](#).

**Problem:** Troubleshooting PostgreSQL Issues

**Solution:**

The table below lists the Data Flow Probe database scripts. These scripts can be modified for administration purposes, both in Windows and Linux environments.

**Note:**

- The scripts are located on the Data Flow Probe machine, in the following location:
- Data Flow Probe database scripts should be changed for specific administration purposes only.

Script	Description
exportPostgresql [PostgreSQL root account password]	Exports all data from the DataFlowProbe database schema to <b>data_flow_probe_export.bin</b> in the current directory
importPostgresql [Export file name] [PostgreSQL root account password]	Imports data from a file created by the <b>exportPostgresql</b> script into the DataFlowProbe schema
enable_remote_user_access	Configures the PostgreSQL Data Flow Probe account to be accessible from remote machines
remove_remote_user_access	Configures the PostgreSQL Data Flow Probe account to be accessible only from the local machine (default)
set_db_user_password [new PostgreSQL Data Flow Probe account password] [PostgreSQL root account password]	Modifies the PostgreSQL Data Flow Probe account password
set_root_password [new PostgreSQL root account password] [Current PostgreSQL root account password]	Modifies the PostgreSQL root account password

**Problem:** The Data Flow Probe database service cannot start.

- **Reason:** Hosts machine must not contain "localhost".

**Solution:** On the Data Flow Probe machine, open

- Windows: %systemroot%\system32\drivers\etc\hosts
- Linux: /etc/hosts

and ensure that all lines containing "**localhost**" are commented out.

- **Reason: Microsoft Visual C++ 2010 x64 Redistributable** is installed during the installation of the Probe. If for some reason this redistributable is uninstalled, PostgreSQL stops working

**Solution:** Check if Microsoft Visual C++ 2010 x64 Redistributable is installed. If not, reinstall it.

## Data Flow Probe Setup - Limitations

- **Limitation:** The Probe cluster range distribution purely handles the potential number of active or inactive IP addresses available in its network range, not the actual number of IP addresses populated or the number of devices available inside those ranges. For example, You have 100 IP addresses, and Probe cluster distributes them into two Probes: 50 IP addresses to one Probe and 50 IP addresses to the other Probe. If only one IP address is active on Probe A and 50 IP addresses are active on Probe B, Probe B would take a disproportional share of the load.

**Reason:** The actual number of IP addresses are unavailable before the actual discovery.

**Workaround:** If many IP ranges are unevenly populated, in order to have full control of the IP address distribution, it is best to avoid using the Probe cluster feature and simply use Probes separately.

- When the Probe is running in separate mode on a machine where both the Gateways and the Manager share a same installation folder, the Data Flow Probe CUP must be installed manually. For details, see [How to Deploy a Data Flow Probe CUP Manually](#).
- Data Flow Probe CUPs that were deployed manually can be uninstalled using manual methods only. For details, see [How to Uninstall Probe CUPs Manually](#).
- Universal Discovery Agent may not callhome in, but not limited to, the following scenario:
  - The callhome IP address that is configured on the Universal Discovery Agent belongs to a client type range that is added to a cluster.

**Note:** The Universal Discovery Agent supports 1 primary and 1 secondary probe.

- The range is a member of a probe cluster.
- The cluster contains two or more probes.

In this scenario, callhome may not work as expected. Contact Micro Focus Support for assistance in configuring callhome.

# Troubleshooting Probe Auto Upgrade

## General issues

- **Probe Downgrade or Rollback**

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

- **Probe Restart**

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

- **How to Change the PostgreSQL Database Default Port**

To change the port for the PostgreSQL database, that is defined by default in the Data Flow Probe installation:

- a. Stop the Probe (if already started).
- b. Stop the UCMDB Probe DB Service.
- c. Modify the port in the following file:
  - Windows: **C:\UCMDB\DataFlowProbe\pgsql\data\postgresql.conf**
  - Linux: **/opt/UCMDB/DataFlowProbe/pgsql/data/postgresql.conf**

The following shows how to change the port from **5432** to **5433**:

**Note:** If two probes coexist on the same machine, plan the port usage carefully so that the ports used by the two probes do not conflict.

```
#port = 5432 # (change requires restart) < Old line  
port = 5433 # (change requires restart) < New line
```

- d. Make the following changes in the **DataFlowProbe.properties** file (in

**C:\UCMDB\DataFlowProbe\conf** on Windows, and **/opt/UCMDB/DataFlowProbe/conf** on Linux):

- Change:

```
jdbc:postgresql://localhost/dataflowprobe
```

to

```
jdbc:postgresql://localhost:5433/dataflowprobe
```

- Change:

```
appilog.agent.local.jdbc.uri =  
jdbc:postgresql://localhost/dataflowprobe
```

to

```
appilog.agent.local.jdbc.uri =  
jdbc:postgresql://localhost:5433/dataflowprobe
```

- Change:

```
appilog.agent.normalization.jdbc.uri =  
jdbc:postgresql://localhost/dataflowprobe
```

to

```
appilog.agent.normalization.jdbc.uri =  
jdbc:postgresql://localhost:5433/dataflowprobe
```

- Change:

```
appilog.agent.netflow.jdbc.uri =  
jdbc:postgresql://localhost/dataflowprobe
```

to

```
appilog.agent.netflow.jdbc.uri =  
jdbc:postgresql://localhost:5433/dataflowprobe
```

- **Probe auto upgrade limitation**

If the probe auto upgrade fails, retry will not resolve the issue. You need to access the corresponding probe server and perform manual deployment of the probe.

- **Probe auto upgrade known issue**

The **C:\UCMDB\temp** folder was created and used by the probe auto upgrader during the upgrade process. If you see this folder on your probe server, you can just ignore it, or safely remove it. It has no functional impact.

- **Problem:** Sometimes due to the environment, the probe installer may be in hung state and cannot finish the upgrade. If this happens, the probe upgrader will abort the probe upgrade process and restore the probe.

**Solution:** Manually upgrade the probe.

- **Problem:** Log shows that “errors occurred installing probe”, and probe service, probe DB service, or XML Enricher service could not be started. It may happen when errors occur launching the probe installer.

**Solution:** You need to manually upgrade the probe.

Most likely it is caused by the missing of some properties in the configuration file. If not, you may need to check the probe auto upgrade log files for further information. For details, see [Probe auto upgrade log files](#).

#### **How to check if resources are placed under the right place after UCMDB server is upgraded to version 2018.08**

1. Check if the Data Flow Probe installer is placed under the right place

Go to the **<UCMDB\_Server>\content\probe\_installer** directory. This directory should contain the probe installer **UCMDB\_DataFlowProbe\_2018.08.exe**.

2. Check if the probe auto upgrader package is placed under the right place

Go to the **<UCMDB\_Server>\runtime\probe\_upgrade** directory. This directory should contain the probe upgrade package **probe-patch-windows.zip**.

If the **probe-patch-windows.zip** package does not exist,

- a. Go to **<UCMDB\_Server>\content\probe\_patch**.
- b. Copy the **probe\_patch-2018.08-windows.zip** package to the **<UCMDB\_Server>\runtime\probe\_upgrade** directory.
- c. Restart the UCMDB server. UCMDB server will then perform probe auto upgrade.

### Probe auto upgrade log files

The following probe auto upgrade log files (in the **<DataFlowProbe>\runtime\log** directory) contains details if the probe auto upgrade fails:

- **pg\_upgrade.log**. Shows the running details of the **pg\_upgrade.bat** script, including the details about PostgreSQL upgrade and table splitting.
- **probe\_upgrade\_conf\_merge.log**. Shows the related information when probe installer merger configuration files.
- **probe\_auto\_upgrade.log**. In the **probeUpgradeLogs** subfolder, shows the related information when the probe auto upgrader upgrades a probe.

For more details about the log files, see ["Data Flow Probe Log Files"](#) in the [Data Flow Management](#) section of the UCMDB Help.

### XML Enricher service port conflict issue

**Problem:** The XML Enricher service may fail to start after the probe upgrade due to port conflict. In that case, the **probe\_auto\_upgrade.log** is placed under the **failed** folder, for example, **<UCMDB\_Server>\runtime\log\probeUpgradeLogs\10.22to2018.08\failed**. You should find the following message in **probe\_auto\_upgrade.log**:

```
2018-07-14 11:27:11 INFO ServiceControl:106 - Starting XML Enricher service...
2018-07-14 11:27:11 INFO ServiceControl:328 - XML EnricherStatus status: STOPPED
2018-07-14 11:27:11 INFO ServiceControl:381 - Waiting for execution...
2018-07-14 11:27:46 ERROR ServiceControl:394 - Problems occurred during execution.
```

**Solution:** Check **<DataFlowProbe>\runtime\logWrapperEnricher.log**, if you find "Port already in use: 34545", you can change the port for XMLEnricher by editing the **<DataFlowProbe>\bin\xmlenriche\WrapperEnricher.conf** file, or free the port **34545**.

### Check the PostgreSQL version to verify if the upgrade is successful or not.

When PostgreSQL finishes upgrade, you can check the PostgreSQL version to verify if the probe upgrade is successful or not.



Or, you can check the **pg\_upgrade.log** in the **<DataFlowProbe>\runtime\log** folder for more details.

If PostgreSQL upgrade is completed successfully, you can find “The new PostgreSQL will be used” message in the **pg\_upgrade.log** file, and you can also see two folders:

**<DataFlowProbe>\pgsql** and **<DataFlowProbe>\pgsql.old**. The **<DataFlowProbe>\pgsql.new** folder was removed when the upgrade is completed successfully. If you manually run the script from the **<DataFlowProbe>/tools/dbscripts** folder to upgrade the database again, the log will tell you that **pgsql.new** does not exist, and running the script again has no functional impact to the PostgreSQL installation.

### How to read log messages when the PostgreSQL upgrade fails?

In some cases the PostgreSQL upgrade may fail. Then you can find three subfolders under **<DataFlowProbe>**: **pgsql**, **pgsql.old**, and **pgsql.new**. You can also find more details in the **pg\_upgrade.log** file, which displays messages that may indicate why the upgrade failed. You may follow the solutions for different log messages.

1. **Log message:** Folder **pgsql.new** doesn't exist.

- **Possible Cause:** Something unexpected happened when installing the probe, and the probe failed to generate the **pgsql.new** folder.

**Solution:** Download PostgreSQL resources for the same version from the official PostgreSQL website and extract the resources to the **pgsql.new** folder, then rerun the **pg\_upgrade.bat** script.

- **Possible Cause:** You have already run the script more than once, and the script already deleted the **pgsql.new** folder previously.

**Solution:** The PostgreSQL upgrade is completed successfully previously. Just check for the PostgreSQL version.

2. **Log message:** The new PostgreSQL database initialization failed.

**Possible Cause:** The conditions for **initdb** were not met.

**Solution:** Check if the password is correct, or there is no **data** folder in **pgsql.new**.

3. **Log message:** The precheck of the old and new PostgreSQL failed.

**Possible Cause:** The script did not run in the local system account or has no full control of the files.

**Solution:** Switch to the local system account, or add full control to the whole folder for users, then rerun the script.

4. **Log message:** PostgreSQL upgrade failed, the old PostgreSQL will still be used.

**Possible Cause:** The conditions for **pg\_upgrade.exe** were not met.

**Solution:** Check the conditions for both the old PostgreSQL and the new PostgreSQL, make sure both are fine. You can manually run the following command to find more details:

```
"%DB_PATH%\pg_upgrade.exe" -b "%BASE_DIR%\pgsql\bin" -B "%BASE_
DIR%\pgsql.new\bin" -d "%BASE_DIR%\pgsql\data" -D "%BASE_
DIR%\pgsql.new\data" -p 5436 -P 5437 -U postgres
```

5. **Log message:** Table splitting failed, the old PostgreSQL will still be used.

**Possible Cause:** There is no **ddm\_discovery\_results** table in the database, or the upgrade failed when creating the **ddm\_discovery\_touch\_results** table.

**Solution:** Check the log details to find out where the problems happened, then check the script **tools\dbscripts\migrateData.cmd**.

After resolving [issue a](#) ~ [issue e](#) above, you can follow the steps below to upgrade PostgreSQL manually:

1. Stop the **UCMDB\_Probe\_DB** service.
2. Remove the content of the **pgsql** folder and copy the content of the **pgsql.old** folder into the **pgsql** folder.
3. Give full control to the user of the **DataFlowProbe** folder, and then from the **<DataFlowProbe>\tools\dbscripts** folder run the following command:

```
pg_upgrade.bat %DB_Password%
```

4. Once the command is successful run, revert the full control you granted to the user.

**Note:** During the upgrade, we do not keep the configuration files for **<DataFlowProbe>\pgsql\data\postgresql.conf**, so make sure you reconfigure it after the upgrade (if necessary).

When the probe installer is launched, it will merge the following configuration files:

- **DataFlowProbe.properties**
- **DataFlowProbeOverride.properties** (If exists)

The result is that all the custom configuration settings will be written into the **DataFlowProbeOverride.properties** file.

**Note:** The recommended value of the **appilog.agent.probe.sendtouchResultsToServer.maxObjects** setting in **DataFlowProbe.properties** for version 10.33 (and later) is **500**. So if your value is greater than 500, it will be reset back to **500**.

The following files will be replaced with the ones from your environment:

- <DataFlowProbe>\conf\postgresql.conf
- <DataFlowProbe>\conf\probeMgrList.xml
- <DataFlowProbe>\conf\WrapperGatewayCustom.conf
- <DataFlowProbe>\conf\WrapperManagerCustom.conf
- <DataFlowProbe>\conf\security\ssl.properties
- <DataFlowProbe>\conf\security\ProbeKeyStore.jks
- <DataFlowProbe>\conf\security\ProbeTrustStore.jks
- <DataFlowProbe>\conf\enricher.properties
- <DataFlowProbe>\conf\EnricherServiceSettings.ini
- <DataFlowProbe>\bin\WrapperEnv.conf
- <DataFlowProbe>\bin\wrapper-platform.conf
- <DataFlowProbe>\bin\WrapperManager.conf
- <DataFlowProbe>\bin\WrapperGateway.conf
- <DataFlowProbe>\bin\xmlenricher\WrapperEnricher.conf

**Problem:** After finishing probe auto upgrade, the probe cannot not be started, and many properties in **DataFlowProbe.properties** are empty. This happens when probe backing up configuration files failed.

**Solution:** You need to manually upgrade the probe. That is to say, uninstall the probe and install version 10.33 (or later) probe manually.

## Troubleshooting and Limitations – Multiple CMDB Integration

### Troubleshooting

When performing troubleshooting, be sure to check both CMDB server and Probe logs.

- CMDB server logs
  - fcldb.log
  - fcldb.adapters.log
  - error.log
  - fcldb.reconciliation.log (for population jobs)
- Probe logs
  - wrapperProbeGw.log
  - fcldb.log
  - fcldb.adapters.log
  - probe-infra.log

Following are some problems that you may encounter and their solutions.

- **Problem.** TQL query not active/persistent error message.

The Query settings have been changed manually.

**Solution.** Run full population to reactivate/persist the query.

- **Problem.** The number of CIs that is populated is much larger than the requested amount.

**Solution.** Since the automatic completion feature for reconciliation is turned on by default, it may populate the CMDB with additional CIs or links, in order to contain sufficient information to insert the CIs into the CMDB.

- **Problem.** Changes are not populated immediately after a job is run.

Changes may take a few minutes to be detected by the live mechanism.

**Solution.** Wait a few minutes for changes to be populated by your next population job.

- **Problem.** CIs are not populated into the CMDB.

Changes may take a few minutes to be detected by the live mechanism.

**Solution.** Wait a few minutes for changes to be populated by your next population job.

Check the CMDB reconciliation logs for more information.

- **Problem.** Deletions are not populated.

**Solution:**

- Make sure that you have selected the **Allow Delete** check box in the population job properties.
- Check the query you are running. Deletes are not supported on federated queries, and the aging mechanism must be used.
- **Problem.** Queries that contain compound relationships fail.  
**Solution.** If you want to let those TQL queries run, remove subgraph and uncheck **Show full path between source and target CIs** in the query's Compound Relationship properties, then the queries can run.
- **Problem.** Authentication fails.  
**Solution.** Since the UCMDB 9.x /10.x adapter uses the UCMDB API for connection, set up an integration user to ensure that you provide proper credentials. For details, see "Create an Integration User" in the *Developer Reference section of the UCMDB Help*.
- **Problem.** The Data Push job fails with the message "Remote UCMDB version is not supported."  
**Solution.** The Data Push flow only supports pushing to UCMDB version 9.05 CUP 9 and later CUPs, or UCMDB version 10.01 and later (it does not support pushing to UCMDB version 10.00). Upgrade your remote UCMDB or alternatively, run the integration using the population flow.
- **Problem.** When the full pull integration job runs a second time, the CIs that were previously created will be deleted. The auto-deletion for cmdb10xadapter may cause the unexpected deletion of CIs due to TQL calculation issue, for example, when trying to delete a relationship, the related CIs are deleted as well.  
**Solution.**
  - Disable the **auto-deletion setting** on the cmdb10xadapter configuration. Use the job level **Allow Integration Job to delete removed Data** setting, and perform delta population to synchronize the CIs to be deleted.
  - Create the push job on source UCMDB server for the purpose of synchronizing the CI deletion.

## Limitations

- If the TQL query for a population job (defined on the source) includes CI types or links that do not exist on the target, or links that are not valid, those types or links are ignored in the target data repository.
- Since the UCMDB 9.x/10.x adapter works with the "changes" population engine, if a population

flow retrieves federated data, no removals are made in the CMDB, since the federation brings only added or updated data.

## Universal Discovery Troubleshooting and Limitations

This section describes general troubleshooting and limitations related to working with Data Flow Management.

- ["Troubleshooting – Universal Discovery" below](#)
- ["Limitations – Universal Discovery" on page 118](#)

### Note:

- For details on using log files to perform basic troubleshooting, see:
  - ["Data Flow Probe Log Files" on page 1](#)
  - ["UCMDB Log Files"](#) in the *Administer section of the UCMDB Help*

## Troubleshooting – Universal Discovery

- ["Discovery Results Do Not Appear in the Topology Map" on the next page](#)
- ["Triggers Running Unexpectedly in Management Zone" on the next page](#)
- ["Job Running Triggers Not Within Probe Limit" on the next page](#)
- ["Networks and IPs" on page 112](#)
- ["TCP Ports" on page 112](#)
- ["Discover Resources on a Windows XP Machine" on page 113](#)
- ["Trigger CIs for jobs in a management zone are in continuous "Progress" status" on page 113](#)
- ["Device attributes are not populating or contain unexpected or null values" on page 113](#)
- ["Inventory Discovery by Scanner job fails" on page 114](#)
- [Data push troubleshooting](#)

- [Test connection failed for UCMDB-UCMDB integration where one UCMDB uses SSL authentication for probes and the other does not](#)

## Discovery Results Do Not Appear in the Topology Map

**Problem.** Data that should have been discovered during the discovery process does not appear in the topology map.

**Verification.** The CMDB cannot retrieve the data or build the query results. Check the Discovery Results pane. If the CIs were not created, the problem is occurring during the Discovery process.

**Solution.** Check the error messages in the **probeMgr-services.log** file located in **C:\UCMDB\DataFlowProbe\runtime\logs**.

## Triggers Running Unexpectedly in Management Zone

**Problem:** There are triggers running in the Management Zone that should not be running.

**Reason:** Running triggers continue to run in the case where a Probe cluster is bound to the Management Zone, and the Probes in the cluster are removed from the cluster while the triggers are running.

**Solution:** To stop the triggers running, deactivate and then reactive the Management Zone.

## Job Running Triggers Not Within Probe Limit

**Problem:** A discovery job is running triggers that are not within its Probe limit.

**Indication:** Triggers are not released from a job in the following cases:

### Scenario 1

1. ProbeA and ProbeB belong to Cluster1.
2. **Range IPs by ICMP** is limited to run only on Cluster1. The job runs on both Probes in Cluster1.
3. ProbeB is removed from Cluster1.
4. In the next scheduled run of **Range IPs by ICMP**, you notice that the trigger is still running on both Probes in the cluster, even though ProbeB no longer belongs to Cluster1.

## Scenario 2

1. ProbeA is in Cluster1; ProbeB is under the Default Domain
2. **Range IPs by ICMP** is limited to run only on ProbeB.
3. ProbeB is added to Cluster1.
4. In the next scheduled run of **Range IPs by ICMP**, you notice that the trigger is still running on ProbeB, even though ProbeB now belongs to Cluster1.

**Solution.** Deactivate and then reactive the job.

## Networks and IPs

**Problem.** Not all networks or IPs have been discovered.

**Indication.** Not all the networks or IPs appear in the topology map results.

**Verification.** The IP address range in the Data Flow Probe Setup window does not encompass the scope of the networks or IPs that should have been discovered.

**Solution.** Change the scope of the Discovery range:

1. Select **Data Flow Management > Data Flow Probe Setup**.
2. Select the Probe and the range.
3. Change the IP address range in the Ranges box as required.

## TCP Ports

**Problem.** Not all TCP ports have been discovered.

**Indication.** Not all TCP ports appear in the topology map results.

**Verification.** Open the **portNumberToPortName.xml** file (**Data Flow Management > Adapter Management > DDM Infra > Configuration Files > portNumberToPortName.xml**), and search for the missing TCP ports.

**Solution.** Add the port numbers that should be discovered to the **portNumberToPortName.xml** file.



## Discover Resources on a Windows XP Machine

**Problem.** Failure to discover resources on a machine running on the Windows platform.

- **Solution 1. Start > Settings > Control Panel > System.** In the Remote tab, verify that the following check box is selected: **Allow users to connect remotely to this computer.**
- **Solution 2.** In Windows Explorer, select **Tools > Folder Options.** In the View tab, clear the **Use simple file sharing (Recommended)** check box.

## Trigger CIs for jobs in a management zone are in continuous "Progress" status

**Problem.** If you notice that trigger CIs for jobs in a management zone are in continuous "Progress" status, configure Data Flow Probe to ignore certain call home requests from the Universal Discovery Agent.

- **Solution.** To resolve this issue, change a parameter value as follows:
  - GlobalSettings.xml file
  - allowCallhomeInterval parameter
  - Default is 24.
  - Measured in hours that call home requests are ignored.
  - Allowable values are any integer greater than 0.

## Device attributes are not populating or contain unexpected or null values

**Problem.** If you notice that certain devices contain unexpected values or contain no values.

- **Solution.** To resolve this issue, run the Rulebase Support Report and send to Micro Focus Support for analysis. For more information, see *Modeling section of the UCMDB Help*.

## Inventory Discovery by Scanner job fails

**Problem.** If you notice that the Inventory Discovery by Scanner job fails.

**Indication.** The Communication log contains the following entry: "Step Wait XML Enricher Process execution failed."

**Solution.** If BDNA Normalize integration is enabled, troubleshoot BDNA Normalize operation using its documentation or contact BDNA support.

## Data push troubleshooting

- **How to get a view of the integrations**

To get a view of the integrations, run the following command:

```
SELECT ds.datastore as integration_point_name ,COUNT(*) as nbr_of_records
,ds.ds_id FROM SYNC_ID_MAP as ID, SYNC_DATASTORE as DS where id.ds_id =
ds.ds_id group by ds.datastore,ds.ds_id
```

- **Clear a given datastore by invoking the `removeIdMappingsOfDataStore` JMX method**

To clear a given datastore, you can invoke the **UCMDB:service=FCMDB Synchronizer Services** > **removeIdMappingsOfDataStore** JMX method.

**Caution:** Make sure you do it only when necessary.

For SM adapters, invoking the **removeIdMappingsOfDataStore** JMX method will resend all CIs, and then create duplicates.

However, in general it is useful for AM adapter and Generic Adapter, when there is assumption that the data push is corrupted.

## Test connection failed for UCMDB-UCMDB integration where one UCMDB uses SSL authentication for probes and the other does not

**Problem.** Test connection failed for UCMDB-UCMDB integration where one UCMDB uses SSL authentication for probes and the other does not.

**Solution.** The connection is built from the non-SSL authentication probe to the target UCMDB server that uses SSL authentication for probes. In this case, the target UCMDB server cert should be imported into the non-SSL probe truststore:

**<DataFlowProbe>\conf\security\ProbeTrustStore.jks** (the SSL configuration is included in **ssl.properties**)

For details about how to import the cert, see "Enable SSL with Server (One-Way) Authentication" in the *Hardening section of the UCMDB Help*.

## How to View the Status of AM and SM Integration Jobs

This task describes how to view the status of Asset Manager (AM) and Service Manager (SM) integration jobs. You need to perform the following steps on the Data Flow Probe JMX console.

1. On the probe machine, launch the web browser and enter the following address:

**https://localhost:8453**

You may have to log in with the user name (default: **sysadmin**) and password.

2. Click the **Data Flow Probe JMX** link.
3. Click the **Local\_<machine name or IP address> > type=IntegrationService** link.
4. Invoke one of the following methods according to your needs:
  - **forceRefreshAll**. This method loads the log files for both AM and SM integration jobs.
  - **listAMIntegrationJobByName**. This method loads the log files for AM integration jobs.
  - **listSMIntegrationJobByAdapterName**. This method loads the log files for SM integration jobs.

**Note:**

- If the total size of the log files that belong to the specified adapter is not bigger than the specified size, all these log files will be loaded. Otherwise, the method only loads the log files that are within the specified days and in total within the specified size.
- If you do not specify the adapter name, the method processes the log files of all adapters and apply the limitations for size and days similarly. For the **forceRefreshAll** method, the default values (200 MB and 7 days) are applied for AM and SM in this manner separately.
- If you do not specify the **Max log size** or **Max days of log history** field, these default values are applied respectively: 200 (MB), 7 (days). The maximum values for these fields are 200 (MB) and 30 (days). If you specify a larger value, the maximum value will be applied. The default values can be modified in the **integrationProgressLog.properties** file under the **<Probe\_installation\_folder>\conf\integration\_progress\**.
- You must invoke one of these methods before you can successfully invoke the methods in the following step. Additionally, in the result of this method, you can see the values of **Index** and **Query name**, which are the required parameters of the methods in the following step.

5. Go back and invoke one of the following methods according to your needs:

Method	Description
<b>getSMIntegrationJobDetails</b>	This method displays the detailed information of the SM integration job that has the specified index.  You must invoke <b>listSMIntegrationJobByAdapterName</b> or <b>forceRefreshAll</b> in the previous step.
<b>getAMIntegrationJobDetailsByName</b>	This method displays the detailed information of the AM integration job that has the specified query name and index.  You must invoke <b>listSMIntegrationJobByAdapterName</b> or <b>forceRefreshAll</b> in the previous step.
<b>getAMIntegrationJobDetails</b>	This method displays the detailed information of the AM integration job that has the specified index.  You must invoke <b>listSMIntegrationJobByAdapterName</b> or <b>forceRefreshAll</b> in the previous step.

**Note:**


- In the **Index** field, you can only specify an index number that is returned in Step 4. Otherwise, these methods will result in an error.
- If you do not invoke any method in Step 5 in 20 minutes, the log files loaded in Step 4 will be cleared from memory. After that, you have to perform Step 4 again.

## How to View the Integration Point Log

From the UCMDB UI, you can directly view the integration point log, which is stored in one of the following locations:

- The **DataFlowProbe\runtime\log** folder of the associated Data Flow Probe, if the integration point uses a Data Flow Probe.
- The **UCMDBServer\integrations\runtime\log** folder of the UCMDB Server, If the integration point uses the UCMDB Integration Service.

To view the integration point log, follow these steps:

1. Go to **Data Flow Management > Integration Studio**.
2. Select the integration point from the **Integration Point** pane.
3. Click the **View Integration Point Log**  button.

### Note:

- If the associated Data Flow Probe or the UCMDB Integration Service is disconnected, an error occurs and you cannot view the log.
- This functionality tries to read the log file that has the name as **fcmdb.adapters.<integration\_point\_name>**. However, certain integration points (for example, the integration point for Micro Focus NNMi) do not have logs with such a name. In this scenario, an empty log will be returned.

## Limitations – Universal Discovery

- When Discovery is installed on a non-English operating system, names of modules, Management Zones, and jobs are limited to English characters (a-z; A-Z).
- When naming entities in Data Flow Management , you can use the following characters:
  - **Modules:** a-z, A-Z, 0-9, hyphen (-), underscore (\_), space ( ), and forward slash (/).
  - **Management Zones:** a-z, A-Z, 0-9, hyphen (-), underscore (\_), and space ( ).
  - **Jobs:** a-z, A-Z, 0-9, hyphen (-), underscore (\_), and space ( ).
  - Names can be a maximum length of 50 chars and MUST NOT start with a digit.
- When entering IP addresses, use only digits and asterisks (\*)
- Each Content Pack installation overrides all out-of-the-box resources with the contents of that Content Pack. This means that any changes you made to these resources are lost. This applies to the following resources: Queries, Views, Enrichments, Reports, Discovery Jython scripts, Discovery adapters, Discovery jobs, Discovery resources, Discovery configuration files, Discovery modules, CI Types, and Relationships. (Attributes added to CI Types and Relationships are not overridden).

## Inventory Discovery Troubleshooting

This chapter includes:

How to view all information related to a device in a centralized view? .....	119
How to troubleshoot network availability and latency issue related to a device? .....	120
How to check the key indexes of the discovery history information for a discovered device? .....	126
How to check device related logs for a discovered device? .....	132
How to invoke discovery job relevant to the discovered device manually and check status to identify potential discovery errors? .....	134
How to check which pattern (management zone) is used in the discovery for a discovered device? .....	144
How to check detailed discovery settings used in the discovery for a discovered device? .....	146
How to check the SNMP credentials used in the discovery for a discovered device? .....	149

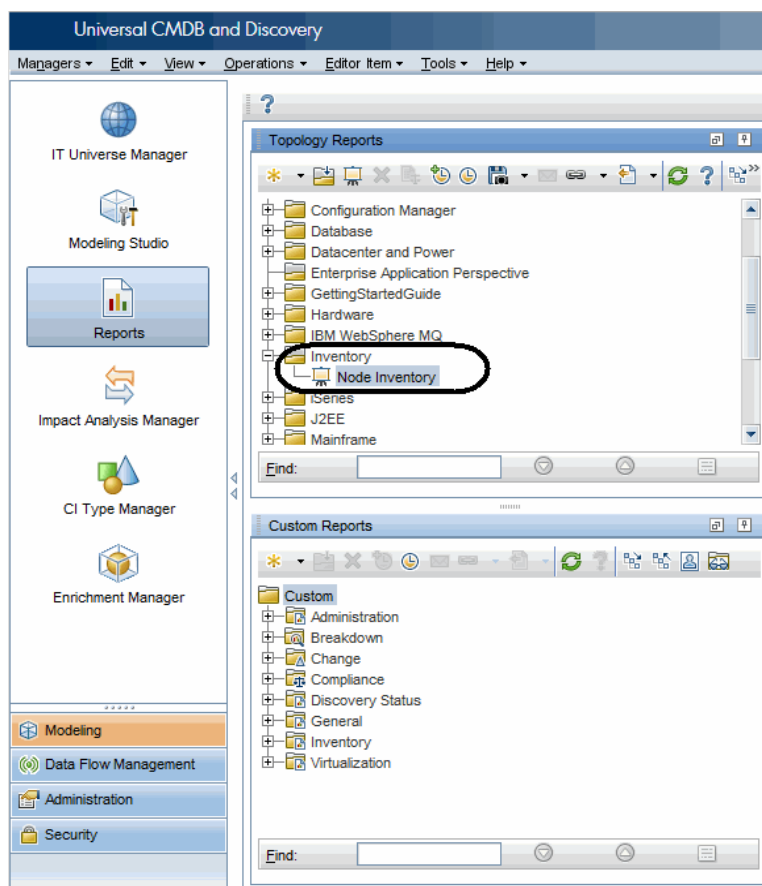
How to View Discovery Status and Errors for a Selected CI from the Discovery Progress Widget .....	151
--	-----

## How to view all information related to a device in a centralized view?

**Question: How can I view all relevant information to a device in a centralized view?**

To view all information related to a device in a centralized view,

1. Select **Modeling > Reports**.
2. In the Topology Reports pane, expand **Inventory > Node Inventory**.






















3. Double-click **Node Inventory** or right-click it and select **Open Report**.

The Node Inventory report opens in the right pane.

4. Do either of the following to view device details:

- Select a specific CI in the right pane and drill down to view more details. Or,
- Export the report to PDF, so that you can view all details in grid view. To do so,
  - i. Right-click **Node Inventory**, select **Export Report > Export to PDF** from the context menu.
  - ii. In the Export dialog box, specify file location and file name for the target PDF file.
  - iii. Click **Export**.
  - iv. Click **Yes** when prompted whether you want to open the PDF file now.

The exported PDF file opens, displaying all details in grid view.

Universal CMDB: Per Device Information Topology Report																	
Display Label	Discovered Location	Discovered Vendor	Discovered Model	Serial Number	BusAsset Tag	Bus Version	Bus Serial Number	Chassis Type	Discovered OS Vendor	Discovered OS Name	Node Operating System Release	Discovered OS Version	Node Operating System Installation type	Last Access Time	Last Modified Time	Count	CPU V
 RAM 8GB #12														Tue Dec 9 2014 03:54 PM CST	Tue Dec 9 2014 03:54 PM CST		
 RAM 8GB #13														Tue Dec 9 2014 03:54 PM CST	Tue Dec 9 2014 03:54 PM CST		
 Processor		VMware, Inc.	VMware Virtual Platform	VMware43 13 14 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 52 53 54 55 56 57 58 59 60 61 62 63 64 65 66 67 68 69 70 71 72 73 74 75 76 77 78 79 80 81 82 83 84 85 86 87 88 89 90 91 92 93 94 95 96 97 98 99 100	VMware43 13 14 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 52 53 54 55 56 57 58 59 60 61 62 63 64 65 66 67 68 69 70 71 72 73 74 75 76 77 78 79 80 81 82 83 84 85 86 87 88 89 90 91 92 93 94 95 96 97 98 99 100	INTEL - 6040000		Other	Microsoft	Windows 2008 R2	7601	6.1.7601	Server Enterprise	Sun Dec 14 2014 06:04 PM CST	Wed Dec 10 2014 05:33 PM CST		
 CPU														Tue Dec 9 2014 03:54 PM CST	Tue Dec 9 2014 03:54 PM CST	1	
 Disk														Tue Dec 9 2014 03:54 PM CST	Tue Dec 9 2014 03:54 PM CST		Gen
 Disk Drive														Tue Dec 9 2014 03:54 PM CST	Tue Dec 9 2014 03:54 PM CST	3	
 Harddisk														Tue Dec 9 2014 03:54 PM CST	Tue Dec 9 2014 03:54 PM CST		
 Harddisk (Intel(R) VMware IDE Controller)														Tue Dec 9 2014 03:54 PM CST	Tue Dec 9 2014 03:54 PM CST		
 Virtual disk_0														Tue Dec 9 2014 03:54 PM CST	Tue Dec 9 2014 03:54 PM CST		
 Graphics Adapter														Tue Dec 9 2014 03:54 PM CST	Tue Dec 9 2014 03:54 PM CST	1	
 Graphics Adapter (VMware IDE Controller)														Tue Dec 9 2014 03:54 PM CST	Tue Dec 9 2014 03:54 PM CST		
 Hardware Board														Tue Dec 9 2014 03:54 PM CST	Tue Dec 9 2014 03:54 PM CST	5	
 Hardware Board (VMware IDE Controller)														Tue Dec 9 2014 03:54 PM CST	Tue Dec 9 2014 03:54 PM CST		
 Bus Master (IDE Controller)														Tue Dec 9 2014 03:54 PM CST	Tue Dec 9 2014 03:54 PM CST		
 Network Controller														Tue Dec 9 2014 03:54 PM CST	Tue Dec 9 2014 03:54 PM CST		
 Network Controller (Intel(R) PRO/1000 MT Network Connection)														Tue Dec 9 2014 03:54 PM CST	Tue Dec 9 2014 03:54 PM CST		
 Disk Drive														Tue Dec 9 2014 03:54 PM CST	Tue Dec 9 2014 03:54 PM CST		
 Disk Drive (Intel(R) SAS-3000 series, 6-port with 10Gb)														Tue Dec 9 2014 03:54 PM CST	Tue Dec 9 2014 03:54 PM CST		
 Disk Drive (VMware IDE Controller)														Tue Dec 9 2014 03:54 PM CST	Tue Dec 9 2014 03:54 PM CST		

2014-12-15 14:42 PM

For more information about the topology report, see the *Modeling section of the UCMDB Help*.

## How to troubleshoot network availability and latency issue related to a device?

**Question: How should I troubleshoot network availability and latency issue related to a device?**

You can troubleshoot network availability and latency issue related to a device in the following ways:

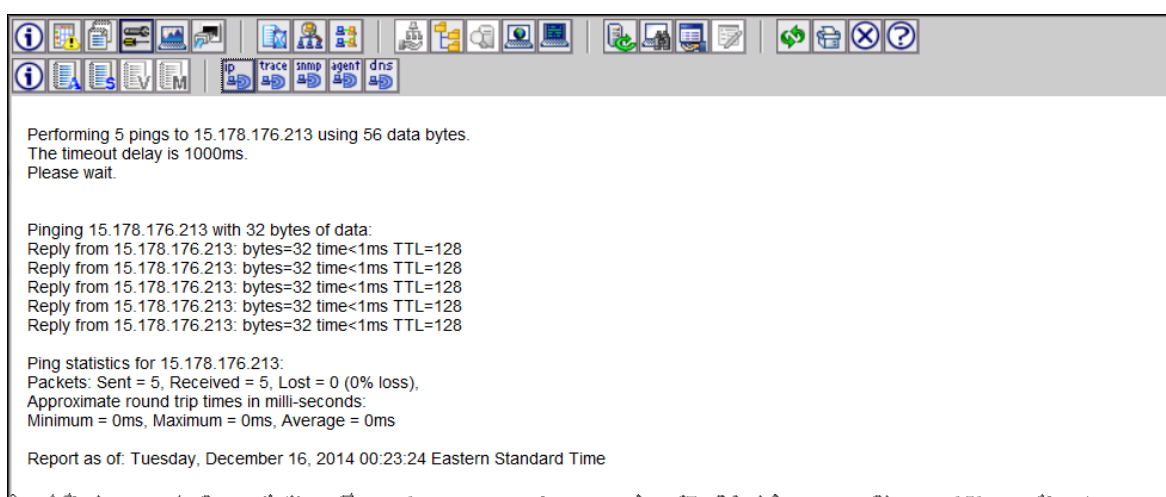


- [IP Ping and Agent Ping](#)
- [SNMP Ping](#)
- [Tracert and DNS Query](#)

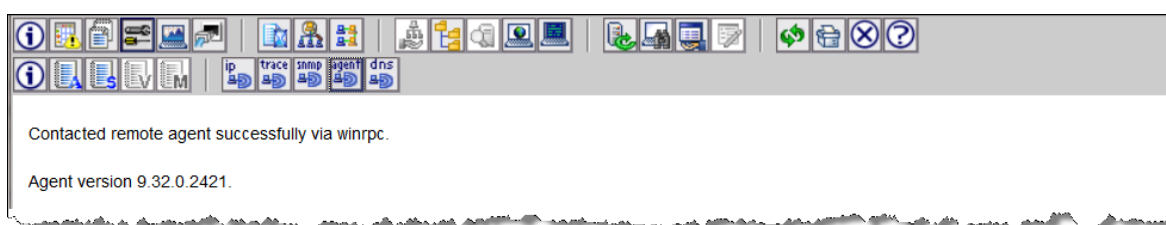
## IP Ping and Agent Ping

In DDMi, you can use IP ping and agent ping.

Result of the IP ping looks similar to the following:



Result of the agent ping looks similar to the following:

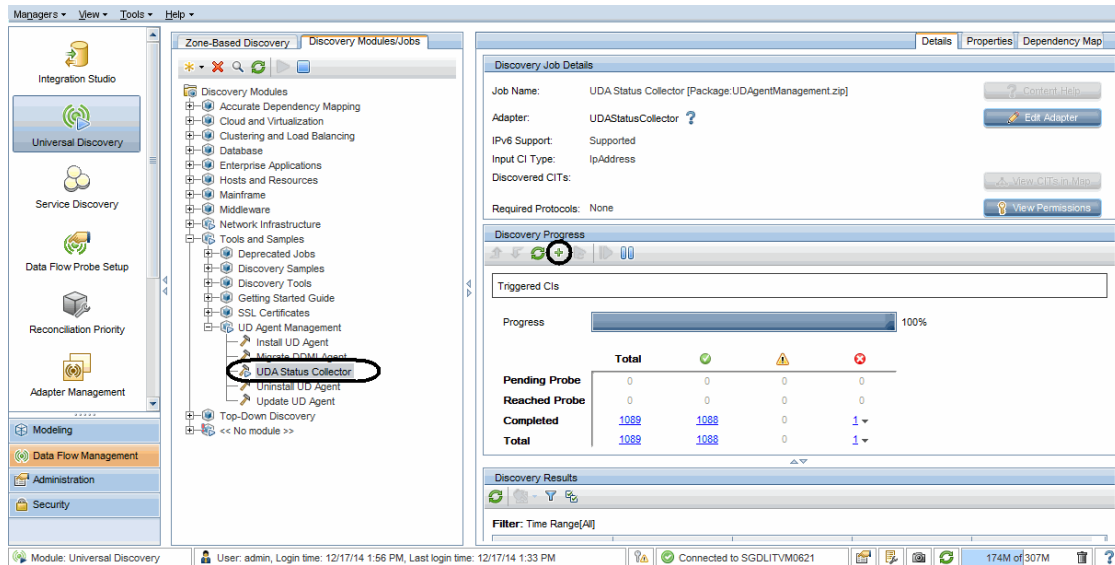




In UD, you can use also use IP ping and agent ping via the UDA Status Collector job.

To use IP ping and agent ping

1. In UCMDB, go to **Data Flow Management > Universal Discovery > Discovery Modules/Jobs** tab.

2. In the Discovery Modules tree, select **Tools and Samples > UD Agent Management > UDA Status Collector**.
3. If the UDA Status Collector job is not activated, right-click **UDA Status Collector**, and select **Activate**.



4. In the Discovery Progress pane, click the **Add CI**  button.
5. In the Choose CIs to Add dialog box, select the IP address of your interest, and click the **Add**  button.

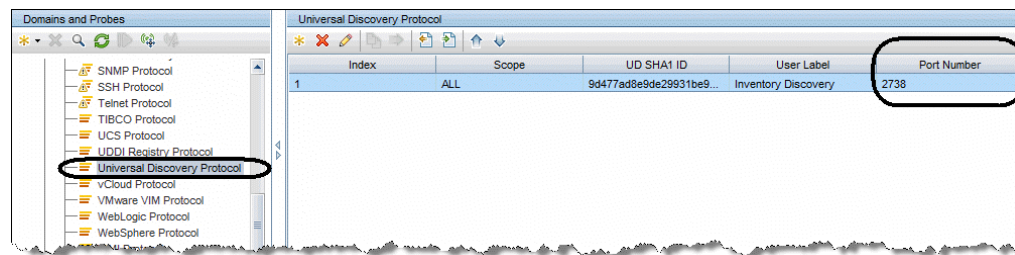
The UDA Status Collector job will ping using IP and agent port to check.

**Note:** Agent port can be found in the **Port Number** parameter value of the Universal Discovery Protocol credential. This is a default parameter in the protocol, and is applied to all agent connections using this protocol.

To view the agent port,

- a. In the Data Flow Management module, go to **Data Flow Probe Setup**.
- b. In the Domains and Probes tree, select a domain of your interest and expand the **Credentials** node, and then select **Universal Discovery Protocol**.
- c. In the Universal Discovery Protocol credentials displayed in the right pane, check the

value for the **Port Number** column.



6. Click the **Close** button to exit the Choose CIs to Add dialog box.

To view the IP ping and agent ping result

1. Access the JMX console on the Data Flow Probe machine by launching the Web browser and enter the following address:

**https://localhost:8453/**

You may have to log in with the user name **sysadmin** and password.

2. Locate the **exportUdaStatus** operation to invoke.

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

Invoke

### exportJobsExecutionTimelineXML

*Export the job execution history time line as xml file to be used by Excel*

Name	Type	Value	Description
groupByCycle	boolean	<input checked="" type="radio"/> True <input type="radio"/> False	

Invoke

Invoke

### exportUdaStatus

*Export UDA Status to CSV*

Name	Type	Value	Description
path	java.lang.String	c:\udastatus	

Invoke

### resumeNowWorkflowJobOnDestination

*resumes a workflow trigger ci that is currently in the state of parking*

Name	Type	Value	Description
jobId	java.lang.String		

- Provide a folder name in the **Value** field.

- Click **Invoke** to run the operation.

The UDA status is exported to a CVS file.

- Open the exported CSV file to view details of the result from the UDA Status Collector job.

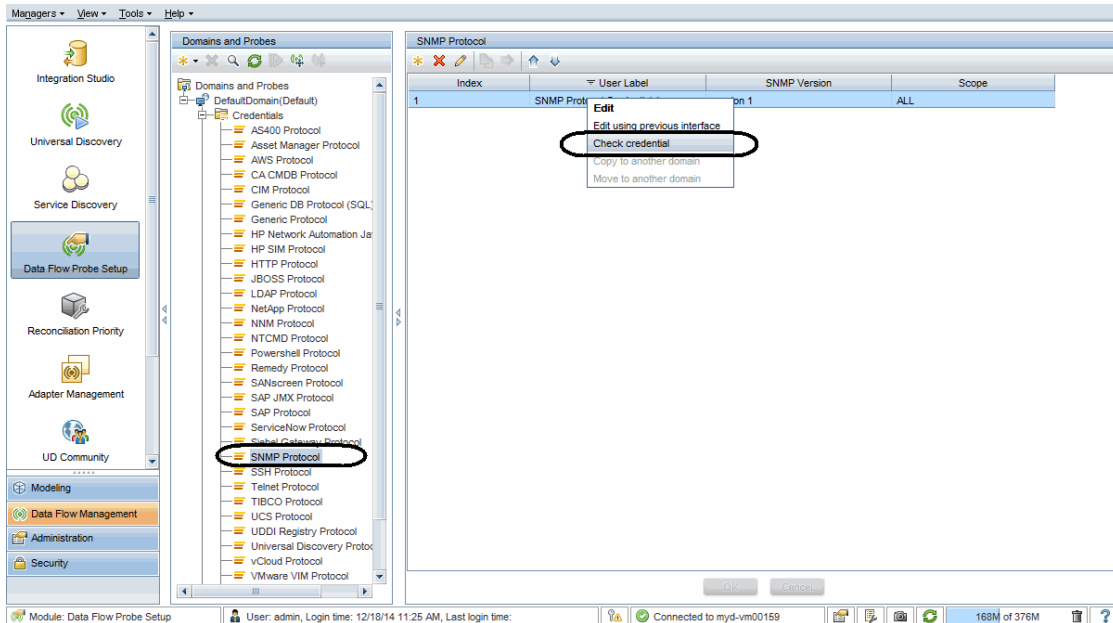
The CSV file shows status details similar to the following:

ipaddress	computerName	alive	portAlive	isDDMI	isWin	osType	agentVersion	UDUniqueid	isNative
16.60.169.33	myd-vm11101.hpswl-abs.adapps.hp.com	TRUE	TRUE	FALSE	FALSE	Linux	v10.20.000 build:346	73a911c4-b0fa-4e10-2047-b270e5a0cb18	TRUE

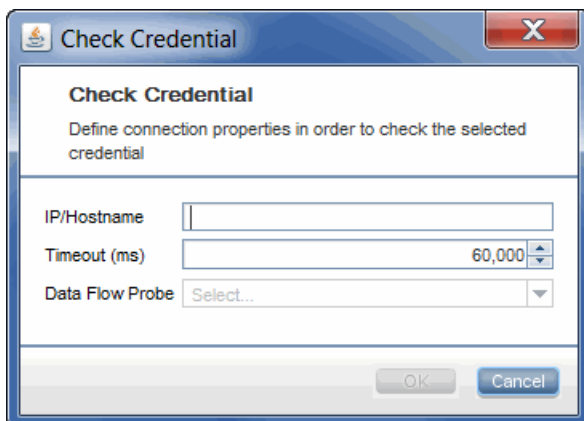
## SNMP Ping

To run SNMP ping in UDI,

1. In the Data Flow Management module, go to **Data Flow Probe Setup**.
2. In the Domains and Probes tree, expand the **Credentials** node, and select **SNMP Protocol**.  
All SNMP credentials are displayed in the right pane.
3. Right-click the SNMP credential you want to use to run SNMP ping, and select **Check credential** from the pop-up menu.



4. In the Check Credential dialog box, specify the host name or IP address (in IPv4/IPv6 format) of the remote machine on which you want the protocol to run SNMP ping, specify a connection timeout (in milliseconds), and select the probe to use.



5. Click **OK**.

The result returns soon.

## Tracert and DNS Query

Currently UD does not have such functionalities as DDMi did.

## How to check the key indexes of the discovery history information for a discovered device?

**Question: For a discovered device, how should I check the key indexes of the discovery history information? For example, when was the device first discovered? When was it last seen?**

To answer this question, let's take a look at the information available from DDMi first:

DDMi Parameter	Value
First discovered:	3 weeks 5 days 0 hours ago at: Wednesday, November 19, 2014 20:20:45 Eastern Standard Time
Added to map:	3 weeks 5 days 0 hours ago at: Wednesday, November 19, 2014 20:48:51 Eastern Standard Time
Last seen:	2 minutes 1 second ago at: Monday, December 15, 2014 21:06:55 Eastern Standard Time in ping or poll by DDM Inventory
Last moved:	3 weeks 5 days 0 hours ago at: Wednesday, November 19, 2014 20:50:47 Eastern Standard Time
Agent last contacted:	1 day 17 hours 7 minutes ago at: Sunday, December 14, 2014 04:01:01 Eastern Standard Time
Agent upgrade time:	2 weeks 6 days 1 hour ago at: Tuesday, November 25, 2014 19:56:04 Eastern Standard Time
Scanner model last updated:	2 weeks 6 days 0 hours ago at: Tuesday, November 25, 2014 20:12:35 Eastern Standard Time
Device last modeled as an unmanaged device:	3 hours 12 minutes 6 seconds ago at: Monday, December 15, 2014 17:56:50 Eastern Standard Time
Device last replied to ICMP during modeling:	2 weeks 3 days 21 hours ago at: Thursday, November 27, 2014 23:12:44 Eastern Standard Time

DDMi Parameter	Value
Mean break diagnosis time:	2 minutes (major alarm)
Agent platform:	Windows (x86)
Agent port number:	2738
Agent version:	10.20.000.346
AUM agent upgrade state:	No AUM agent
Workflow type:	Agent
Scanner version:	9.32.000.2421
Scanner configuration:	<default_delta>
Scan file location:	https://15.155.155.155/nm/scans/QASERVER1_005056B81459.xsf
Scan type:	HP Discovery and Dependency Mapping Inventory
Scan CRC:	295532891
Scan modification time:	2014-11-25 22:47:26
Mean device modeler update run time:	4 minutes 52 seconds
Recent device modeler update run times:	4 minutes 48 seconds, 4 minutes 17 seconds, 6 minutes 32 seconds, 3 minutes 53 seconds
Rulebase id:	266305

In Universal Discovery, you can find similar attributes for most of DDMi parameters as shown in the table below:

DDMi Parameter	Corresponding Attributes in UD
First discovered:	<b>Create Time</b> attribute (of the <b>node CI</b> )
Added to map:	N/A
Last seen:	<b>Last Access Time</b> attribute (of the <b>node CI</b> )
Last moved:	N/A
Agent last contacted:	<b>Last Access Time</b> attribute (of the <b>UDA CI Type</b> )
Agent upgrade time:	<b>LastModifiedTime</b> attribute (of the <b>UDA CI Type</b> )
Scanner model last updated:	<b>LastModifiedTime</b> attribute (of the <b>InventoryScanner CI Type</b> )



DDMi Parameter	Corresponding Attributes in UD
Device last modeled as an unmanaged device:	N/A
Device last replied to ICMP during modeling:	N/A
Mean break diagnosis time:	N/A
Agent platform:	<b>Platform</b> attribute (of the <b>UDA</b> CI Type)
Agent port number:	<b>Application Listening Port Number</b> attribute (of the <b>UDA</b> CI Type)
Agent version:	<b>Version</b> attribute (of the <b>UDA</b> CI Type)
AUM agent upgrade state:	N/A
Workflow type:	N/A
Scanner version:	<b>Version</b> attribute (of the <b>InventoryScanner</b> CI Type)
Scanner configuration:	<b>ScannerConfiguration</b> attribute (of the <b>InventoryScanner</b> CI Type)
Scan file location:	<b>ProcessedScanFilePath</b> attribute (of the <b>InventoryScanner</b> CI Type)
Scan type:	<b>Scan Type</b> attribute (of the <b>InventoryScanner</b> CI Type)
Scan CRC:	N/A
Scan modification time:	<b>Last Access Time</b> or <b>Scan File Last Downloaded Time</b> attribute (of the <b>InventoryScanner</b> CI Type)
Mean device modeler update run time:	N/A
Recent device modeler update run times:	<b>Scan Duration</b> attribute (of the <b>InventoryScanner</b> CI Type)
Rulebase id:	N/A

**Note:** "N/A" indicates that there is no corresponding attribute in UD now.

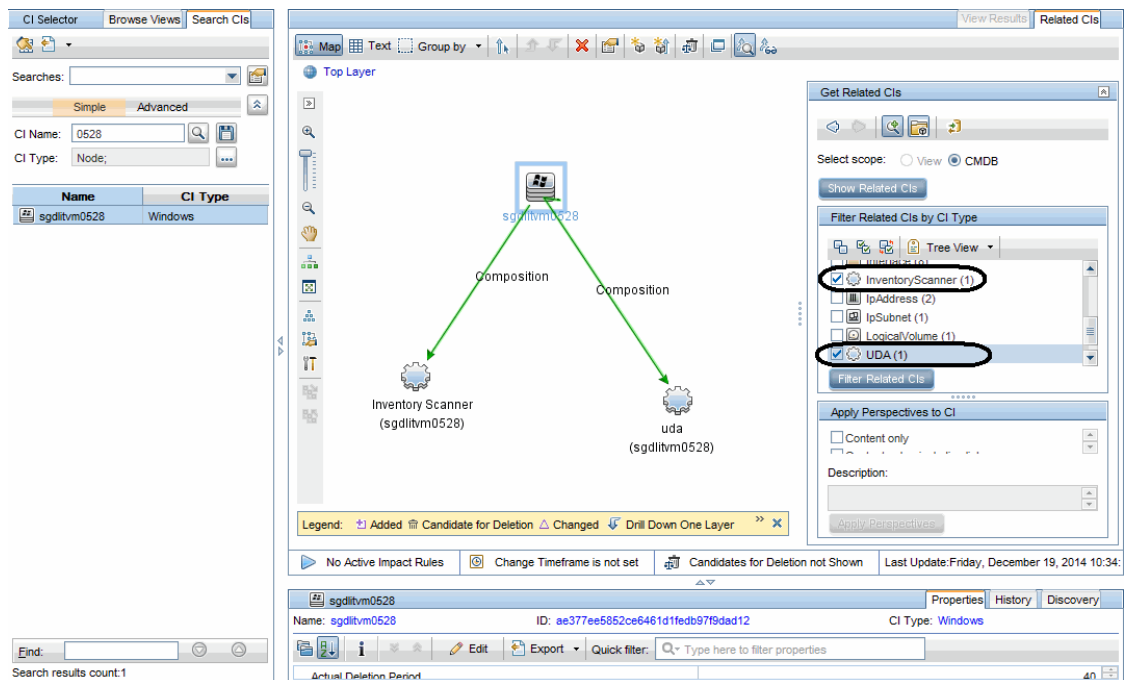
To check similar information in UD,

1. In UCMDB, go to **Modeling > IT Universal Manager**.
2. In the CI Selector pane, go to the **Search CIs** tab.
3. In the Simple search mode, search for a CI of Node CI type.



- a. In the **CI Name** field, enter a keyword to search, for example, **0528**.
  - b. For the **CI Type** field, click , locate and select the **Node** CI type.
  - c. Click .
4. Click the node CI in the search result list.  
The node CI map displays in the Related CIs pane.
  5. In the Filter Related CIs by CI Type sub-pane, locate and select **Inventory Scanner** and **UDA** CI types, then click **Filter Related CIs**.

The Related CIs map refreshes.



The screenshot displays the CMS interface with the following components:

- CI Selector:** Shows search results for "sgdlitm0528" with CI Type "Windows".
- Map View:** A hierarchical diagram showing "sgdlitm0528" at the top, connected by "Composition" relationships to "Inventory Scanner (sgdlitm0528)" and "uda (sgdlitm0528)".
- Filter Related CIs by CI Type:** A pane on the right with checkboxes for "InventoryScanner (1)" and "UDA (1)", both of which are checked and circled. Below this is a "Filter Related CIs" button.
- CI Details:** At the bottom, the details for "sgdlitm0528" are shown, including its ID "ae377ee5852ce6461d1fedb97f9dad12" and CI Type "Windows".

6. Click the **uda** or **Inventory Scanner** CI icon in the map.  
In the CI Details pane below the map, check attributes that correspond to DDMI parameters.  
The highlighted **uda** attributes in the screenshot below correspond to similar DDMI parameters.

uda (sgdlitvm0528)		Properties	History	Discovery
Name: uda (sgdlitvm0528)		ID: b4d11b46f879822f59d86b66dfc3a98c		CI Type: UDA
		Quick filter: <input type="text" value="Type here to filter properties"/>		
Actual Deletion Period				40
Allow CI Update	True			
Application Category				
Application Installed Path				
Application IP	16.187.190.28			
Application IP Routing Domain	DefaultDomain			
Application IP Type	IPv4			
Application Listening Port Number				2738
Application Timeout				
Application Username				
Application Version Description				
Architecture	amd64			
classification				
Container name	(sgdlitvm0528)			
Create Time	Thu Dec 18 2014 03:08 PM GMT+08:00			
Created By	UCMDBDiscovery: Host Connection by Shell			
Deletion Candidate Period				20
Description				
DiscoveredProductName	uda			
Display Label	uda (sgdlitvm0528)			
Edition				
Enable Aging	True			
Global Id	b4d11b46f879822f59d86b66dfc3a98c			
Is Candidate For Deletion	False			
Last Access Time	Thu Dec 18 2014 11:57 PM GMT+08:00			
LastModifiedTime	Thu Dec 18 2014 11:57 PM GMT+08:00			
layer	software			
Name				
Note				
Origin				
Platform	windows			
ProductName				
Reference to the OS credentials dictionary entry	NA			
StartupTime				
Updated By	Enrichment: Enrichment's rule: SoftwareElementDisplayLabel...			
User Label				
Vendor				
Version	v10.20.000 build:364			

The highlighted **Inventory Scanner** CI attributes in the screenshot below correspond to similar DDMi parameters.

Inventory Scanner (sgdlitvm0528)		Properties	History	Discovery
Name: Inventory Scanner (sgdlitvm0528)		ID: 00601fdc3845ee3a50e5b148618e8be3	CI Type: InventoryScanner	
		Quick filter: <input type="text" value="Type here to filter properties"/>		
Actual Deletion Period	40			
Allow CI Update	True			
Application Category				
Application Installed Path				
Application IP				
Application IP Routing Domain				
Application IP Type	IPv4			
Application Listening Port Number				
Application Timeout				
Application Username				
Application Version Description				
classification				
Container name	(sgdlitvm0528)			
Create Time	Thu Dec 18 2014 03:51 PM GMT+08:00			
Created By	UCMDBDiscovery: Inventory Discovery by Scanner			
Deletion Candidate Period	20			
Description	Hardware-only Inventory Scanner			
DiscoveredProductName	Inventory Scanner			
Display Label	Inventory Scanner (sgdlitvm0528)			
Edition				
Enable Aging	True			
FilesProcessed	0			
FilesRecognized	0			
FilesTotal	0			
Global Id	00601fdc3845ee3a50e5b148618e8be3			
Is Candidate For Deletion	False			
Last Access Time	Thu Dec 18 2014 11:57 PM GMT+08:00			
LastModifiedTime	Thu Dec 18 2014 11:57 PM GMT+08:00			
layer	software			
Name				
Note				
Origin				
ProcessedScanFilePath	C:\hp\UCMDB\DataFlowProbe\runtime\xmlenricher\Scans\pr...			
ProcessedScanFileProbe	DataFlowProbe			
ProductName				
root_iconproperties				
Scan File Last Downloaded Time	Thu Dec 18 2014 03:49 PM GMT+08:00			
ScanDuration	1			
ScannerCommandLine	-cfg:scan.cxz -l:local.xsf -appliance			
ScannerConfiguration	_hwnonly.cxz			
* ScannerType	WINDOWS_X64			
StartupTime	Thu Dec 18 2014 10:13 AM GMT+08:00			
Updated By	Enrichment: Enrichment's rule: SoftwareElementDisplayLabel...			
Upgrade Date	Thu Dec 18 2014 03:43 PM GMT+08:00			
User Label				
Vendor				
Version	10.20.000 build 364			

## How to check device related logs for a discovered device?

**Question: For a discovered device, where should I check the device related logs? Such as agent deployment log, scanner deployment log, virtualization log, and so on.**


The following sections provide details about checking device related log in Universal Discovery.

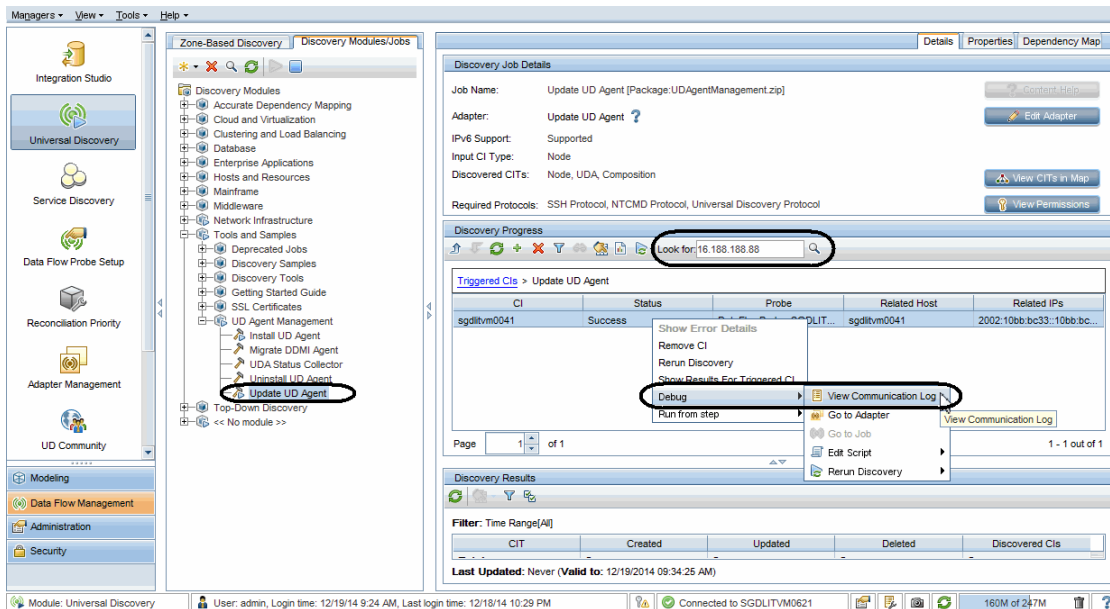
- [Agent deployment log](#)
- [Scanner deployment log](#)
- [Virtualization log](#)

### Agent deployment log

The agent related action record (the Install UD Agent job and the Update UD Agent job) can be found in the Communication Log.

To view communication log for agent related jobs,

1. In UCMDB, go to **Data Flow Management > Universal Discovery > Discovery Modules/Jobs** tab.
2. In the Discovery Modules tree, select **Tools and Samples > UD Agent Management > Install UD Agent** (or **Update UD Agent**).
3. Right-click **Install UD Agent** (or **Update UD Agent**), select **Activate** from the context menu if the job is not activated, and wait for the Triggered CIs list to refresh.
4. In the Triggered CIs list in the Discovery Progress pane, click a number with link.
5. In the **Look for** field that is just enabled, enter the IP address for the target agent and click .
6. Right-click the returned entry, and from the context menu, select **Debug > View Communication Log**.




7. In the communication log that opens,
  - search **Step [Install Agent]** as keyword to locate the log entry where probe starts the agent installation
  - search **Step [Check Agent Installed]** as keyword to locate the log entry that indicates whether the agent is installed

## Scanner deployment log

The Inventory Discovery by Scanner job related action record (the Install UD Agent job and the Update UD Agent job) can be found in the Communication Log.

To view communication log for scanner deployment related jobs,

1. In UCMDB, go to **Data Flow Management > Universal Discovery > Discovery Modules/Jobs** tab.
2. In the Discovery Modules tree, select **Hosts and Resources > Inventory Discovery > Inventory Discovery by Scanner**.
3. Right-click **Inventory Discovery by Scanner**, select **Activate** from the context menu if the job is not activated, and wait for the Triggered CIs list to refresh.

4. In the Triggered CIs list in the Discovery Progress pane, click a number with link of your interest.
5. In the **Look for** field that is just enabled, enter the IP address for the scanner and click .
6. Right-click the returned entry, and from the context menu, select **Debug > View Communication Log**.
7. In the communication log that opens,
  - search **Step [Run Scanner]** as keyword to locate the log entry where the probe starts running the scanner
  - search **Step [Download Scan File]** as keyword to locate the log entry that indicates the probe starts downloading the scan file

## Virtualization log

This log is not frequently used in DDMI. However, in UD, the Communication Log for the following jobs can provide you detailed logs about virtualization environments:

- VMware ESX Connection by VIM job
- VMware vCenter Connection by VIM job

## How to invoke discovery job relevant to the discovered device manually and check status to identify potential discovery errors?

**Question: For a discovered device, to identify any potential discovery errors, how should I invoke discovery job relevant to the device manually, and check the progress/on-going status of the discovery?**

In DDMI, if you find any error in the discovery result, you can run the DDMI jobs in an ad-hoc way. In UD, similar jobs are available to provide similar functionalities.


The table below describes DDMI jobs and the corresponding UD jobs that can be run in an ad-hoc way:

DDMi Job	UD Job
Deploy Agent	<a href="#">Install UD Agent</a>
Upgrade Agent	<a href="#">Update UD Agent</a>
Run Scanner	<a href="#">Run Scanner</a>
Retrieve Scan File	<a href="#">Download Scan File</a>
Uninstall Agent	<a href="#">Uninstall UD Agent</a>
Run Agentless Scanner	<a href="#">Run Agentless Scanner</a>
Enrich XML	<a href="#">Parse Enriched Scan File</a>
Run Rulebase	The normalization functionality is included the <a href="#">Rerun Discovery</a> option for each job
Run VMware Discovery	<a href="#">VMware discovery jobs</a>

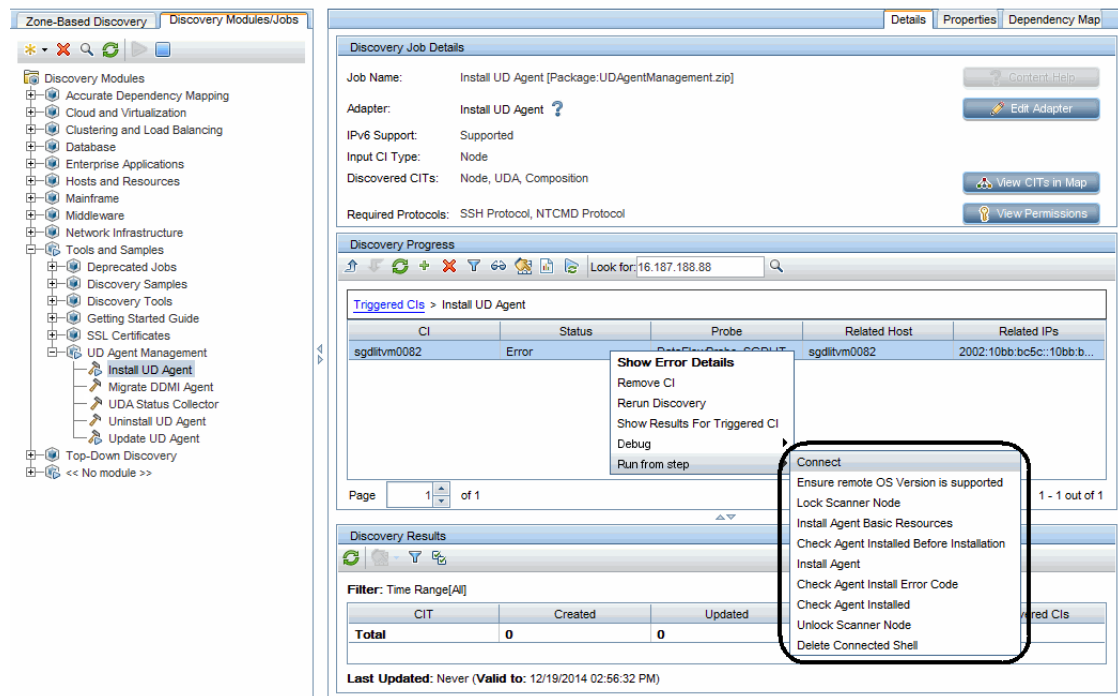
For details, click the UD job of your interest in the table above.

## Install UD Agent

To invoke discovery job relevant to the device manually,

1. In UCMDB, go to **Data Flow Management > Universal Discovery > Discovery Modules/Jobs** tab.
2. In the Discovery Modules tree, select **Tools and Samples > UD Agent Management > Install UD Agent**.
3. Right-click **Install UD Agent**, select **Activate** from the context menu if the job is not activated, and wait for the Triggered CIs list to refresh.
4. In the Triggered CIs list in the Discovery Progress pane, click a number with link.
5. In the **Look for** field that is just enabled, enter the IP address for the target device and click .
6. Right-click the returned entry, and from the context menu, select **Run from step > <Select an**

action>.



To check the progress/on-going status of the discovery job,

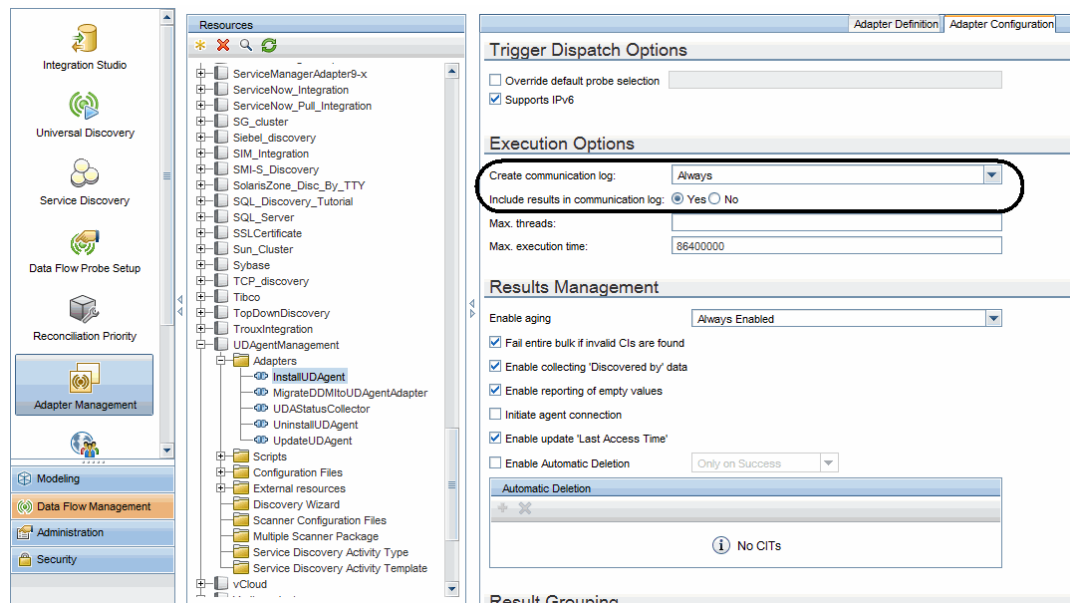
1. Modify the adapter's configuration to make sure that the communication log is always created.

In this case, modify the Install UD Agent adapter's configuration.

- a. In the Data Flow Management module, go to **Adapter Management**.
- b. In the Resources pane, expand **UDAgentManagement > Adapters > InstallUDAgent**.
- c. In the right pane, click the **Adapter Configuration** tab.
- d. In the Execution Options section, set the following:
  - **Create communication log: Always**



- **Include results in communication log: Yes**




2. Return to the Universal Discovery window, right-click the returned entry, from the context menu, select **Debug > View Communication Log**

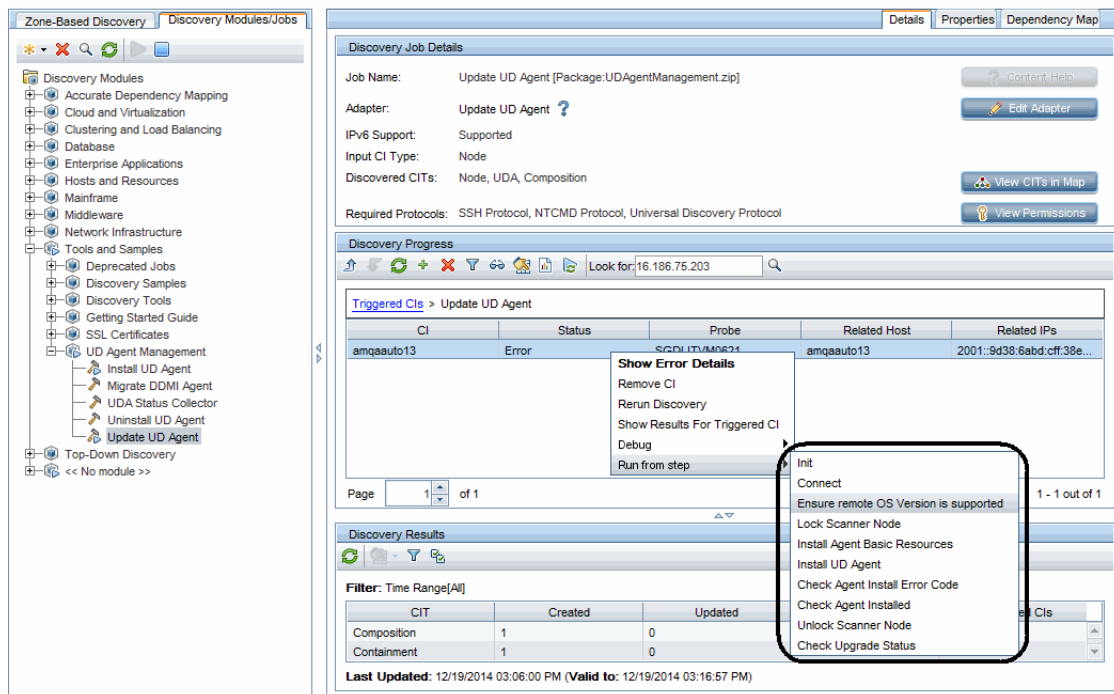
For details, see ["How to check device related logs for a discovered device?"](#) on page 132.

## Update UD Agent

To invoke discovery job relevant to the device manually, and check progress and status of the discovery job:

1. In UCMDB, go to **Data Flow Management > Universal Discovery > Discovery Modules/Jobs** tab.
2. In the Discovery Modules tree, select **Tools and Samples > UD Agent Management > Update UD Agent**.

3. Right-click **Update UD Agent**, select **Activate** from the context menu if the job is not activated, and wait for the Triggered CIs list to refresh.
4. In the Triggered CIs list in the Discovery Progress pane, click a number with link.
5. In the **Look for** field that is just enabled, enter the IP address for the target device and click .
6. Right-click the returned entry, and from the context menu, select **Run from step > <Select an action>**.



7. To check the progress/on-going status of the discovery job,
  - a. Modify the Update UD Agent adapter's configuration to make sure that the communication log is always created.


For detailed instructions, see ["To check the progress/on-going status of the discovery job," on page 136.](#)

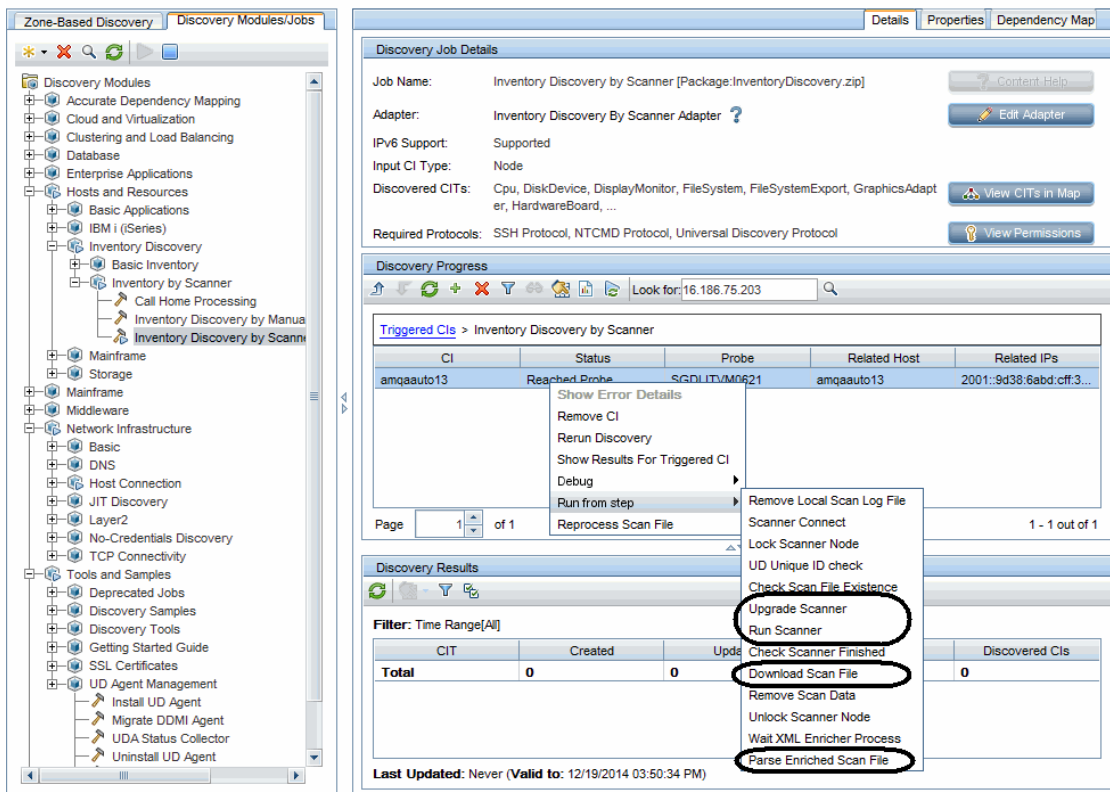
- b. Right-click the returned entry in the Discovery Progress pane, from the context menu, select **Debug > View Communication Log**.

For details, see ["How to check device related logs for a discovered device?" on page 132.](#)

## Upgrade Scanner / Run Scanner / Download Scan File / Parse Enriched Scan File / Run Agentless Scanner

To invoke discovery job relevant to the device manually, and check progress and status of the discovery job:

1. In UCMDB, go to **Data Flow Management > Universal Discovery > Discovery Modules/Jobs** tab.
2. In the Discovery Modules tree, select **Hosts and Resources > Inventory Discovery > Inventory Discovery by Scanner**.
3. Right-click **Inventory Discovery by Scanner**, select **Activate** from the context menu if the job is not activated, and wait for the Triggered CIs list to refresh.
4. In the Triggered CIs list in the Discovery Progress pane, click a number with link of your interest.
5. In the **Look for** field that is just enabled, enter the IP address for the scanner and click .
6. Right-click the returned entry, and from the context menu, select **Run from step > <Select an action>**.

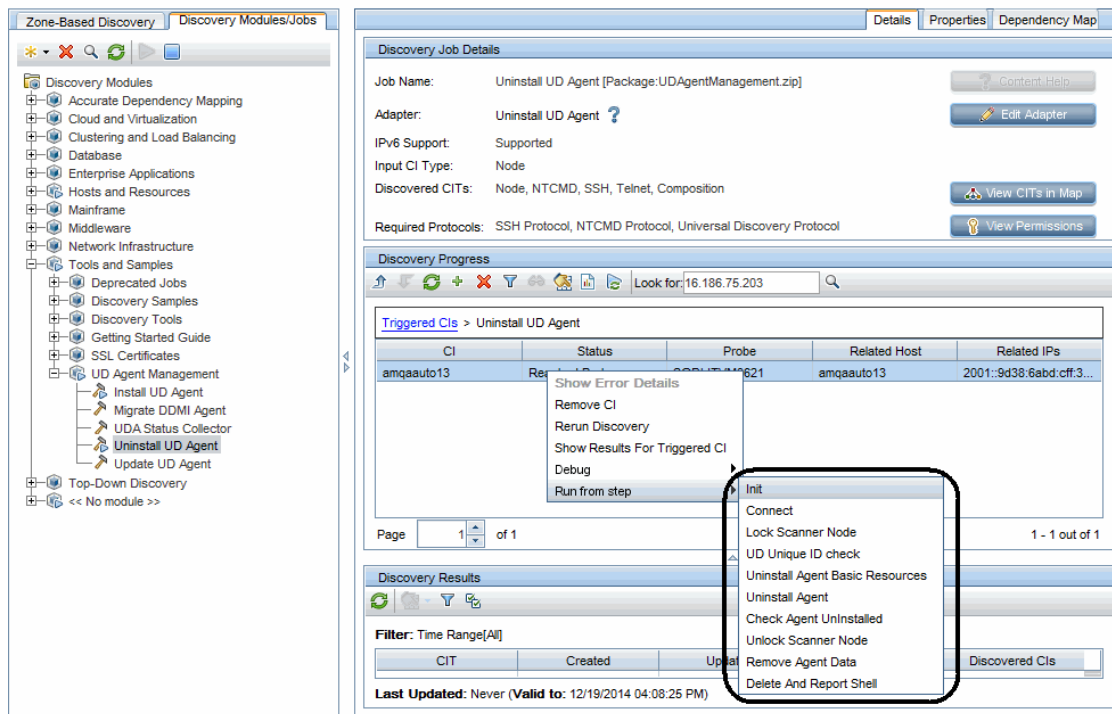


**Note:** To **Run Agentless Scanner**, before selecting a **Run from step** option, set Universal Discovery Protocol scope to **Probes: Disabled**.

To do so,

- In the Data Flow Management module, go to **Data Flow Probe Setup**.
- Expand **Domains and Probes > DefaultDomain(Default) > Credentials > Universal Discovery Protocol**.
- In the right Universal Discovery Protocol pane, right-click a protocol and select **Edit**.
- In the Universal Discovery Protocol Parameters dialog box, click the **Edit** Edit... button for the Network Scope field.
- In the Scope Definition dialog box, click the **Edit** Edit button for the Selected Probes section.
- In the Selected Probes dialog box, clear the check box for **All Data Flow Probes** and click **OK** three times to exit.
- Repeat [step c](#) through [step f](#) for other protocols.





7. To check the progress/on-going status of the discovery job,
  - a. Modify the Uninstall UD Agent adapter's configuration to make sure that the communication log is always created.  
  
For detailed instructions, see ["To check the progress/on-going status of the discovery job," on page 136.](#)
  - b. Right-click the returned entry in the Discovery Progress pane, from the context menu, select **Debug > View Communication Log.**  
  
For details, see ["How to check device related logs for a discovered device?" on page 132.](#)

## Rerun Discovery

The Run Rulebase feature is implemented in UD normalization, which covers all jobs.

To invoke the normalization manually, in the Discovery Progress pane, right-click the CI entry returned from your search and select **Rerun Discovery** from the context menu, which will perform the normalization.

**Note:** Normalization cannot be invoked alone in UD. By selecting **Rerun Discovery**, you can invoke the normalization, but would also trigger other operations included in the discovery job in addition to the normalization.

To check the progress/on-going status of the discovery job,

1. Modify the concerning adapter's configuration to make sure that the communication log is always created.


For detailed instructions, see ["To check the progress/on-going status of the discovery job," on page 136.](#)

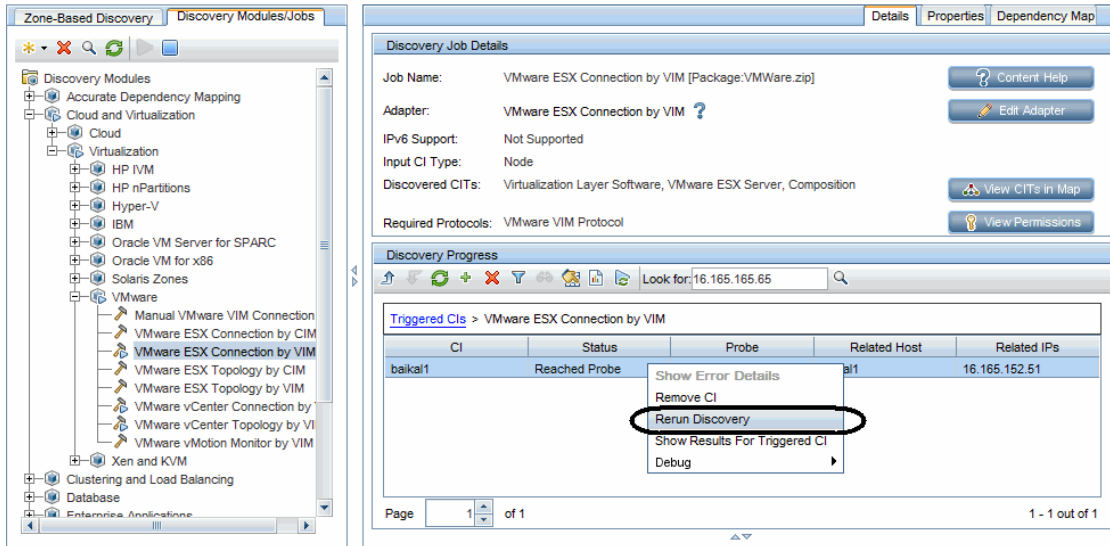
2. Right-click the returned entry in the Discovery Progress pane, from the context menu, select **Debug > View Communication Log**.

For details, see ["How to check device related logs for a discovered device?" on page 132.](#)

## VMware Discovery Jobs

To invoke the VMware discovery job manually,

1. In UCMDB, go to **Data Flow Management > Universal Discovery > Discovery Modules/Jobs** tab.
2. In the Discovery Modules tree, select **Cloud and Virtualization > VMware > <select a job>**.
3. Right-click the selected job, select **Activate** from the context menu if the job is not activated, and wait for the Triggered CIs list to refresh.
4. In the Triggered CIs list in the Discovery Progress pane, click a number with link.
5. In the **Look for** field that is just enabled, enter the IP address for the target device and click .
6. Right-click the returned entry, and select **Rerun Discovery** from the context menu.



7. To check the progress/on-going status of the discovery job,

- Modify the concerning adapter's configuration to make sure that the communication log is always created.

For detailed instructions, see ["To check the progress/on-going status of the discovery job,"](#) on page 136.

- Right-click the returned entry in the Discovery Progress pane, from the context menu, select **Debug > View Communication Log**.

For details, see ["How to check device related logs for a discovered device?"](#) on page 132.


## How to check which pattern (management zone) is used in the discovery for a discovered device?

**Question: For a discovered device, how should I check which pattern (management zone) is used in the discovery?**

In UD, there are two ways to check the management zone used:



- **From IT Universe Manager**

- In the Modeling module, go to **IT Universe Manager**.
- On the Search CIs tab, enter the IP address for a discovered device in the **CI Name** field, select **Managed Object** for the **CI Type** field, and click .
- Click the returned entry on the Search CIs tab. CI details are displayed in the right pane.
- Go to the **Properties** tab for the CI and check the value for the following attributes:
  - Created By
  - Updated By

For example,

Create Time	Thu Dec 4 2014 10:36 PM IST
Created By	UCMDBDiscovery: MZ_SGDLITVM0567_test_infrastructure_Network_Range IPs by ICMP
Deletion Candidate Period	
UcmdbRoutingDomain	DefaultDomain
Updated By	UCMDBDiscovery: MZ_SGDLITVM0567_test_infrastructure_Network_Host Connection by Shell
User Label	

- **From the Management Zone Description**

- In the Data Flow Management module, go to **Universal Discovery > Zone-Based Discovery**.
- From the Management Zones tree, select a management zone. The Management Zone description displays in the right pane.

For example

**Management Zone:** SGDLITVM0567\_AIX Machines

Description:

Ranges Method: Based on partial Data Flow Probe ranges

Ranges:

Domains and Probes

- DefaultDomain
- QASERVER7

Range	Type
16.157.130.92	Data Center
16.157.132.236	Data Center
16.157.132.237	Data Center
16.173.232.59	Data Center

## How to check detailed discovery settings used in the discovery for a discovered device?

**Question: For a discovered device, how should I check the detailed discovery settings (such as job parameters and scan settings) used in the discovery?**

In UD, there are two ways to check detailed settings used in the discovery:

- **From UI** (the Properties tab and the Edit Inventory Discovery Activity dialog box)

- Run jobs in **Discovery Modules/Jobs**

The Properties tab of the Inventory Discovery by Scanner job displays all parameters and scanner settings of the job

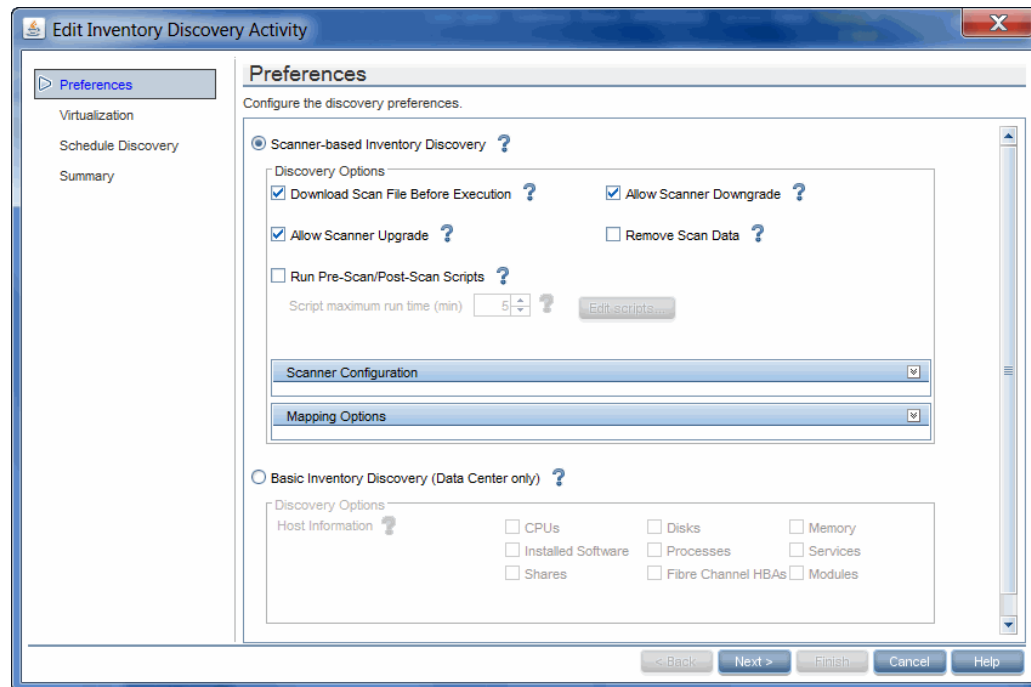
- In UCMDB, go to **Data Flow Management > Universal Discovery > Discovery Modules/Jobs** tab.
- In the Discovery Modules tree, select **Hosts and Resources > Inventory Discovery > Inventory Discovery by Scanner**.
- In the pane, go to the **Properties** tab.

All parameters and scanner settings of the job are displayed.

Override	Name	Value
<input type="checkbox"/>	DownloadScanFileBeforeExecution	true
<input type="checkbox"/>	IsPrePostScriptAllowed	false
<input type="checkbox"/>	IsScannerDowngradeAllowed	true
<input type="checkbox"/>	IsScannerUpgradeAllowed	true
<input type="checkbox"/>	MappingConfiguration	Scan file model mapping configurations
<input type="checkbox"/>	P2PServerPorts	*
<input type="checkbox"/>	PrePostScriptExecTimeout	5
<input type="checkbox"/>	RemoveScanData	false
<input type="checkbox"/>	ScannerConfigurationFile	use file default cxx for all platforms
<input type="checkbox"/>	ScannerLogLevel	info
<input type="checkbox"/>	collectIPv6Connectivity	false
<input type="checkbox"/>	discoverProcesses	false
<input type="checkbox"/>	discoverRunningSW	Microsoft Hyper-V Hypervisor, VMware VirtualC...
<input type="checkbox"/>	enableStamping	true
<input type="checkbox"/>	filterP2PProcessesByName	system,svchost.exe,lsass.exe,System Idle Proc...
<input type="checkbox"/>	ignoreP2PLocalConnections	false
<input type="checkbox"/>	onlyStampingClient	true

- Run jobs in **Zone-Based Discovery**
  - In the **Data Flow Management** module, go to **Universal Discovery > Zone-Based Discovery**.
  - From the Management Zones tree, select a management zone.
  - Right-click a discovery job and select **Edit** from the context menu.

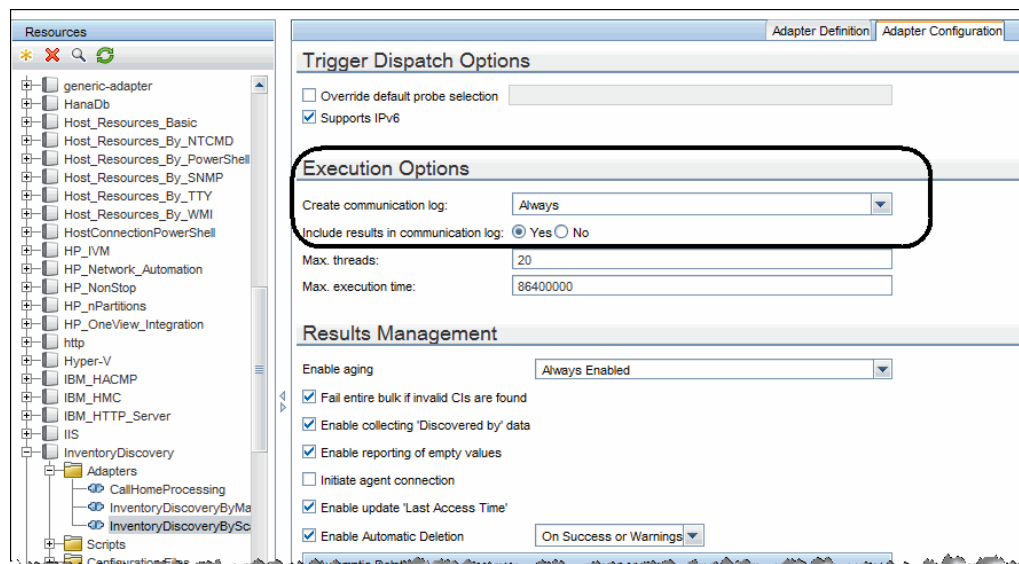
The Edit Discovery Activity dialog box opens.




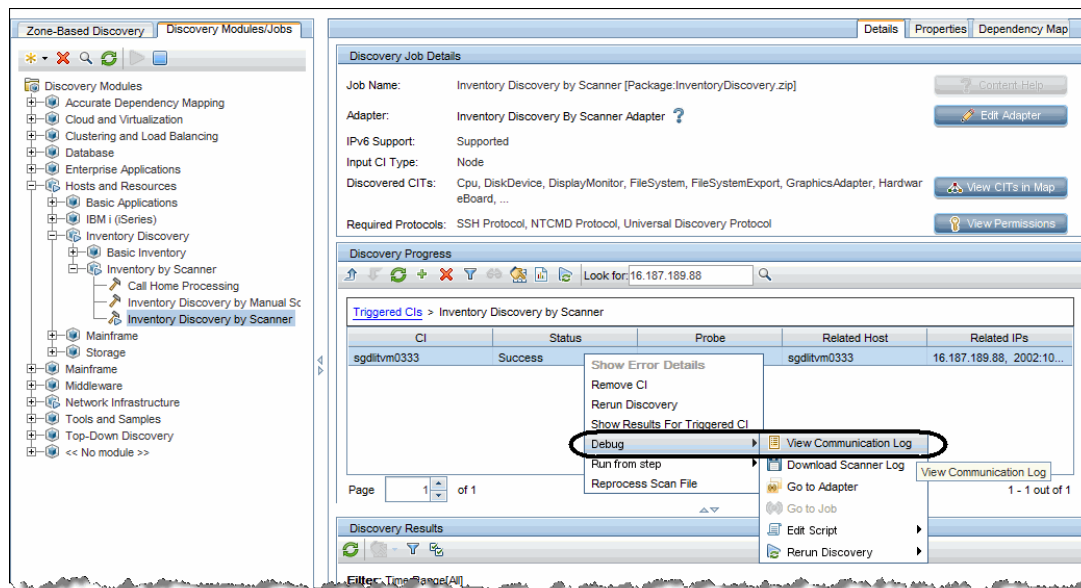
You can find the discovery job parameters and scanner settings in this dialog box.

- From the **Communication Log**
  - a. Modify the configuration of the adapter for the Inventory Discovery by Scanner job to make sure that the communication log is always created.
    - i. In the Data Flow Management module, go to **Adapter Management**.
    - ii. In the Resources pane, expand **InventoryDiscovery> Adapters > InventoryDiscoveryByScanner**.
    - iii. In the right pane, click the **Adapter Configuration** tab.
    - iv. In the Execution Options section, set the following:
      - **Create communication log: Always**

- **Include results in communication log: Yes**



- In UCMDB, go to **Data Flow Management > Universal Discovery > Discovery Modules/Jobs** tab.
- In the Discovery Modules tree, select **Hosts and Resources > Inventory Discovery > Inventory Discovery by Scanner**.
- (Optional) Right-click **Inventory Discovery by Scanner**, select **Activate** from the context menu if the job is not activated, and wait for the Triggered CIs list to refresh.
- In the Triggered CIs list in the Discovery Progress pane, click a number with link of your interest.
- In the **Look for** field that is just enabled, enter the IP address for the scanner and click .
- Right-click the returned entry, and from the context menu, select **Debug > View Communication Log**.



h. In the log that opens, search keywords to check details:

- To locate where the job parameters start in the log, search **<params>**.
- To locate where the job parameters end in the log, search **</params>**.
- To locate where the scanner configuration file is used in the log, search **Config file to be used:**.

## How to check the SNMP credentials used in the discovery for a discovered device?


**Question: For a discovered device, how should I check the SNMP credentials used in the discovery?**

To check the SNMP credentials used in the discovery, you can search the Communication Log of the Host Connection by SNMP job.

To view communication log for agent related jobs,

1. In UCMDB, go to **Data Flow Management > Universal Discovery > Discovery Modules/Jobs** tab.
2. In the Discovery Modules tree, select **Network Infrastructure > Host Connection > Host**

### Connection by SNMP.

3. (Optional) Right-click **Host Connection by SNMP**, select **Activate** from the context menu if the job is not activated, and wait for the Triggered CIs list to refresh.
4. In the Triggered CIs list in the Discovery Progress pane, click a number with link.
5. In the **Look for** field that is just enabled, enter the IP address for the target device and click .
6. Right-click the returned entry, and from the context menu, select **Debug > View Communication Log**.
7. In the log that opens, search **<CONNECT start** as keyword to locate the entry in the log that indicates starting from when the device is connected.

For example:

```
<CONNECT start="08:05:20" duration="4" CMD="client_connect" RESULT="success"
type="snmp" credentialsId="7_1_CMS">
  <ClientProperties>
    <prop name="protocol_index" value="1" />
    <prop name="protocol_timeout" value="3000" />
    <prop name="credentialsId" value="7_1_CMS" />
    <prop name="cm_credential_id" value="7_1_CMS" />
    <prop name="snmpprotocol_version" value="version 2c" />
    <prop name="protocol_type" value="snmpprotocol" />
    <prop name="snmpprotocol_postfix" value="" />
    <prop name="port" value="161" />
    <prop name="protocol_netaddress" value="DEFAULT" />
    <prop name="ip_address" value="16.187.190.19" />
    <prop name="snmpprotocol_privalg" value="3DES" />
    <prop name="snmpprotocol_authalg" value="MD5" />
    <prop name="protocol_port" value="161" />
    <prop name="snmpprotocol_retry" value="2" />
    <prop name="snmpprotocol_snmpmethod" value="getnext" />
    <prop name="user_label" value="SNMP Protocol Credential 1" />
    <prop name="snmpprotocol_authmethod" value="noAuthNoPriv" />
    <prop name="retry" value="2" />
    <prop name="protocol_username" value="" />
    <prop name="protocol_in_use" value="false" />
  </ClientProperties>
</CONNECT>
```

This log example indicates that the device is connected successfully by SNMP and the credential ID is **7\_1\_CMS**.

The log information between the **<ClientProperties>** and **</ClientProperties>** tags are the details of the SNMP credential used in the discovery. Among these properties information, to find

out the credential name, you can check the value for the **user\_label** attribute (highlighted above) of the SNMP credential that you defined in the SNMP protocol.

**Note:** The SNMP community strings you defined in the protocol are encrypted in UD, therefore they are not visible in the log.

## How to View Discovery Status and Errors for a Selected CI from the Discovery Progress Widget

Discovery administrators and data consumers can view warning or error indicators for discovery issues with discovery jobs in the Discovery Progress widget, they can also view summary and detailed discovery status, errors, and warnings for a selected CI in the Discovery Progress widget.

**Note:** To use this feature, you need to have the **Run Discovery and Integration** or the **View Discovery Status and Error** permissions. The out-of-the-box **Discovery and Integrations Admin** role has all these permissions by default.

You also need the **View** permission to the Discovery Progress widget.

This task includes the following steps:

- [Prerequisites: Grant the Required Permissions](#)
- [View the Discovery Progress widget in the UCMDB Browser module](#)

### 1. **Prerequisites: Grant the Required Permissions**

**Note:** This step is performed by the system administrator.

To view the **Discovery Progress** widget from the **UCMDB Browser** module, your administrator needs to grant the following permissions to you:

- **Run Discovery and Integrations** (for discovery administrators) or **View Discovery Status and Error** (for data consumers)
- **Access to UCMDB Browser**
  - a. Log in to UCMDB and go to **Security > Roles Manager > Roles**.
  - b. Select the role to which you want to add the permission.


Create a new role if you do not have such a role.

**Note:** The **View Discovery Status and Error** permission is not available for all out-of-the-box roles.

- c. Click the **General Actions** tab.
- d. In the Data Flow Management Actions section, select the **Run Discovery and Integrations** or **View Discovery Status and Error** action in the Available Actions pane and move it to the Selected Actions pane.
- e. In the System Access Actions section, select **Access to UCMDB Browser** in the Available Actions list and add it to the Selected Actions list.

## 2. View discovery status, errors, and warnings for a selected CI in the Discovery Progress widget

- a. Launch the UCMDB Browser and access the Discovery Progress widget.
  - **For discovery administrators, launch the Discovery Progress widget from the Discovered CIs dialog in UCMDB UI.**

When performing job-based discovery troubleshooting in the Universal Discovery module, after drilling down to the Discovered CIs dialog (for example, by following the **Triggered CIs > Completed with Errors >** <Double-click an error message, and then right-click a detailed message> > **Show Results for Triggered CI >** <Select a CIT and click **Show Additional Data** > > **Discovered CIs**), you may want to find out more details about an affected CI.

To do so,

- A. In the Discovered CIs dialog, right-click a discovered CI and select **Open UCMDB Browser** from the context menu.

The UCMDB Browser launches, with the CI Details pane opening in the right side of the UCMDB Browser search page.

- B. In the CI details pane, click **DISCOVERY PROGRESS** or **Show All** in the Discovery Progress widget in CI Overview mode.

The Discovery Progress widget opens to its widget details mode.

- **For data consumers, launch UCMDB Browser and open the Discovery Progress widget for a selected CI**

- A. log in to the UCMDB Browser, enter either of the following in a web browser:

**http://<server\_name>:<8088>/ucmdb-browser**



**https://<server\_name>:<8443>/ucmdb-browser**

where <server\_name> represents the fully qualified domain name (FQDN) of the UCMDB server.

- B. Search for the CI of your interest.

The returned search results page displays a list of all CIs. The discovery indicator (✓, ⚠, or ✖) next to each returned CI gives you a straightforward discovery status of the CI.

- C. On the returned search results page, click the CI of your interest.

The CI Details pane opens in the right side of the page.

- D. Click **DISCOVERY PROGRESS** or **Show All** in the Discovery Progress widget in CI Overview mode.

The Discovery Progress widget opens to its widget details mode.

- b. View discovery indicators, discovery status, errors, and warnings for a selected CI in the Discovery Progress widget.

For details about the Discovery Progress widget, see the *Discovery Progress Widget* section in the *Use section of the Universal CMDB Browser Online Help*.

## APLS Integration Troubleshooting - Error Handling Messages

- **Message:** APLS configuration entries are missing

**Meaning:** Make sure AutoPass settings are properly configured in the **UCMDB UI > Administration Infrastructure Settings Manager** module.

- **Message:** Authentication fails

**Meaning:** Make sure APLS username/password are properly set in the **UCMDB UI > Administration Infrastructure Settings Manager** module.

- **Message:** SSL handshake issue

**Meaning:** When there is a SSL handshake issue, the following error message can be found in the log:

SSLHandshakeException, No trusted certificate found: xxxx

- **Message:** No usage available

**Meaning:** When there is no usage available, the following error messages can be found in the log:

No discovery Unit is being used, skip reporting this to APLS.

No third party MDR Unit is being used, skip reporting this to APLS.

- **Message:** APLS server is down (ConnectException)

**Meaning:** When there is a server down issue, the following error message can be found in the log:

Cannot establish connection with APLS. Make sure APLS is up and running.

Exception: xxxx

# Chapter 6: Troubleshooting Configuration Manager


This chapter includes:

Troubleshooting and Limitations – Content Management .....	155
Troubleshooting and Limitations – Federating Data to UCMDB .....	156
Troubleshooting – Explore Views .....	156
Troubleshooting – Review/Authorize .....	159
Troubleshooting and Limitations – Views .....	161
Troubleshooting and Limitations – Policies .....	161

## Troubleshooting and Limitations – Content Management

**Problem.** Changes in CIs in UCMDB are not reflected in Configuration Manager.

**Solution.** Configuration Manager runs an offline asynchronous analysis process. The process may not yet have processed the latest changes in UCMDB. To resolve this, try one of the following:

- Wait a few minutes. The default interval between analysis process executions is 10 minutes. This value is configurable in under **Administration > Settings**.
- Execute a JMX call to run the offline analysis calculation on the relevant view.
- Navigate to **Policies**. Click the **Recalculate Policy Analysis**  button. This invokes the offline analysis process for all views (which may take some time). You may also need to make an artificial change to one policy and save it.

**Problem.** When you click the **Launch UCMDB**  button, the UCMDB login page appears.

**Solution.** In order to access UCMDB without logging in again, you need to enable single sign-on. For details, see the section about enabling LW-SSO between Configuration Manager and UCMDB in the *Universal CMDB Deployment Guide*. Additionally, ensure that the Configuration Manager user logged on is defined in the UCMDB user management system.

**Problem.** The **Matching Rules** tab does not appear in Universal CMDB when you navigate to **Managers > Modeling > CI Type Manager**, and select **CI Types** from the list box in the CI Types pane.

**Solution.** Navigate to **Managers > Administration > Infrastructure Settings** in Universal CMDB and set **Enable Configuration Manager Matching Rules** as `True`. After you log out and then log in again, the Matching Rules tab appears in the CI Type Manager.

## Troubleshooting and Limitations – Federating Data to UCMDB

- Federation only works with CIs in the actual state. Therefore:
  - Policy compliance is federated only for CIs in the actual state.
  - The authorization status for CIs that were deleted from the actual state is not shown.
- The maximum number of CIs that can be federated is configurable. To change this number, edit the value of the Max Num To Federate setting in the Infrastructure Settings Manager in UCMDB. For details about changing settings, see "Infrastructure Settings Manager" in the *Administer section of the UCMDB Help*. The recommended number of CIs is no more than 20,000, if large views have been enabled in Configuration Manager. For details about enabling support for large views, see the section about large capacity planning in the interactive *Universal CMDB Deployment Guide*.
- If the test connection fails, click **Details** and check the first error in the stack trace for more information.
- Since a CI can be managed in multiple views, the same policy may be applied to the same CI in multiple views and may receive different similarity results, since the similarity group may be different in different views.

## Troubleshooting – Explore Views

- **Problem.** Buttons for creating RFCs are disabled.

**Possible reasons:**

- The Change Management integration has been disabled for the activated configuration.
- The Change Management integration has been defined, saved, and activated, but the user did not log in to Configuration Manager again.

**Solution.** Do the following:

- a. Navigate to **Administration > Integrations > Change Management**. To configure the integration, select the check box and provide the details for the Service Manager configuration.
  - b. Save and activate the configuration.
  - c. Log out and then log in again to see the changes take effect.
- **Problem.** RFC creation fails.
    - **Reason 1:** Incorrect credentials were defined for the integration user under **Administration > Integrations > Change Management > Service Manager**.  
**Solution 1:** In Service Manager, verify that the integration user exists. If required, update the password (for details, see the Service Manager documentation).
    - **Reason 2:** The user does not have the proper credentials to invoke a call to the Service Manager web-service.  
**Solution 2:** Enable the ability to execute the SOAP API for this integration user (for details, see the Service Manager documentation).
    - **Reason 3:** The UNL file for this integration has not been loaded into Service Manager.  
**Solution 3:** To detect if the UNL file has been uploaded, call the following Service Manager URL:  
  
<host>:<port example:13080>/sm/7/ucmdcm.wsdl  
  
If the call returns an XML file, then a web-service is on, meaning that the UNL file has been uploaded. If not, follow the directions in [Import a UNL File into Service Manager](#).
    - **Reason 4:** An RFC has been created with at least one of the following mismatches:
      - The service does not exist in Service Manager.
      - One or more of the selected CIs does not exist in Service Manager.
      - The category value does not match a valid value in Service Manager.
      - The risk assessment value does not match a valid value in Service Manager.
      - The impact value does not match a valid value in Service Manager.
      - The urgency value does not match a valid value in Service Manager.**Solution 4:** Change the values for each of the possible mismatches listed above under **Administration > Application Management > RFC > RFC Creation**, so they match with the corresponding values in Service Manager. Save and activate the configuration for the settings to take effect.
    - **Problem.** Configuration Manager doesn't display RFCs.

**Tip:** As a first step in identifying whether the problem is in UCMDB or Service Manager, you can execute a TQL query in UCMDB that fetches all RFCs from Service Manager. If RFCs are expected but do not appear in the query's results, it means that there is an issue with the integration between UCMDB and Service Manager.

To execute this TQL query: log in to UCMDB and navigate to **Modeling > Modeling Studio > Resources** tab (select Queries as the Resource Type) > **Configuration Manager > Configuration Manager – Do not modify > Generate RFC Queries** and execute **amber\_rfc\_by\_id**.

- **Reason 1:** The integration point between UCMDB and Service Manager is either not correctly configured or does not exist.

**Solution 1:** See the UCMDB documentation for details on how to set up the integration between UCMDB and Service Manager.

- **Reason 2:** An RFC change phase value in the Configuration Manager settings does not match the RFC phase definition in Service Manager.

**Solution 2:** Change the value for the RFC Change Phase field in the Configuration Manager settings to a valid value (as defined in Service Manager). Navigate to **Administration > Application Management > RFC > Fetch RFCs Criteria > RFC Filters** to change the settings. Note that the Change Phases field can contain multiple comma-separated values. Save and activate the configuration for the settings to take effect.

- **Reason 3:** The RFC does not meet the time window condition defined in the Configuration Manager settings for fetching RFCs.

**Solution 3:** Make sure that the RFC meets the time window condition in the Configuration Manager settings, or change the condition so that the RFC matches the time window. Save and activate the configuration for the settings to take effect.

- **Reason 4:** The date and time format between the integration user used by Configuration Manager for this integration has a different format than the corresponding user in Service Manager.

**Solution 4:** Make sure that the time format is defined identically for both user instances. In Configuration Manager, the Date Format definition is found under **Administration > Integrations > Change Management > Service Manager > Date Format**.

## Troubleshooting – Review/Authorize

- **Problem.** Buttons for creating RFCs are disabled.

**Possible reasons:**

- The Change Management integration has been disabled for the activated configuration.
- The Change Management integration has been defined, saved, and activated, but the user did not log in to Configuration Manager again.

**Solution.** Do the following:

- a. Navigate to **Administration > Integrations > Change Management**. To configure the integration, select the check box and provide the details for the Service Manager configuration.
- b. Save and activate the configuration.
- c. Log out and then log in again to see the changes take effect.

- **Problem.** RFC creation fails.

- **Reason 1:** Incorrect credentials were defined for the integration user under **Administration > Integrations > Change Management > Service Manager**.

**Solution 1:** In Service Manager, verify that the integration user exists. If required, update the password (for details, see the Service Manager documentation).

- **Reason 2:** The user does not have the proper credentials to invoke a call to the Service Manager web-service.

**Solution 2:** Enable the ability to execute the SOAP API for this integration user (for details, see the Service Manager documentation).

- **Reason 3:** The UNL file for this integration has not been loaded into Service Manager.

**Solution 3:** To detect if the UNL file has been uploaded, call the following Service Manager URL:

<host>:<port example: 13080>/sm/7/ucmdcm.wsdl

If the call returns an XML file, then a web-service is on, meaning that the UNL file has been uploaded. If not, follow the directions in [Import a UNL File into Service Manager](#).

- **Reason 4:** An RFC has been created with at least one of the following mismatches:
  - The service does not exist in Service Manager.
  - One or more of the selected CIs does not exist in Service Manager.

- The category value does not match a valid value in Service Manager.
- The risk assessment value does not match a valid value in Service Manager.
- The impact value does not match a valid value in Service Manager.
- The urgency value does not match a valid value in Service Manager.

**Solution 4:** Change the values for each of the possible mismatches listed above under **Administration > Application Management > RFC > RFC Creation**, so they match with the corresponding values in Service Manager. Save and activate the configuration for the settings to take effect.

- **Problem.** Configuration Manager doesn't display RFCs.

**Tip:** As a first step in identifying whether the problem is in UCMDB or Service Manager, you can execute a TQL query in UCMDB that fetches all RFCs from Service Manager. If RFCs are expected but do not appear in the query's results, it means that there is an issue with the integration between UCMDB and Service Manager.

To execute this TQL query: log in to UCMDB and navigate to **Modeling > Modeling Studio > Resources** tab (select Queries as the Resource Type) > **Configuration Manager > Configuration Manager – Do not modify > Generate RFC Queries** and execute `amber_rfc_by_id`.

- **Reason 1:** The integration point between UCMDB and Service Manager is either not correctly configured or does not exist.

**Solution 1:** See the UCMDB documentation for details on how to set up the integration between UCMDB and Service Manager.

- **Reason 2:** An RFC change phase value in the Configuration Manager settings does not match the RFC phase definition in Service Manager.

**Solution 2:** Change the value for the RFC Change Phase field in the Configuration Manager settings to a valid value (as defined in Service Manager). Navigate to **Administration > Application Management > RFC > Fetch RFCs Criteria > RFC Filters** to change the settings. Note that the Change Phases field can contain multiple comma-separated values. Save and activate the configuration for the settings to take effect.

- **Reason 3:** The RFC does not meet the time window condition defined in the Configuration Manager settings for fetching RFCs.

**Solution 3:** Make sure that the RFC meets the time window condition in the Configuration Manager settings, or change the condition so that the RFC matches the time window. Save and activate the configuration for the settings to take effect.



- **Reason 4:** The date and time format between the integration user used by Configuration Manager for this integration has a different format than the corresponding user in Service Manager.

**Solution 4:** Make sure that the time format is defined identically for both user instances. In Configuration Manager, the Date Format definition is found under **Administration > Integrations > Change Management > Service Manager > Date Format**.

## Troubleshooting and Limitations – Views

The following limitations are applicable when working with managed views in Configuration Manager:

- Views that contain federated TQL queries cannot be selected for addition to the managed views list.
- If a view contains a node with a date restriction, you will see updated data for this view only if it is configured to be updated once per day (not each time the view is updated). To see updated data for such a view, use the JMX console to manually refresh the view.

## Troubleshooting and Limitations – Policies

The following limitation is applicable when working with policies:

Condition TQL queries must not include attribute conditions on unmanaged attributes.

# Chapter 7: Troubleshooting Automated Service Modeling

This chapter includes:

Troubleshooting Automated Service Modeling (ASM) - General Guideline .....	162
Troubleshooting ASM - Host Discovery by Shell job .....	164
Troubleshooting ASM - References .....	170
Add an IP Range to the Ranges Setting .....	170
Discover Load Balancers .....	170
Add or Edit Credentials .....	170
Edit the portNumberToPortName.xml File .....	171
Add or Edit Application Signatures .....	171

## Troubleshooting Automated Service Modeling (ASM) - General Guideline

This chapter introduces the general troubleshooting guidelines for problems that may occur during the Service Modeling process.

When an error occurs with a particular CI in the topology map, an error icon appears on the CI.



The following steps demonstrate the basic troubleshooting procedure for such an error:

1. View the error message in the UCMDB Browser module.
  - a. Click the error icon on the CI.

The **Discovery Issues** pane appears and lists all the related discovery issues.

Discovery Issues	
All Discovery Issues	1
Credential-Related Errors	1

- b. Click one of the categories.

A list of errors of the category appears.

- c. Click an error to view the detailed error message.

#### Software Related Errors

The following outgoing ports are filtered because they are not in portNumberToPortName.xml: 13080, 61447, 61448, 61449, 61450, 61451, 61452, 61453, 61454, 61455, 61456, 61457, 61458, 65121, 65305, 65306

[Download Discovery Log](#) [Email Administrator](#) [Troubleshooting Guide](#)

Add Port Number

2. Perform one of the following actions when appropriate.

- For some errors under **Software Related Errors**, you can directly provide some missing information in the UCMDB Browser module. As in the above example, if you click the **Add Port Number** button, you will be able to add the missing port numbers.

[http]16.155.155.45:8080/webtier-9.51/index.do  
Problem Source: Some outgoing ports are filtered

Back to List

#### Add Port Number

PORT UPDATE  
We have discovered new port numbers

Application Name

Port Number [Select All](#) [Deselect All](#)

<input type="checkbox"/>	13080
<input type="checkbox"/>	61447
<input type="checkbox"/>	61448
<input type="checkbox"/>	61449
<input type="checkbox"/>	61450
<input type="checkbox"/>	61451
<input type="checkbox"/>	61452

Save Mapping

- Search the error message in this chapter, and try the suggested solutions.

3. Rerun the Service Modeling task.

# Troubleshooting ASM - Host Discovery by Shell job

This chapter describes the error messages you may receive from the Host Discovery by Shell job and provides suggested solutions.

---

**Error Message:** The IP address is not in the discovery IP Range

**Error Category:** Probe Errors



## Probe Errors

16.■■■■ is not in the discovery IP Range. You need to create a new IP range.

The following jobs are impacted:

1. SD\_3\_Host Discovery by Shell

Add IP Range

 Download Discovery Log    Email Administrator    Troubleshooting Guide

**Solution:** Add the IP address or range to the **Ranges** setting of the probe. For more details, see "[Add an IP Range Manually](#)" on page 1.

---

**Error Message:** Inaccessible network path to target server. Perhaps it is a virtual IP address.

**Error Category:** Connection Errors

## Others

Inaccessible network path 16.■■■■36 to target server. Perhaps it is a virtual IP address.

Add Physical IPs

 Download Discovery Log    Email Administrator    Troubleshooting Guide

**Solution:** Add physical IPs as entry points of next hop

[https]16.36:8443 /  
Problem Source: Inaccessible network path to target server

Back to L

Add Physical IPs

IP\*

Port\*

Context

Add Physical IP

OK

Cancel

**Error Message:** Need credential to the host

**Error Category:** Credential-related Errors

**Credential-Related Errors**  
No valid credentials to the host 16.155.155.155 are found. You need to create valid credentials.

Download Discovery Log

Email Administrator

Troubleshooting Guide

Enter Creden

**Solution:** Add the valid credentials. For more information about how to do this, see ["Add or Edit Credentials" on page 170](#).

[\[https\]16.155.155.155:8743 /webtier-9.51/index.do](#)  
Problem Source: No valid credentials found

Back to List

**ENTER CREDENTIALS**

Possible Applicable Protocols

NTCMD

Network Scope

☒ All Discovery Issues ☐ Selected Range

username

password

confirm\_password

connection\_timeout

20000

run\_windows\_commands\_impersonated

☐ true ☒ false

remote\_share\_path

local\_share\_path

Save

**Error Message:** Connection timeout

**Error Category:** Timeout Errors

#### Timeout Errors

SSH: Timeout trying to connect to the remote agent. Try increasing the timeout value.

[Download Discovery Log](#) [Email Administrator](#) [Troubleshooting Guide](#)

#### Solution:

- Increase the timeout value in protocol settings.
- For Windows machines, wait for a few minutes and then try again.

**Error Message:** The discovery job did not find any process listening on port: <port\_number>

**Error Category:** Software Related Errors

#### Solution:

- Check if the configured account has sufficient privileges to run relevant commands. Specifically,
  - `ps -e`
  - `netstat -nap`

- **Isotf**

Elevate privilege for UNIX credentials.

- Verify if the service is still accessible.
- Check if **Isotf** is installed on the target machine if it runs UNIX.

---

**Error Message:** No application signature matches the process `<process_info>` listening on port `<port_number>`

**Error Category:** Software Related Errors

**Solution:** Add the signature for the application. For more information about how to do this, see ["Add or Edit Application Signatures" on page 171](#).

---

**Error Message:** The following outgoing ports are filtered because they are not in `portNumberToPortName.xml`

**Error Category:** Software Related Errors

**Software Related Errors**

No application signature matches the process [Process('ucmdb\_server.exe', 2632, "jre\bin\ucmdb\_server"  
-server -XX:+PrintCommandLineFlags -XX:+UseG1GC -XX:+UnlockExperimentalVMOptions  
-XX:MaxGCPauseMillis=2000 -Dsun.rmi.dgc.client.gcInterval=0x7fffffffef  
-Dsun.rmi.dgc.server.gcInterval=0x7fffffffef -verbose:gc -XX:+PrintGCDetails -Ducmdb.home=..  
-Dcom.sun.management.jmxremote -Djava.io.tmpdir=../runtime/jetty-cache  
-Djava.naming.factory.url.pkgs=org.mortbay.naming  
-Djava.naming.factory.initial=org.mortbay.naming.InitialContextFactory -Ducmdb.browser.home=



Add Application Signature

Download Discovery Log Email Administrator Troubleshooting Guide

**Solution:** Add the port number to `portNumberToPortName.xml`.

To do this, click the **Application Signature** button in the error message and then follow the instructions. Alternatively, you can directly modify the `portNumberToPortName.xml` file to add the port number.

[\[https\]16.187.187.87:8443 /ucmdb-ui/login\\_page.jsp](#)  
*Problem Source: No application signature matches the process*

**Add Application Signature**

Software Library

[Add](#) [Delete](#) [Refresh](#) [Expand](#)

▶

📁 Software Element Categories

Software Signature ID

Category

Supported Version

**Created CI Properties**

CI Type

RunningSoftware

Discovered Product Name

Vendor

**Processes**

Key	Main	Name	Port	Command Line
-----	------	------	------	--------------

Save

Cancel

[Add](#) [Edit](#)

**Error Message:** The following outgoing ports are filtered because they are not in `portNumberToPortName.xml`.

**Error Category:** Software Related Errors

**Software Related Errors**  
The following outgoing ports are filtered because they are not in `portNumberToPortName.xml`: 13080, 61447, 61448, 61449, 61450, 61451, 61452, 61453, 61454, 61455, 61456, 61457, 61458, 65121, 65305, 65306

[Download Discovery Log](#) [Email Administrator](#) [Troubleshooting Guide](#)

Add Port Number

**Solution:** Add the port number to `portNumberToPortName.xml`.

To do this, click the **Add Port Number** button in the error message and then follow the instructions. Alternatively, you can directly modify the `portNumberToPortName.xml` file to add the port number.



[\[http\]16.155.155.16:8080/webtier-9.51/index.do](#)  
Problem Source: Some outgoing ports are filtered

Back to List

Add Port Number

PORT UPDATE

We have discovered new port numbers

Application Name

Port Number

Select All Deselect All

☐ 13080

☐ 61447

☐ 61448

☐ 61449

☐ 61450

☐ 61451

☐ 61452

Save Mapping

---

**Error Message:** Failed to resolve host name to IP

**Error Category:** IP-related Errors

**Solution:** Check DNS server configuration.

---

**Error Message:** Need sudo permission

**Error Category:** Software Related Errors

**Solution:** Elevate privilege for UNIX credentials to run the relevant command.

---

**Error Message:** No lsof installed on the host

**Error Category:** Software Related Errors

**Solution:** Install lsof on the target machine.

---

**Error Message:** The host is a Solaris local zone

**Error Category:** Software Related Errors

**Solution:** None for this release. Currently Solaris local zone is not supported by ASM.

---

**Error Message:** No SCP reported from configuration signature.

**Error Category:** Others


**Solution:** No SCP reported from configuration signature for application <Application Name>. Check the **ConfigurationFileSignature.xml** file to make sure all parameter values for your application are correct.

---

## Troubleshooting ASM - References

This chapter provides instructions for some of the solutions mentioned earlier.

### Add an IP Range to the Ranges Setting



1. Go to **Data Flow Probe Setup > Domains and Probes** pane > **Domains and Probes** root node > a domain > **Data Flow Probes** > a Data Flow Probe.
2. In the **Ranges** pane, click **New Range** .
3. Provide the necessary information on the **New Ranges** dialog box, and then click **OK**.

### Discover Load Balancers


1. Run the Host Connection by SNMP job.
2. Run one of the following jobs depending on the type of the load balancer:
  - F5 BIG-IP LTM by SNMP
  - Alteon application switch by SNMP
  - Cisco CSS by SNMP

### Add or Edit Credentials


1. Go to **Data Flow Probe Setup > Domains and Probes** pane > **Domains and Probes** root node > a domain > **Credentials** > a protocol.
2. In the right pane, perform one of the following actions to add or edit an entry:

- To add a new connection detail, click **Create new connection details for selected protocol type** .
  - To edit an existing credential, select the entry and then click **Edit connection details for selected protocol type** .
3. Provide the information on the dialog box that pops up, and then click **OK**.

## Edit the portNumberToPortName.xml File

1. Go to **Data Flow Management > Adapter Management**.
2. Click the **Search** button , and then search for **portNumberToPortName.xml**.
3. Edit the **portNumberToPortName.xml** file, and then click **Save**.

## Add or Edit Application Signatures

1. Go to **Data Flow Management > Adapter Management**.
2. In the Resources pane, select **Host\_Resources\_By\_TTY > Adapters > TTY\_HR\_All**.
3. In the **Adapter Definition** tab > **Global Configuration Files** section, select **applicationsSignature.xml** and then click **Edit** .

## Chapter 8: Troubleshooting Development

This chapter includes:

Troubleshooting Migration from Jython Version 2.1 to 2.5.3 .....	172
String Formatting .....	172
Checking String Type .....	173
Non-ASCII character in file .....	173
Import sub-packages .....	174
Iterator Changes .....	174
Raising Exceptions .....	174
Troubleshooting and Limitations – Developing Generic Database Adapters .....	175
General Limitations .....	175
JPA Limitations .....	175
Functional Limitations .....	176
Troubleshooting - Build an Adapter Package .....	176

## Troubleshooting Migration from Jython Version 2.1 to 2.5.3

Universal Discovery now uses Jython version 2.5.3. All out-of-the-box scripts have been properly migrated. If you developed your own Jython scripts prior to this upgrade for use by Discovery, you may run into the following issues and have to make the fixes indicated.

**Note:** You must be an experienced Jython developer to make these changes.

### String Formatting

- **Error message:** `TypeError: int argument required`
- **Possible cause:** Using string formatting to decimal integer from string variable containing integer data.

- **Problematic Jython 2.1 code:**

```
variable = "43"  
print "%d" % variable
```

- **Correct Jython 2.5.3 code:**

```
variable = "43"  
print "%s" % variable
```

or

```
variable = "43"  
print "%d" % int(variable)
```

## Checking String Type

The code below may not work correctly if input contains unicode strings:

- **Problematic Jython 2.1 code:**

```
isinstance(unicodeStringVariable, '')
```

- **Correct Jython 2.5.3 code:**

```
isinstance(unicodeStringVariable, basestring)
```

The comparison should be done with `basestring` to test whether an object is an instance of `str` or `unicode`.

## Non-ASCII character in file

- **Error Message:**

```
SyntaxError: Non-ASCII character in file 'x', , but no encoding declared;  
see http://www.python.org/peps/pep-0263.html for details
```

- **Correct Jython 2.5.3 code:** (add this to the first line in the file)

```
# coding: utf-8
```

## Import sub-packages

- **Error message:**

```
AttributeError: 'module' object has no attribute 'sub_package_name'
```

- **Possible cause:** A sub-package is imported without explicitly specifying the name of sub-package in the import statement.

- **Problematic Jython 2.1 code:**

```
import a  
print dir(a.b)
```

The sub-package is not explicitly imported.

- **Correct Jython 2.5.3 code:**

```
import a.b  
  
or  
  
from a import b
```

## Iterator Changes

Starting from Jython 2.2, the `__iter__` method is used to loop over a collection in the scope of a **for-in** block. The iterator should implement the **next** method, returning an appropriate element or throw the **StopIteration** error if it reached the end of the collection. If the `__iter__` method is not implemented, the **getitem** method is used instead.

## Raising Exceptions

- **Jython 2.1 method for raising exceptions is obsolete:**

```
raise Exception, 'Failed getting contents of file'
```

- **Recommended Jython 2.5.3 method for raising exceptions:**

```
raise Exception('Failed getting contents of file')
```

# Troubleshooting and Limitations – Developing Generic Database Adapters

This section describes troubleshooting and limitations for the generic database adapter.

## General Limitations

- When you update an adapter package, use Notepad++, UltraEdit, or some other third-party text editor rather than Notepad (any version) from Microsoft Corporation to edit the template files. This prevents the use of special symbols, which cause the deployment of the prepared package to fail.
- In most of the cases, after making a change, it is needed to reload the adapter on the probe side, otherwise the adapter will not function properly
  - a. Log in to the probe JMX console: **<https://localhost:8453/>**
  - b. Locate the **adapters** bean, and reload adapter with the integration point name.

If the adapter is not reloaded after each change, issues may occur (wrong error messages, query failures, and so on).

## JPA Limitations

- All tables must have a primary key column.
- CMDB class attribute names must follow the JavaBeans naming convention (for example, names must start with lower case letters).
- Two CIs that are connected with one relationship in the class model must have direct association in the database (for example, if node is connected to ticket there must be a foreign key or linkage table that connects them).
- Several tables that are mapped to the same CIT must share the same primary key table.

## Functional Limitations

- You cannot create a manual relationship between the CMDb and federated CITs. To be able to define virtual relationships, a special relationship logic must be defined (it can be based on properties of the federated class).
- Federated CITs cannot be trigger CITs in an impact rule, but they can be included in an impact analysis TQL query.
- A federated CIT can be part of an enrichment TQL, but cannot be used as the node on which enrichment is performed (you cannot add, update, or delete the federated CIT).
- Using a class qualifier in a condition is not supported.
- Subgraphs are not supported.
- Compound relationships are not supported.
- The external CI CMDbId is composed from its primary key and not its key attributes.
- A column of type bytes cannot be used as a primary key column in Microsoft SQL Server.
- TQL query calculation fails if attribute conditions that are defined on a federated node have not had their names mapped in the **orm.xml** file.

## Troubleshooting - Build an Adapter Package

The procedure for building a new push adapter requires complete and correct re-naming and replacing. Any error will likely affect the adapter. The package must be unzipped and re-zipped correctly to act as a UCMDb package. Refer to the out-of-the-box packages as examples. Common errors include:

- Including another directory on top of the package directories in the ZIP file.  
**Solution:** ZIP the package in the same directory as the package directories such as **discoveryResources**, **adapterCode**, etc. Do not include another directory level on top of this in the ZIP file.
- Omitting a critical re-name of a directory, a file, or a string in a file.  
**Solution:** Following the instructions in this section very carefully.
- Misspelling a critical re-name of a directory, a file, or string in a file.



**Solution:** Do not change your naming convention in mid-stream once you begin the re-naming procedure. If you realize that you need to change the name, start over completely rather than trying to retroactively correcting the name, as there is a high risk of error. Also, use search and replace rather than manually replacing strings to reduce risk of errors.

- Deploying adapters with the same file names as other adapters, especially in the **discoveryResources** and **adapterCode** directories.

**Solution:** You may be using a UCMDB version with a known issue that prevents mappings files from having the same name as any other adapter in the same UCMDB environment. If you attempt to deploy a package with duplicates names, the package deployment will fail. This problem may occur even if these files are in different directories. Further, this problem can occur regardless of whether the duplicates are within the package or with other previously deployed packages.

At this point you can create a new push adapter job in the Integration Studio using the new adapter you just deployed.

## Chapter 9: Troubleshooting Hardening

This chapter includes:

Troubleshooting and Limitations - Data Flow Credentials Management .....	178
Troubleshooting and Limitations - LW-SSO Authentication .....	178
Known Issues .....	178
Limitations .....	179
Troubleshooting Hybrid User Management - LDAP authentication .....	181
Troubleshooting - High Availability Mode .....	182
Troubleshooting - Database TLS Connection Issues .....	183

### Troubleshooting and Limitations - Data Flow Credentials Management

If you change the default domain name on the UCMDB server, you must first verify that the Data Flow Probe is not running. After the default domain name is applied, you must execute the **DataFlowProbe\tools\clearProbeData.bat** script on the Data Flow Probe side.

**Note:** Execution of the **clearProbeData.bat** script will cause a discovery cycle on the Probe side once the Probe is up.

### Troubleshooting and Limitations - LW-SSO Authentication

This section describes known issues and limitations when working with LW-SSO authentication.

#### Known Issues

This section describes known issues for LW-SSO authentication.

- **Security context.** The LW-SSO security context supports only one attribute value per attribute name.

Therefore, when the SAML2 token sends more than one value for the same attribute name, only one value is accepted by the LW-SSO framework.

Similarly, if the IdM token is configured to send more than one value for the same attribute name, only one value is accepted by the LW-SSO framework.

- **Multi-domain logout functionality when using Internet Explorer 7.** Multi-domain logout functionality may fail under the following conditions:

- The browser used is Internet Explorer 7 and the application is invoking more than three consecutive HTTP 302 redirect verbs in the logout procedure.

In this case, Internet Explorer 7 may mishandle the HTTP 302 redirect response and display an **Internet Explorer cannot display the webpage** error page instead.

As a workaround, it is recommended to reduce, if possible, the number of application redirect commands in the logout sequence.

## Limitations

Note the following limitations when working with LW-SSO authentication:

- **Client access to the application.**

**If a domain is defined in the LW-SSO configuration:**

- The application clients must access the application with a Fully Qualified Domain Name (FQDN) in the login URL, for example, `http://myserver.companydomain.com/WebApp`.

**Note:** The length of the FQDN cannot be longer than the value of the **Maximum domain extension length** setting in the Infrastructure Settings Manager. The default value is 8.

- LW-SSO cannot support URLs with an IP address, for example, `http://192.168.12.13/WebApp`.
- LW-SSO cannot support URLs without a domain, for example, `http://myserver/WebApp`.

**If a domain is not defined in the LW-SSO configuration:** The client can access the application without a FQDN in the login URL. In this case, a LW-SSO session cookie is created specifically for a single machine without any domain information. Therefore, the cookie is not delegated by the browser to another, and does not pass to other computers located in the same DNS domain. This means that LW-SSO does not work in the same domain.

- **LW-SSO framework integration.** Applications can leverage and use LW-SSO capabilities only if

integrated within the LW-SSO framework in advance.

- **Multi-Domain Support.**

- Multi-domain functionality is based on the HTTP referrer. Therefore, LW-SSO supports links from one application to another and does not support typing a URL into a browser window, except when both applications are in the same domain.
- The first cross domain link using **HTTP POST** is not supported.

Multi domain functionality does not support the first **HTTP POST** request to a second application (only the **HTTP GET** request is supported). For example, if your application has an HTTP link to a second application, an **HTTP GET** request is supported, but an **HTTP FORM** request is not supported. All requests after the first can be either **HTTP POST** or **HTTP GET**.

- LW-SSO Token size:

The size of information that LW-SSO can transfer from one application in one domain to another application in another domain is limited to 15 Groups/Roles/Attributes (note that each item may be an average of 15 characters long).

- Linking from Protected (HTTPS) to non-protected (HTTP) in a multi-domain scenario:

Multi domain functionality does not work when linking from a protected (HTTPS) to a non-protected (HTTP) page. This is a browser limitation where the referrer header is not sent when linking from a protected to a non-protected resource. For an example, see:

<http://support.microsoft.com/support/kb/articles/Q178/0/66.ASP>

- Third-Party cookie behavior in Internet Explorer:

Microsoft Internet Explorer 6 contains a module that supports the "Platform for Privacy Preferences (P3P) Project," meaning that cookies coming from a Third Party domain are blocked by default in the Internet security zone. Session cookies are also considered Third Party cookies by IE, and therefore are blocked, causing LW-SSO to stop working. For details, see:

<http://support.microsoft.com/kb/323752/en-us>.

To solve this issue, add the launched application (or a DNS domain subset as \*.mydomain.com) to the Intranet/Trusted zone on your computer (in Microsoft Internet Explorer, select **Menu > Tools > Internet Options > Security > Local intranet > Sites > Advanced**), which causes the cookies to be accepted.

**Caution:** The LW-SSO session cookie is only one of the cookies used by the Third Party application that is blocked.

- **SAML2 token**

- Logout functionality is not supported when the SAML2 token is used.

Therefore, if the SAML2 token is used to access a second application, a user who logs out of the first application is not logged out of the second application.

- **The SAML2 token's expiration is not reflected in the application's session management.**

Therefore, if the SAML2 token is used to access a second application, each application's session management is handled independently.

- **JAAS Realm.** The JAAS Realm in Tomcat is not supported.

- **Using spaces in Tomcat directories.** Using spaces in Tomcat directories is not supported.

It is not possible to use LW-SSO when a Tomcat installation path (folders) includes spaces (for example, Program Files) and the LW-SSO configuration file is located in the **common\classes** Tomcat folder.

- **Load balancer configuration.** A load balancer deployed with LW-SSO must be configured to use sticky sessions.
- **Demo mode.** In Demo mode, LW-SSO supports links from one application to another but does not support typing a URL into a browser window, due to an HTTP referrer header absence in this case.

## Troubleshooting Hybrid User Management - LDAP authentication

**Problem:** After upgrading UCMDB from version 10.30 (or earlier) to 10.31 (or later), LDAP authentication fails and users cannot log in to UCMDB. For example, a scenario like the following:

- You had UCMDB version 10.30 (or earlier)
- You configured LDAP server, and the UCMDB UI login is performed with multiple LDAP accounts
- You upgraded UCMDB to version 2018.08

**Cause:** As a part of Hybrid User Management, each user will be assigned a repository (UCMDB or a configured LDAP repository). If, during the upgrade, there are some connection issues related to the LDAP Server, then the existing LDAP users that were already synchronized to UCMDB cannot be authenticated on that LDAP repository, as a result, those users will be assigned to UCMDB repository.

To check if it is the case with your environment, in UCMDB UI, go to **Security > Users and Groups**, in the **Users** tab check the existing users. All the users are listed there with the corresponding repositories. If the repository set for an external user is UCMDB instead of the corresponding LDAP server repository, then there was a connection error to the LDAP server when the upgrade was performed.

**Solution:** In this case, the users will not be able to log in anymore to UCMDB UI only by using the username. To fix the issue, do either of the following:

- Perform the login by specifying the repository at login time.

For details, see ["How the hybrid user management authentication mechanism works"](#) (check "The repository is specified as an email address or Windows domain user" section).

In this way, the user will be authenticated against the repository specified, not on the UCMDB repository. As a result, in UCMDB there will be 2 users with the same username but on different repositories: the one on UCMDB repository that will not be able to log in and the one on the LDAP repository which will be able to login when the repository is also entered at login time.

- Delete from database all the external users that have been wrongly associated to UCMDB repository at upgrade.

An example of such an SQL statement that selects the users who should be deleted is:

```
select * from urm_resources where type='Auth_USER' and resource_id like '%###UCMDB' and text_data like '%isExternal="true"%'
```

After deleting these users, the login is performed properly and the users are re-synchronized to UCMDB.

**Note:** There could be other external users synchronized to UCMDB that are not LDAP-related, so double check which external users are deleted.

## Troubleshooting - High Availability Mode

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

Some examples of wrong cluster encryption configuration are:

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

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

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

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

## Troubleshooting - Database TLS Connection Issues

In case the UCMDB configuration wizard cannot access the MSSQL 2016 with TLS 1.2 protocol, do the following to resolve the UCMDB database TLS connection issue:

In the **UCMDBServer\conf\jdbc.properties** file, add the following parameter:

```
ddmssql.ValidateServerCertificate=false
```

This parameter just skips validating the Self-Signed Fallback certificate from Achmea DB server, and all the connections are still protected by the TLS protocol.

Meanwhile, another java option parameter should remain in the **<UCMDB\_Server>/bin/configure.bat** file, as shown below:

```
%JAVA% -Xms128m -Xmx512m -Dcom.sun.net.ssl.enableECC=false -cp  
"%ROOT%\tools\server\*;%ROOT%\bin\jre\lib\*;%ROOT%\lib\*;%UI%\jide-  
grids.jar;%UI%\jide-components.jar;%UI%\jide-common.jar;%UI%\jide-  
action.jar;%UI%\forms.jar;%UI%\swing_core.jar;%UI%\ui_core.jar;" -  
Ducmdb.home=%ROOT% com.hp.config_wizard.ui.frame.ConfigWizardMain %*
```

# Chapter 10: Troubleshooting Modeling

This chapter includes:

Troubleshooting and Limitations – Topology Query Language .....	184
Understanding Validation Restrictions .....	185
Impact Analysis TQL Query Validation .....	186
Enrichment TQL Query Validation .....	187
Troubleshooting and Limitations – CI Selector .....	188
Unavailable Views and CIs .....	189

## Troubleshooting and Limitations – Topology Query Language

This section describes troubleshooting and limitations for Topology Query Language.

- When creating resources, such as TQL queries, views, and Impact rules, make sure that there are no spaces at the end of the resource name.
- In a multi-tenancy environment, TQL query names cannot contain an @ character.
- 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.

The instructions below are an example for your reference:

- a. Create a tenant.
- b. Create a role with the following permissions: All permissions on view and folder, and permissions to access Modeling Studio.
- c. Create a user with the above role in the context of tenant from step a.
- d. Go to **Modeling Studio > Resources > View**, assign the tenant created in step a for the desired folder as owner tenant. (Meaning that the views are assigned to the tenant associated with the user who will perform the import.)



- e. Log in as the new user.
- f. In Modeling Studio, import a new view.
- If an error occurs while working with views in the Modeling managers, when adding CIs to the CMDDB, or when updating existing CIs, and the error log indicates that objects are missing in the database, do the following:
  - a. Perform a DB backup.
  - b. Access the JMX console and run the following methods under **service=DAL services**:
    - **rebuildModelViews**
    - **rebuildModelDBSchemaAndViews**

**Caution:** Invoking the above JMX method could drop the following: attributes, tables, indexes. Random usage is prohibited.

- If the login takes a long time when navigating to the Modeling modules, go to Infrastructure Settings Manager and set the value of the **mam.gui.automation.flow.mapping.enabled** setting to false. This disables the Automation Flow functionality but improves the login time for the Modeling modules.
- For TQL queries to be valid, they must comply with certain restrictions.

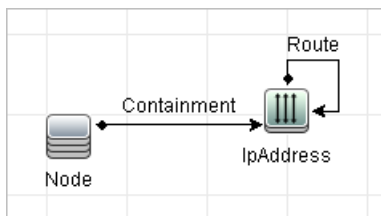
This section includes the following topics:

- ["Understanding Validation Restrictions" below](#)
- ["Impact Analysis TQL Query Validation" on the next page](#)
- ["Enrichment TQL Query Validation" on page 187](#)

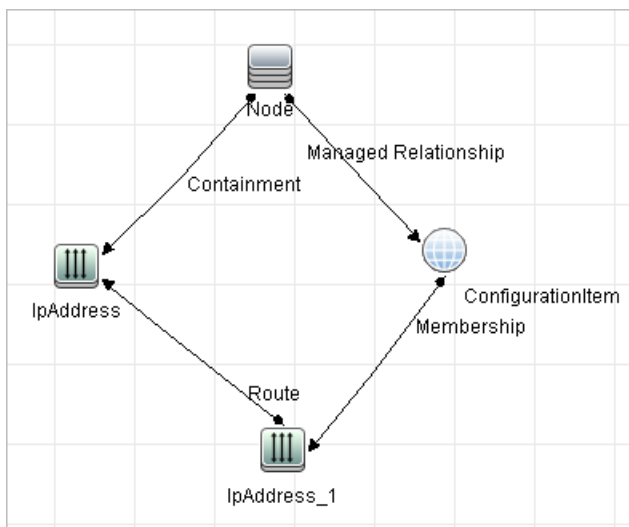
## Understanding Validation Restrictions

For Impact Analysis, Discovery, and Enrichment TQL query types to be valid, they must comply with the following restrictions:

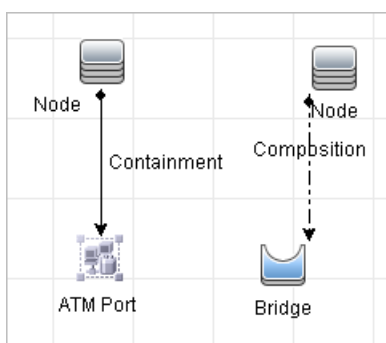
- **Unique Names.** TQL query elements must have unique names.
- **Self Relationships.** A TQL query must not contain self relationships, that is, a relationship must not lead from a query node to itself, as the following example illustrates:



- **Cyclic Graph.** The TQL query structure cannot be a closed circle, as shown in the following example:



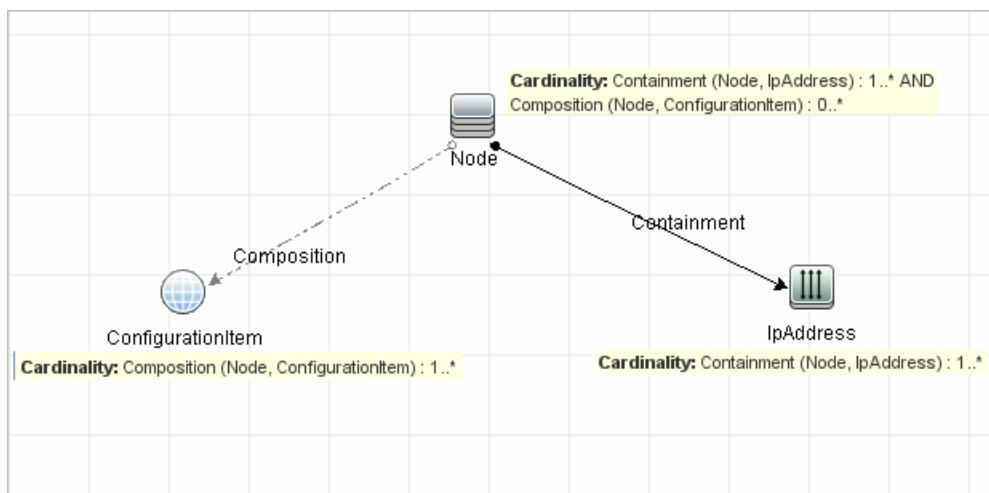
- **Separate Query Nodes and Groups.** All the TQL query nodes must be linked to one another, that is, the TQL query cannot contain separate query nodes or groups, as the following example illustrates:



## Impact Analysis TQL Query Validation

Impact Analysis TQL queries must also comply with the following restrictions:

- **Number of query nodes.** An Impact Analysis TQL query must consist of at least two query nodes.
- **Trigger and affected query nodes must be connected.** There must be a path of relationships from the triggered query node to the affected query nodes.
- **Selecting query nodes to function as Impact Analysis triggers.** When selecting query nodes to function as Impact Analysis triggers, the query nodes must comply with the following restrictions:
  - You can select more than one query node as a trigger. However, you cannot define a query node both as affected and as a trigger.
  - If a query node has a relationship whose minimum limit is 0 (meaning that one of its ends does not necessarily have a query node linked to it), the query node that is linked to its other end cannot be a root cause query node (because it may or may not exist in the TQL query). For details about minimum limits, see "[Cardinality Tab](#)". For example, **Configuration Item** cannot be either a root cause or affected query node because it is connected to the query node with a **Min** limit of 0.



**Note:** A query node that is hidden cannot be a root cause or an affected query node.

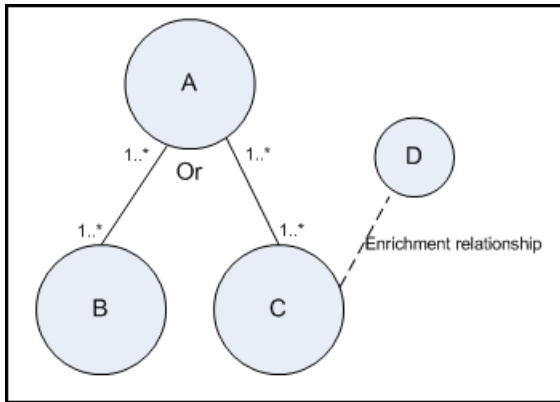
- **The connection between trigger and affected query nodes.** The trigger query node and affected query nodes you define must be connected by a path of relationships from the triggered query node to the affected query nodes.

## Enrichment TQL Query Validation

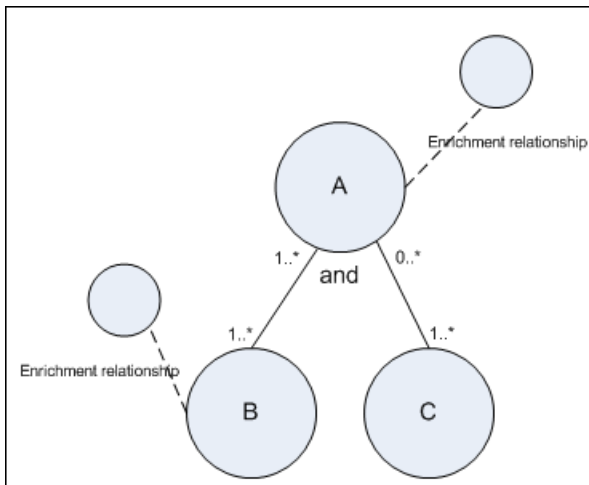
Enrichment TQL queries must comply with the following restriction:

- **Required elements.** You cannot perform Enrichment on a non-required query node, that is, a query node that does not necessarily appear in the TQL query results.

**Example 1.** In this example, the TQL query results can be either **A** and **B** or **A** and **C**. Therefore, you cannot add an Enrichment query node to query nodes **B** or **C** because they are not required elements. You can add an Enrichment query node to query node **A** because it always appears in the TQL query results. For details on how to add Enrichment query nodes and relationships, see [Add Enrichment Query Nodes and Relationships to an Enrichment TQL Query](#).



**Example 2.** In this example, both **A** and **B** are required elements that always appear in the TQL query results. Only **C** is not a required element because it has a cardinality of 0. Therefore, you cannot add an Enrichment query node to it.



## Troubleshooting and Limitations – CI Selector

This section describes troubleshooting and limitations for the CI Selector.

## Unavailable Views and CIs

The View list in the CI Selector may not display all views in the CMDB, or it may not display the contents of a view, for any of the following reasons:

- The View list includes only the views for which you have the necessary permissions. Similarly, Search mode is only available if you have the **Allow Search** general action permission. To set permissions, select **Managers > Administration > Roles Manager**. For more information, see Roles Manager in the *Administer section of the UCMDB Help*.
- Views that are currently inactive appear in red in the View list, but they cannot be selected. In IT Universe Manager, inactive views appear in faded text.
- Out-of-the-box views for which you do not have a license may appear in the View list, but these views do not contain CIs. For information on the out-of-the-box views, see [Predefined Folders and Views](#).

**Note:** After deleting one or more query nodes from a TQL query, it can take time for changes to be updated to the view; meanwhile, the removed CIs appear in the view. If you select one of these CIs before it is updated, an error message is displayed. Click the **Refresh** button to update the view.

## 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 CMS Troubleshooting Guide (Configuration Management System (CMS) 2018.08)**

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@microfocus.com](mailto:cms-doc@microfocus.com).

We appreciate your feedback!