



Universal CMDB

Software Version: 10.33

Data Flow Management Guide

Document Release Date: September 2017 (Second Edition)

Software Release Date: July 2017



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 - 2017 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.

Document Changes

Publication Date	Summary of Changes
10.33 (2nd Edition, September 2018)	Added clarification that Call Home does not work when DirectAccess is involved in "Call Home Overview" on page 167 .

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

Part I: Introduction	17
Chapter 1: Introduction to Data Flow Management	18
Data Flow Management Overview	18
Discovery	19
Data Flow Management Modules	19
Reconciliation	22
Data Flow Management Architecture	22
Data Flow Management Concepts	23
Part II: Data Flow Management Setup	28
Chapter 2: Data Flow Probe Setup	29
Data Flow Probes and Probe Clusters	30
UCMDB Integration Service	30
Cluster Range Distribution Policy	31
Limiting IP Movement in a Cluster	34
Job Execution Policies	36
Running Jobs When a Job Execution Policy Is Running	37
Data Flow Probe Auto Upgrade	37
Data Flow Probe Auto Upgrade Overview	37
Data Flow Probe Auto Upgrade Workflow	39
Troubleshooting Probe Auto Upgrade	40
Effects of Range Type on Discovery Workflows	46
Using HTTPS Port 8453 as Default for Data Flow Probe	48
How to Install a Second Data Flow Probe on a Windows Machine	48
How to Set Master Key for Password Encryption on Data Flow Probe	53
How to Add Data Flow Probes to UCMDB	54
How to Add Probe Clusters to UCMDB	55
How to Start a Data Flow Probe	56
How to Stop a Data Flow Probe	58
How to Change the Data Flow Probe Default Domain	58
How to Change the Data Flow Probe Port	59
How to Move Resources From One Domain to Another Domain	60
How to Change the UCMDB Integration Service Default Domain	61

How to Check the UCMDB Integration Service Status	62
How to Limit IP Movement in a Cluster	63
How to Update the Data Flow Probe's IP Address	64
How to Update the Data Flow Probe Memory Size	65
How to Define Owner Tenants on Data Flow Probes	66
How to Configure the Number of Connections to Other Machines	67
How to Configure Periodic Data Flow Task Updates	68
How to Prevent Probes from Sending Touch Information Simultaneously	70
How to Encrypt/Decrypt IP Ranges Information on the Probes	71
How to Configure the Data Flow Probe to Automatically Delete CIs	72
How to Delete Unsent Probe Results	73
How to Clear Data Flow Probe Data	73
How to Clear UCMDB Integration Service Data	74
How to Deploy a Data Flow Probe CUP	75
How to Deploy a Data Flow Probe CUP Manually	76
How to Align the Data Flow Probe CUP with the UCMDB Server CUP ..	77
How to Uninstall Probe CUPs Manually	79
How to Set Maximum Objects for Insert Results	80
Data Flow Probe Process Ports	80
DataFlowProbe.properties File	83
DataFlowProbe.properties Parameters	84
DataFlowProbeOverride.properties File	97
Data Flow Probe Database Scripts	98
Data Flow Probe Log Files	99
Data Flow Probe Setup User Interface	103
New/Edit Policy Dialog Box	103
Add New Domain Dialog Box	104
Data Flow Probe Setup Window	105
Domains and Probes Details Pane	110
<Domain> Details Pane	111
<Protocol> Details Pane	113
Protocol Parameter Dialog Box	115
Cluster Details Pane	119
Data Flow Probe Details Pane	122
Passive Discovery Probes Pane	126
Passive Discovery Probe Details Pane	128

New/Edit Range Dialog Box	131
Troubleshooting and Limitations – Data Flow Probe Setup	136
Data Flow Probe Setup - Troubleshooting	136
Data Flow Probe Setup - Limitations	140
Troubleshooting Probe Auto Upgrade	140
Chapter 3: Data Flow Probe Status	147
How to View Job Information on the Data Flow Probe	147
Data Flow Probe Status User Interface	148
<Job Name> Dialog Box	148
Data Flow Probe Status Window	149
Discovery Job Operation Commands	153
Job Operation Parameters	160
Chapter 4: Universal Discovery Agents	163
Universal Discovery Agent Overview	163
Universal Discovery Agent Deployment	164
Universal Discovery Agent Certificates	166
Using Certificates	166
Call Home Overview	167
FDCC/USGCB Support	169
How to Create New Certificates for Universal Discovery Agent	171
How to Customize Platforms for Universal Discovery Agent Deployment	172
How to Install the Universal Discovery Agent Manually	174
How to Install Universal Discovery Agent to Run Under a Non-Root Account on UNIX	177
How to Configure Call Home	178
How to Enable Changing the Default Port Number for Call Home	179
How to Specify Data and Temp Folder Locations when Installing or Updating the Universal Discovery Agent for UNIX	180
How to Completely Uninstall the Universal Discovery Agent	181
Agent Installation Wizard Overview	182
Agent Installation User Interface	183
Agent Installation Wizard	183
Set Up Type Page	183
Agent Configuration for Complete Installation Page	184
Software Utilization Page	186
Uninstall Options Page	186

Uninstall Type Page	187
Discovery Node Disk Requirements	187
Universal Discovery Agent Installation Resources	188
Universal Discovery Resources for Windows	189
Universal Discovery Resources for Mac	191
Universal Discovery Resources for UNIX	191
Universal Discovery Agent File Locations	195
Software Identification Tags	197
Chapter 5: Scanner Scheduler	202
Scanner Scheduler Overview	202
How to Deploy the Scanner Scheduler	202
Scanner Scheduler Resources	205
Chapter 6: Store and Forward	210
Store and Forward Overview	210
How to Install the Store and Forward Server	210
Store and Forward Installation Wizard	214
Destination Folder Page	214
Data Files Page	215
Store and Forward Configuration Page	215
SSL Certificate Generation Page	216
Store and Forward Resources	216
Store and Forward Commands	221
Part III: Adapter Management	223
Chapter 7: Adapter Configuration	224
Identifying Running Software by Processes	224
Automatically Deleted CIs and Relationships and Candidates for Deletion CIs	226
How to Configure Adapter Settings	227
How to Define the Owner Tenant Adapter Parameter	228
How to Configure Full Population Run	228
How to Configure Global Probe Result Filtering	229
Configure Filtering in UCMDB	230
Configure Filtering Using the globalFiltering.xml File	231
How to Configure CI Aging Settings	234
How to Define CITs to be Deleted by Java-based Population Adapters	235
How to Attach Discovery Documentation to a Discovery Package	235

How to Attach a Readme to a Discovery Package	236
How to View Discovery Resource History	237
How to Create and Configure Mapping Files Using the Visual Mapping Tool	239
Prerequisites	239
How to Open and View a Supported Mapping File Using the Visual Mapping Tool	239
How to Create a Mapping File Using the Visual Mapping Tool	241
How to Edit and Update a Mapping File Using the Visual Mapping Tool	242
How to Synchronize Class Model Changes to External System through Push Adapter	249
Pre/Post-Scan Script Editor	251
Pre-Scan and Post-Scan Scripts	251
Adapter Management User Interface	252
Adapter Definition Tab	253
Adapter Configuration Tab	259
Adapter Management Window	265
Adapter Source Editor Window	265
Attributes Assignment Editor Dialog Box	267
Choose Discovered Class Dialog Box	268
Configuration File Pane	269
Edit Process Dialog Box	271
Find Resource/Jobs Dialog Box	272
Find Text Dialog Box	273
Input Query Editor Window	274
Mapping Tool Editor Window	277
Permission Editor Dialog Box	284
Resources Pane	285
Script Pane	288
Software Identification Rule Editor Dialog Box	290
Software Library Dialog Box	292
Global Filtering Dialog Box	293
Internal Configuration Files	295
Chapter 8: Discovery Rules Engine	296
Discovery Rules Engine Overview	296
Discovery Rules Syntax	297

Example 1	297
Example 2	298
Example 3	299
Example 4 (link rules)	300
Explanation of Examples	301
How to Define Discovery Rules	306
How to View Discovery Rules in JMX	307
How to Disable the Discovery Rules Engine	308
Part IV: Integrations	309
Chapter 9: Integration Studio	310
Integration Studio Overview	310
Population	311
Federation	312
Data Push	314
Integration in a Multi-Tenancy Environment	316
How to Work with Federated Data	317
How to Work with Population Jobs	318
How to Work with Data Push Jobs	320
Live Data Push Jobs	323
How to Set Up an Integration Point	324
How to Save an Integration Point Configuration as an Adapter Default	326
How to Remove Adapter Defaults	329
How to Deploy a Package to a Remote Data Repository	330
How to Configure Probe IP Ranges with Active Directory	333
How to Increase the Number of Threads for Data Push Jobs	334
Integration Studio User Interface	335
Data Push Tab	336
Deploy Package to Remote Data Repository using <Integration Point>	337
Federation Tab	337
Integration Jobs Pane	339
Integration Point Pane	346
Integration Studio Page	348
New Integration Job/Edit Integration Job Dialog Box	349
Job Definition	350
Scheduler Definition	351

New Integration Point/Edit Integration Point Dialog Box	353
Population Tab	356
Select Adapter Dialog Box	357
Topology CI Creation Wizard	358
Topology Preview	359
Define CI: <CI name>	359
Define Credentials	360
Topology Creation	361
Summary	361
Limitations – Integration Studio	362
Chapter 10: Integrating Multiple CMDBs	364
Integrating Multiple CMDBs Overview	364
Use Cases – Multiple CMDB Deployments: Discovery-CMS Solution ..	365
Multiple Deployments with Version 9.x/10.x CMDBs Using Population ..	366
Multiple Deployments with Version 9.x/10.x CMDBs Using Data Push ..	370
Federation in Version 9.x/10.x CMDBs	371
How to Perform Initial UCMDB-UCMDB Synchronization	372
How to Configure Global ID Generation	373
How to Use SSL with the UCMDB 9.x/10.x Adapter	374
How to Set Up Integrations Between Multiple CMDBs	375
How to Enable Scheduling Pushback of Global IDs When Using UCMDB 10.x Adapter	379
How to Push Data from Authorized State to Actual State	380
How to Protect CIs from Being Deleted on Target CMDBs during Data Push	381
Troubleshooting and Limitations – Multiple CMDB Integration	383
Chapter 11: Integrating UCMDB with CyberArk Enterprise Password Vault	386
Overview	387
Deployment	387
How the CyberArk Integration Works	388
Supported Versions	388
Supported CyberArk Versions	388
Supported Probe Types	388
Supported Protocols	389
How to Configure CyberArk Integration	389
CyberArk Integration Configuration Workflow	391

How to Configure CyberArk Integration	392
How to Create and Configure CyberArk Account for the Integration ..	399
How to Add CyberArk Credential for Protocols from JMX	407
How to Calculate Hash Code for JARs with Annotation	408
How to Set a Default List of CyberArk Properties Using JMX	409
CyberArk Integration Troubleshooting and Limitations	411
Part V: Universal Discovery	415
Chapter 12: Introduction to Universal Discovery	416
Universal Discovery Overview	416
Universal Discovery Community	416
Agent-based vs. Agentless Discovery Overview	417
Script-based vs Scanner-based Discovery	417
Chapter 13: Zone-based Discovery	420
Zone-based Discovery Overview	420
Management Zone Ranking	421
Discovery Troubleshooter	424
Configure IP Ranges for Management Zones at Domain Level	425
How to Run Zone-based Discovery	428
How to Create Management Zones	429
How to Define Discovery Activities in a Management Zone	431
How to Create Discovery Activity Templates	431
How to Define Custom Discovery Activities from an Activity Template ..	432
How to Rank Management Zones	434
How to Configure Global Management Zone Settings	435
How to Organize the Management Zones Tree	436
How to Migrate Management Zone Folders	437
How to Migrate Management Zones	438
How to Rename Management Zones	439
How to Rename Activities	440
Zone-based Discovery User Interface	441
Discovery Troubleshooter Wizard	441
Activity Instances Mapping Page	442
Target Host Page	443
Additional Information Is Required Page	444
Investigate Missing Node CI Page	444
Retrieve Running Software CIs Page	445

New/Edit Management Zone Dialog Box	446
New/Edit Range Dialog Box	450
Find Management Zone Dialog Box	454
Management Zone Ranking Dialog Box	454
Global Settings Dialog Box	455
Zone-based Discovery View	457
Chapter 14: Module/Job-based Discovery	466
Discovering Running Software	466
Modules/Jobs-based Discovery Overview	467
Viewing Permissions While Running Jobs	467
Discovered CIs and Relationships In a Multi-Tenancy Environment	468
How to Verify Whether a Discovery Job Supports IPv6	470
How to Run Module/Job-based Discovery	470
How to Manually Activate Modules/Jobs/CIs	473
How to Discover Running Software – Scenario	473
How to Define the Owner Tenant For a Discovery Job	476
Module/Job-based Discovery User Interface	477
Create New Discovery Job Dialog Box	477
Discovery Modules/Jobs Window	481
Discovery Modules/Jobs – Discovery Modules Pane	482
Right-Click Menu	484
Discovery Module/Jobs – Details Tab	486
Discovery Module/Jobs – Dependency Map Tab	489
Discovery Modules/Jobs – Properties Tab	490
Discovery Permissions Window	495
Discovery Scheduler Dialog Box	496
Find Jobs Dialog Box	499
Time Templates Dialog Box	500
Trigger Query Editor Window	501
Chapter 15: Inventory Discovery	505
Inventory Discovery Overview	507
Inventory Discovery Scanners	509
Inventory Discovery Deployment Overview	512
Scan Files	516
Processing Scan Files	519
Scan File Processing Power	520

XML Enricher	521
Software Application Index (SAI) Files	523
Filter.zsai File	523
Overview	523
Filtering Mechanism	524
How to Create and Update Filter.zsai Using the SAI Editor	524
How to Deploy Filter.zsai to UCMDB	524
XML Enricher Log Files	525
Application Teaching	527
Using Rules to Teach Applications	527
Overview	527
How to Use Rules to Teach Applications	530
Enriched Scan File Structure	530
Hardware and Software Recognition	532
App Store Applications	534
Custom Hardware or Asset Mapping	534
Inventory Tools	534
BDNA Normalize Integration	536
Debug Mode	537
Software Utilization	538
Discovery Options for Client IP Ranges	538
How to Run Inventory Discovery	538
How to Run Inventory Discovery Manually	539
How to View Discovery Status of an Inventory CI in JMX	541
How to View Agent Deployment Log for an Inventory CI in JMX	544
How to Edit Pre-/Post-Scan Scripts	544
How to Set Up Asset Fields for Data Collection	547
Asset Fields	548
Asset Field Parameters	550
Calculated Fields	550
Derived Fields	554
Order of the Fields in the Form	557
How to Set Up Asset Fields for Data Collection - Example	558
How to Set up the Scanner to Handle Delta Scan Files in Manual Deployment Mode	561
How to Configure XML Enricher to Suit the Probe Deployment Mode ...	564

How to Configure the Maximum Number of Threads to Process Scan Files	567
How to Check XML Enricher Health Using JMX	568
How to Limit the XML Enricher Port to Allow Local Connection Only	568
How to Reprocess Scan Files	569
How to Import SAIs to the Data Flow Probe	569
How to Import Normalization Rules to the Data Flow Probe	570
How to Configure and Optimize Inventory Discovery	571
How to Configure Analysis Asset Fields	572
How to Map Scan File Attributes to UCMDB	572
Mapping Hardware or Asset Fields to UCMDB - Use-Case Scenarios ..	574
How to Set Extract Options	577
Configure Filtering in UCMDB	579
How to Enable Discovery of App-V Applications	580
Application Virtualization Supported Technologies	581
How to Rename Scanner Executable Files	581
How to Integrate BDNA Normalize with Universal Discovery	582
How to Discover Client IP Ranges Without SNMP	584
How to Discover Windows Device Drivers using the Inventory Discovery by Scanner Job	584
Scanner Command Line Parameters Overview	585
Scanner Command Line Parameters	586
Scanner Information Type Parameters	593
Scanner File Locations	595
Web Server Configuration for Saving Scan Files via HTTP	596
XML Enricher Directory Structure	598
Enriched XSF File Structure	600
Inventory Discovery User Interface	600
Hardware Mapping Configuration Dialog Box	600
Scanner Generator Wizard	605
Scenario Page	605
Standard Configuration Page	607
Collection Page	609
Hardware Data Page	609
Software Data Page	615
Software Details Page	617

File Information to Store tab > Select Files to Process Dialog Box	627
Asset Data Page	630
Asset Field Configuration Dialog Box	632
Scanner Options Page	635
Scanners to Generate Page	645
Generating Scanners Page	649
XML Enricher: Software Recognition Configuration Dialog Box	650
Chapter 16: Just-In-Time Discovery	655
Just-In-Time Discovery Overview	655
How to Configure Just-In-Time Discovery	655
Chapter 17: Discovery Progress and Results	658
Managing Problems With Error Reporting	658
Error Table in Database	658
Data Validation on the Data Flow Probe	659
Class Model Data Validation	659
Content Data Validation	659
Filtering Discovery Results	660
How to View the Current Status of Discovered CIs	661
How to Find Discovery Errors	661
How to Manage Discovery Errors	662
How to Enable Content Data Validation	663
Content Data Validation Jython Scripts	664
Handling Errors and Warnings	665
Discovery Progress and Results User Interface	666
Choose CIs to Add Dialog Box	667
Discovered/Created/Last Updated CIs Dialog Box	668
Discovery Progress Dialog Box	670
Discovery Results Tab/Pane	678
Related CIs Window	680
Show Results for Triggered CI Dialog Box	681
Chapter 18: Software Library	682
Software Library Overview	682
Software Library User Interface	682
SAI Files Pane	682
Software Library Window	684

Advanced Search Dialog Box	689
Chapter 19: Express Teaching	691
Express Teaching Overview	691
Unrecognized Files	691
How to Teach Applications Using Express Teaching Wizard	692
How to Deploy User SAI Files	694
How to Clean Up Unrecognized Files	694
How to Clean Up Aged Unrecognized Files	695
How to Send a Publisher File to Micro Focus	696
Express Teaching User Interface	697
Express Teaching Wizard	697
Select a Probe Page	697
Select an Application Page	698
Select Files Page	699
Select Application Details Page	701
Review Data Page	702
Summary Page	703
Chapter 20: Software License Compliancy	704
Software License Compliancy Overview	704
Software Utilization	704
How to Calculate License Compliancy for IBM	705
How to Calculate Licenses for Oracle	707
How to Configure Software Utilization	708
Part VI: Service Discovery	709
Chapter 21: Business Service Discovery	710
Service Discovery Overview	710
How to Create Service Discovery Activities	711
How to Edit Service Discovery Activities	712
How to Run Service Discovery	712
Service Discovery User Interface	714
Discovery Progress Dialog Box	715
Discovery Status – Progress Tab	722
Discovery Status – Results Tab	729
New/Edit Service Discovery Activity Dialog Box	731
Service Discovery Activity Templates Dialog Box	733
Service Discovery Page	734

Part VII: Reconciliation	738
Chapter 22: Data Reconciliation	739
Reconciliation Overview	739
Identification Service	740
Identification and Match Criteria Configuration	743
Examples of Identification Configuration	745
Data-In Service - Populating UCMDB	746
Server-Side Data Normalization	749
Multiple CI Matching - Example 1	750
Multiple CI Matching - Example 2	751
How to Specify High Priority Callers for the Data-In Operations	753
Merging Matched CIs Using Reconciliation Priority Rules	753
How to Create an Identification Rule	754
How to Add Reconciliation Priorities to a CI Type	756
Identification Rule Schema	757
Reconciliation Priority Window	764
How to Add Reconciliation Priority for API-based Integrations	768
How to Enable Redundant Reverse Check	769
How to Enable Attribute Name Verification during the Matching Phase of Identification	769
How to Modify the Maximum Number of Threads for the Data-In Service	770
How to Enable CI Type Tenant Owner Verification during the Matching Phase of Identification	771
Tenant Owner Related Known Issues, Problems, and Workaround	773
Appendix A: Troubleshooting and Limitations – Data Flow Management	776
Troubleshooting – Universal Discovery	776
How to View the Status of AM and SM Integration Jobs	780
How to View the Integration Point Log	782
Limitations – Universal Discovery	782
Send documentation feedback	784

Part I: Introduction

Chapter 1: Introduction to Data Flow Management

This chapter includes:

Data Flow Management Overview	18
Data Flow Management Architecture	22
Data Flow Management Concepts	23

Data Flow Management Overview

This section gives an overview about the Universal Discovery and Integrations.

This section includes:

- ["Integrations" below](#)
- ["Discovery" on the next page](#)
- ["Data Flow Management Modules" on the next page](#)
- ["Reconciliation" on page 22](#)

Integrations

You use the Integration Studio to set up integrations with external data repositories.

You can set up the following types of integrations:

- **Population.** Integration that populates the CMDB with CI and relationship information.
- **Federation.** Integration that retrieves CIs and relationships from an external repository whenever the data is requested in an ad hoc fashion.
- **Data Push.** Integration that pushes CIs and relationships from the CMDB to an external data repository.

Each integration adapter supports certain types of integrations. For example, an integration adapter that supports both population and federation types can retrieve data periodically for storage within the CMDB or upon query time; both of these configurations can co-exist within a single integration.

Discovery

The Discovery process is the mechanism that enables you to collect information about your IT infrastructure resources and their interdependencies. Discovery automatically discovers and maps logical application assets in Layers 2 through 7 of the Open System Interconnection (OSI) Model.

Discovery discovers resources such as installed and running applications, network devices, servers, and so on. Each discovered IT resource is delivered to, and stored in, the configuration management database (CMDB) where the resource is represented as a managed CI.

Discovery is an ongoing, automatic process that continuously detects changes that occur in the IT infrastructure and updates the CMDB accordingly. You can discover nodes using agent-based or agentless discovery.

After configuration, Universal Discovery automatically discovers the network on which the Data Flow Probe is located, the Node on which the Probe resides, and the Node's IP address. A CI is created for each of these objects. These discovered CIs populate the CMDB. They act as triggers that activate discovery jobs. Every time a job is activated, the job discovers more CIs, which in turn are used as triggers for other jobs. This process continues until the entire IT infrastructure is discovered and mapped.

For details on out-of-the-box discovery packages and supported integrations, see the *Universal CMDB Discovery and Integrations Content Guide*.

Data Flow Management Modules

Note: The Data Flow Management modules are available only when you are logged into UCMDDB in **Actual** state.

Data Flow Management (DFM) includes the following application modules:

Integration Studio

The Integration Studio enables you to set up UCMDDB integrations to define and control data flows from

external data repositories to the CMDB, or from the CMDB to external data repositories.

Note: You must have a valid license to integrate with third-party products. Contact your Micro Focus Account Manager for more details.

For more information, see ["Integration Studio" on page 310](#).

Universal Discovery

Note: You must have a valid license to use this module. Contact your Micro Focus Account Manager for more details.

The Universal Discovery module enables you to manage the process for discovery of the CIs and relationships of your IT infrastructure. You control the process by activating discovery jobs.

You can manage discovery by partitioning your enterprise into zones and activating discovery activities (groups of discovery jobs) to discover infrastructure (IPs, nodes), basic software (shallow running software including application servers, databases, and web servers), deep database configuration, and inventory (for example, CPUs, installed software, logical volumes), among other data.

You could also control the process by manually activating discovery jobs. You can choose to activate all or some of the jobs in a module. You can also edit discovery jobs, and schedule a job to run at a certain time.

For more information, see ["Introduction to Universal Discovery" on page 416](#).

Data Flow Probe Setup

The Data Flow Probe Setup module enables you to add Data Flow Probes to the system and to manage existing Data Flow Probes. You define the network range that each Data Flow Probe covers.

You also manage communication credentials from the Data Flow Probe Setup module. These credentials are used for both discovery and integration purposes.

Universal Discovery integrates with Real User Monitor (RUM) to provide passive, real-time discovery and monitoring of traffic in a given environment. This is known as the Just-In-Time discovery mechanism. You manage IP ranges and port ranges for passive discovery probes from the Data Flow Probe Setup module.

For more information, see ["Data Flow Probe Setup" on page 29](#).

Reconciliation Priority

The Reconciliation Priority module enables you to specify the reconciliation priority for a particular integration point, CIT, or attribute.

For more information, see ["How to Add Reconciliation Priorities to a CI Type" on page 756](#).

Adapter Management

The Adapter Management module enables you to edit adapters, scripts, configuration files (including discovery rules), and scanner configurations. You can also replace or remove external resources needed for discovery or integration from this module.

For more information, see ["Adapter Configuration" on page 224](#).

Universal Discovery Community

The Universal Discovery Community website provides you with a convenient way to obtain the latest CMS Discovery and Integration Content Pack. The Content Pack provides all of the out-of-the-box discovery packages and integration adapters required for performing discovery and integrating with other Micro Focus products and third-party sources.

For more information, see ["Universal Discovery Community" on page 416](#).

Data Flow Probe Status

The Data Flow Probe Status module enables you to view the current status of a particular Data Flow Probe: which discovery or integration job the Probe is currently running, execution statistics, and so on.

Note: Data Flow Probes installed on *Windows* platforms only are displayed in this module.

For details, see ["Data Flow Probe Status" on page 147](#).

Software Library

The Software Library module enables you to view the contents of the SAI files that are contained in UCMDB. This module also enables to you teach applications to Universal Discovery.

For more information, see ["Software Library " on page 682](#) or ["Express Teaching Overview" on page 691](#).

Reconciliation

The Reconciliation process consists of two important steps:

- **Identification.** The process by which CIs and relationships within the CMDB are identified against existing CIs within the CMDB, other CIs within the same bulk, or CIs coming from various federated data sources.
- **Reconciliation Priority.** The process by which the CMDB reconciliation engine decides how to deal with conflicting data. When conflicting values are given for the same CI attribute by different integrations, the CMDB reconciliation engine resolves the conflict by looking at the reconciliation priority assigned to each integration.

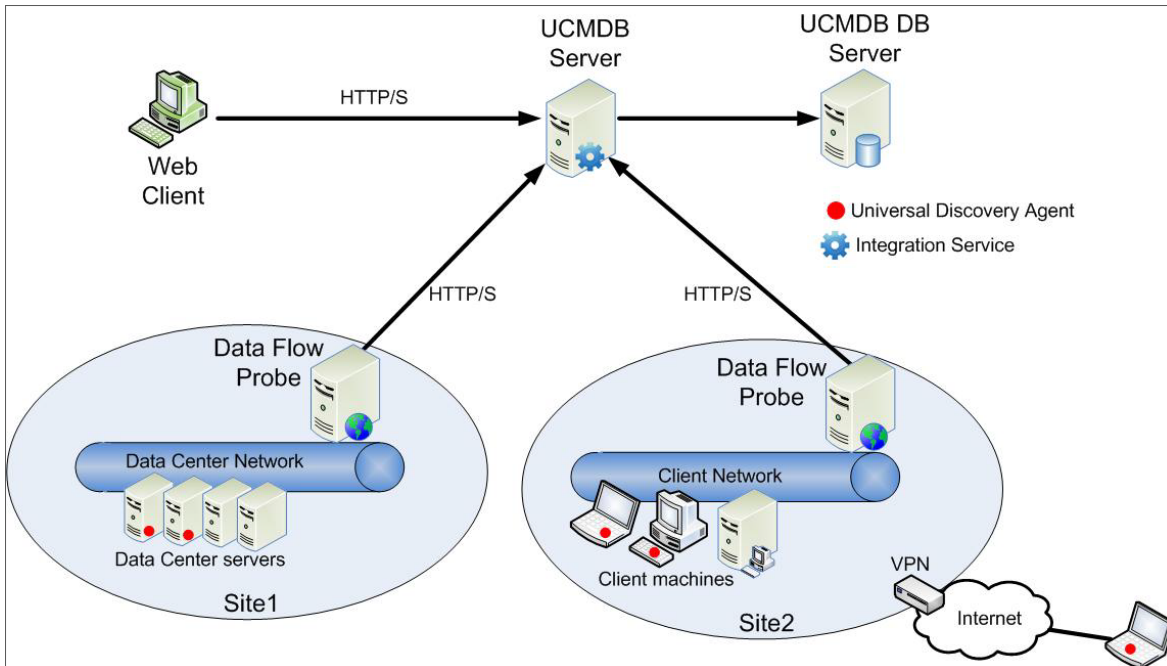
By default, unless you customize the reconciliation priorities within the Reconciliation Priority Manager, the CMDB reconciliation engine uses the last reported value as the most accurate, that is, all integrations have exactly the same priority.

For more information about reconciliation, see ["Data Reconciliation" on page 739](#).

For details about the Reconciliation Priority Manager, see ["Reconciliation Priority Window" on page 764](#).

Data Flow Management Architecture

Data Flow Management architecture is deployed as follows:



- The Data Flow Probe is responsible for integration of data to and from external data repositories and for performing discovery.
- The Data Flow Probe initiates communication with the UCMDB Server using HTTP or HTTPS traffic, enabling the product to bypass possible firewalls.

Data Flow Management Concepts

This section describes the main topics of Universal Discovery:

Data Flow Probe

The **Data Flow Probe** is the main component responsible for requesting tasks from the server, scheduling and executing discovery and integration tasks, and sending the results back to the UCMDB Server. You define a range of network addresses for a specific, installed Data Flow Probe. Each Data Flow Probe is identified by its name, chosen during the Data Flow Probe installation process.

Probe Cluster

A **probe cluster** is a logical container for a number of Data Flow Probes. You define a network range for a cluster. The cluster is responsible for calculating how to distribute the IPs in its network range to ensure a maximum balance of its IPs among its Probes.

UCMDB Integration Service

If your remote managed data repositories are accessible from the UCMDB server machine, you can use the UCMDB Integration Service (installed on the UCMDB Server) instead of a Data Flow Probe, to run non-Jython-based integrations.

This enables running non-Jython-based integrations without the need for using Data Flow Probe resources, leaving the Data Flow Probe resources available for other discovery tasks.

Passive Discovery Probe

A passive discovery probe is an Micro Focus Real User Monitor (RUM) probe that is configured to integrate with a Data Flow Probe to provide passive, real-time discovery and monitoring of traffic in a given environment. This is known as Just-in-Time discovery.

Communication Protocols

Discovery of the IT infrastructure components uses protocols such as SNMP, WMI, JMX, Telnet, and so on for communication. For details about each protocol, see the *UCMDB Discovery and Integrations Content Guide - Supported Content*.

Agent-based Discovery

To collect inventory information, you can deploy Universal Discovery agents (UD agents) on client or server machines. The UD agent provides a secured communication channel between the Data Flow Probe and the nodes being discovered. After setting up the secure communication channel, Universal Discovery deploys and activates scanners onto the nodes being discovered. The Scanners scan the nodes for inventory information and store the scanned results in scan files which are downloaded to the Data Flow Probe through the secured communication channel established with the UD agent.

When the UD agent is installed, collection of software utilization information is enabled. The UD agent also enables you to benefit from the Call Home feature. Call Home is useful in the case where a node was unavailable for scanning for a long period. It enables the UD agent to notify the Data Flow Probe that the node is currently available for scanning.

Agentless Discovery

Although agentless discovery does not require the installation of dedicated agents on the servers that are to be discovered, it does depend on native OS or standard agents that are already installed such as SNMP, WMI, TELNET, SSH, NETBIOS, and others. Other discovery capabilities are based on application-specific protocols such as SQL, JMX, SAP, Siebel, and so on. For details on supported protocols, see the *UCMDB Discovery and Integrations Content Guide - Supported Content*.

Discovery and Integration Adapters

Adapters on which discovery jobs and integrations are based.

- **Jython Adapter.** An adapter based on a set of Jython scripts that are executed sequentially.
- **Java Adapter.** An adapter based on Java code that implements the various DFM interfaces and is wrapped in a JAR file.
- **Generic DB Adapter.** An adapter that uses SQL queries and maps database tables to CIs and relationships by using an ORM file.
- **Generic Push Adapter.** An adapter that uses a mapping file and Jython scripts to push data to an external data repository.

The adapters themselves do not contain information about the target to which they are to connect and from which they are to retrieve information. For data flow to be configured correctly, adapters require further context information, which can include an IP address, port information, credentials, and so on.

For discovery adapters (adapters used for performing discovery), the additional information is brought from the Trigger CIs associated with the discovery jobs; for integration adapters, the information is manually fed when creating the integration or taken from the selected Trigger CI.

For details on making adapter changes, see ["Adapter Management Window" on page 265](#). For details on creating adapters, see Adapter Development and Writing in the *Universal CMDB Developer Reference Guide*.

Discovery Modules

The module is a grouping of discovery jobs that logically belong together, can be operated and managed together, and so on. This helps to reduce clutter in the main view when many jobs need to be written, and can also offer better manageability.

When creating a job, you should add it to a module or create a new module. If you are creating several jobs, the best practice is to split them into logical groups and assign them to modules accordingly.

Discovery Modules support a hierarchy of folders, to facilitate easy finding of the relevant discovery capability.

Management Zones

A Management Zone is a region in the network defined by a collection of IP ranges. A region of an organization's infrastructure should be defined as a Management Zone when you want to discover all the managed objects of the region using the same scheduling policy and parameters.

You can set up multiple Management Zones to run different instances of a discovery activity in different data centers in your enterprise.

For information, see ["Zone-based Discovery" on page 420](#).

Discovery and Integration Content Pack

The latest discovery and integration content for UCMDB are installed in a Content Pack during the installation of UCMDB. Updates to the Content Pack are available for download via the [ITOM Marketplace](#). For details on downloading and installing Content Pack updates, see the ["Universal Discovery Community" on page 416](#).

Integration Points

Integration points are entities used to set up UCMDB integrations. Each integration point is created with a selected integration adapter and the additional configuration information required to set up the integration. For details on creating integration points, see ["Integration Studio" on page 310](#).

Discovery Jobs

A job enables reuse of a discovery adapter for multiple discovery process flows. Jobs enable scheduling the same adapter differently over different sets of triggered CIs and also supplying different parameters to each set. You can launch a discovery by activating the relevant set of discovery jobs that must be run. Relevant trigger CIs are automatically added to the activated discovery jobs based on their trigger queries.

Discovery Activities

You use discovery activities within Management Zones to discover infrastructure (IPs, nodes), basic software (shallow running software including application servers, databases, and web servers), deep database configuration, and inventory (for example, CPUs, installed and virtualized software, logical

volumes), among other information.

Input Queries

Note: Input queries refer only to discovery adapters and Jython integration adapters.

Each adapter is assigned an input query that is used as follows:

- **The input query defines a minimal set of requirements** for every Trigger CI included in a discovery job or integration point that triggers this adapter. (This is true even when no trigger query is associated with the job.)

For example, an input query can query for IPs related to nodes with an SNMP agent installed and discovered on them, that is, only IPs with installed SNMP agents can trigger this adapter. This prevents the case where a user could manually create a Trigger CI that adds all IPs as triggers to an adapter.

- **An input query defines how to retrieve data information from the CMDB.** Destination data information, even if it is not included in a Trigger CI, can be retrieved by the input query. The input query defines **how** to retrieve the information.

For example, you can define a relationship between a Trigger CI (a node with the node name of **SOURCE**) and the target CI and then can refer to the target CI according to this node name.

For details on using input queries when writing adapters, see Step 1: Create an Adapter in the *Universal CMDB Developer Reference Guide*.

Trigger CIs and Trigger Queries

A **trigger CI** is a CI in the CMDB that activates a discovery job. Every time a job is activated, the job may discover additional CIs, which in turn are used as triggers for other jobs. This process continues until the entire IT infrastructure is discovered and mapped.

A **trigger query** associated with a job is a subset of the **input query**, and defines which specific CIs should automatically trigger a job. That is, if an input query queries for IPs running SNMP, a trigger query queries for IPs running SNMP in the range 195.0.0.0-195.0.0.10.

Note: A trigger query must refer to the same objects as the input query. For example, if an input query of an adapter queries for IPs running SNMP, you cannot define a trigger query for an associated job to query for IPs connected to a node. This is because some of the IPs may not be connected to an SNMP object, as required by the input query.

Part II: Data Flow Management Setup

Chapter 2: Data Flow Probe Setup

This chapter includes:

Data Flow Probes and Probe Clusters	30
UCMDB Integration Service	30
Cluster Range Distribution Policy	31
Limiting IP Movement in a Cluster	34
Job Execution Policies	36
Data Flow Probe Auto Upgrade	37
Effects of Range Type on Discovery Workflows	46
Using HTTPS Port 8453 as Default for Data Flow Probe	48
How to Install a Second Data Flow Probe on a Windows Machine	48
How to Set Master Key for Password Encryption on Data Flow Probe	53
How to Add Data Flow Probes to UCMDB	54
How to Add Probe Clusters to UCMDB	55
How to Start a Data Flow Probe	56
How to Stop a Data Flow Probe	58
How to Change the Data Flow Probe Default Domain	58
How to Change the Data Flow Probe Port	59
How to Move Resources From One Domain to Another Domain	60
How to Change the UCMDB Integration Service Default Domain	61
How to Check the UCMDB Integration Service Status	62
How to Limit IP Movement in a Cluster	63
How to Update the Data Flow Probe's IP Address	64
How to Update the Data Flow Probe Memory Size	65
How to Define Owner Tenants on Data Flow Probes	66
How to Configure the Number of Connections to Other Machines	67
How to Configure Periodic Data Flow Task Updates	68
How to Prevent Probes from Sending Touch Information Simultaneously	70
How to Encrypt/Decrypt IP Ranges Information on the Probes	71

How to Configure the Data Flow Probe to Automatically Delete CIs	72
How to Delete Unsent Probe Results	73
How to Clear Data Flow Probe Data	73
How to Clear UCMDB Integration Service Data	74
How to Deploy a Data Flow Probe CUP	75
How to Deploy a Data Flow Probe CUP Manually	76
How to Align the Data Flow Probe CUP with the UCMDB Server CUP	77
How to Uninstall Probe CUPs Manually	79
How to Set Maximum Objects for Insert Results	80
Data Flow Probe Process Ports	80
DataFlowProbe.properties File	83
DataFlowProbe.properties Parameters	84
DataFlowProbeOverride.properties File	97
Data Flow Probe Database Scripts	98
Data Flow Probe Log Files	99
Data Flow Probe Setup User Interface	103
Troubleshooting and Limitations – Data Flow Probe Setup	136

Data Flow Probes and Probe Clusters

The **Data Flow Probe** is the main component responsible for requesting tasks from the server, scheduling and executing discovery and integration tasks, and sending the results back to the UCMDB Server. You define a range of network addresses for a specific, installed Data Flow Probe. Each Data Flow Probe is identified by its name, chosen during the Data Flow Probe installation process.

A **probe cluster** is a logical container for a number of Data Flow Probes. You define a network range for a cluster. The cluster is responsible for calculating how to distribute the IPs in its network range to ensure a maximum balance of its IPs among its Probes.

UCMDB Integration Service

If your remote managed data repositories are accessible from the UCMDB server machine, you can use the **UCMDB Integration Service**, installed on the UCMDB Server, instead of a Data Flow Probe,

to run non-Jython-based integrations.

This makes Data Flow Probe resources available for other discovery tasks.

For information on using the UCMDB Integration Service to run integrations, see ["How to Set Up an Integration Point" on page 324](#).

Note:

- The UCMDB Integration Service is supported in a standalone UCMDB environment only.
- The UCMDB Integration Service must be started on the UCMDB Server.
- If there is a Data Flow Probe installed and running on the UCMDB Server machine, you must first stop the Data Flow Probe before you can start the UCMDB Integration Service. For details, see ["How to Check the UCMDB Integration Service Status" on page 62](#).
- The UCMDB Integration Service on Linux supports the following integrations:
 - HPE SIM
 - SE
 - NNMi
 - EMC Control Center
 - CMS Sync

Cluster Range Distribution Policy

A probe cluster is a logical container for a number of Data Flow Probes. When you define a network range for the cluster, the cluster distributes IP ranges to its Probes, thereby ensuring that the load on the Probes is evenly balanced.

A cluster balances its IPs among its Probes as follows:

1. To ensure that specific IPs are always distributed to a particular Probe, you can set a TQL query constraint on that Probe. When the TQL query runs, the resulting IPs are distributed to the respective Probe.
2. All of the remaining IP addresses in the cluster's range are then distributed evenly among all of the cluster's Probes (including the Probes with the TQL query constraints).

Note: The cluster balances its IPs over its Probes in such a way so as to minimize

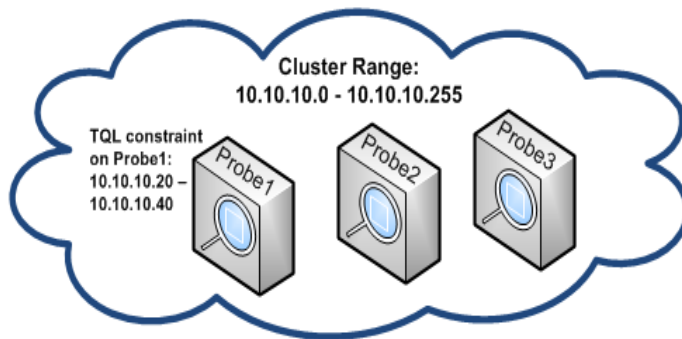
IP movement after the IPs have been distributed to the Probes.

If the cluster's IPs become unbalanced, the cluster tries to re-balance the IPs among its Probes. The cluster is allowed to retry to balance the Probes depending on how much IP movement is allowed. For details, see ["How to Limit IP Movement in a Cluster"](#) on page 63.

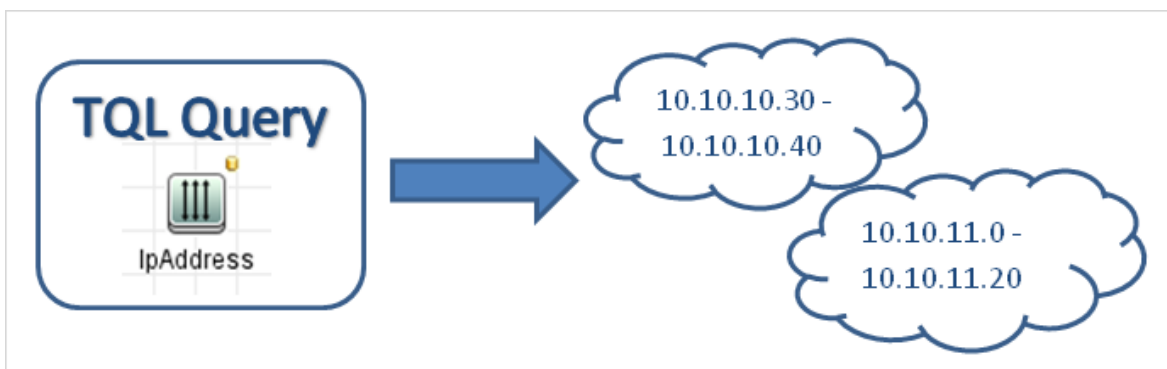
Example

Consider the following scenario:

- Cluster Range: **10.10.10.0 - 10.10.10.255**
- Cluster includes **Probe1, Probe2, Probe3**
- TQL constraint on Probe1: Probe1's range must include IPs 10.10.10.20 - 10.10.10.40



After running a TQL query on UCMDB, the following IPs are returned:



The cluster balances its network ranges among its Probes as follows:

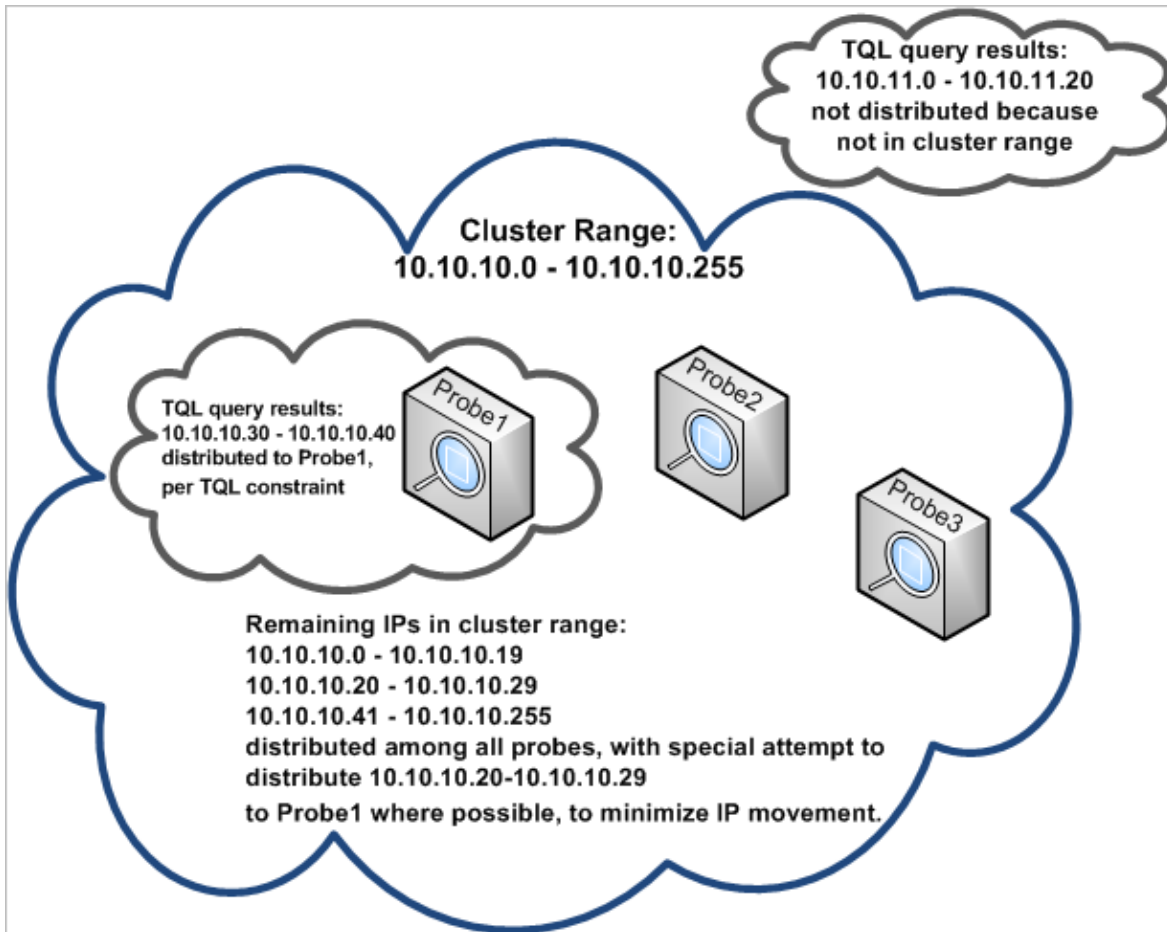
- Because of the TQL constraint on Probe1, range **10.10.10.30 - 10.10.10.40** is specifically distributed to Probe1
- Range **10.10.11.0 - 10.10.11.20** is out of the cluster's range, so it is not distributed to any of the cluster's Probes
- The remaining IPs in the cluster's ranges are then evenly balanced among all of the cluster's Probes. The remaining ranges are:
 - 10.10.10.0 - 10.10.10.29
 - 10.10.10.41 - 10.10.10.255

The cluster always attempts to distribute an IP address to a Probe whose TQL constraint includes that IP address

Note: Technically, IPs **10.10.10.20 - 10.10.10.29**, which fall within Probe1's TQL constraint, can be distributed to any of the cluster's Probes, and not necessarily only to Probe 1. This is because these addresses were not found by the TQL query, which means they do not exist in UCMDDB. In turn, no actual workload can be distributed to them anyway, so it is insignificant which Probe received these IP addresses.

Nonetheless, the cluster does make a special effort to distribute these IPs to Probe1. This way, if a subsequent recalculation of the TQL query returns these IPs, they are already in place, and IP movement is minimized.

Furthermore, when the TQL query is recalculated, and if these addresses are found in UCMDDB, these IP addresses are indeed distributed to Probe 1, per its TQL constraint.



Limiting IP Movement in a Cluster

In a probe cluster, unassigned IPs are assigned to the cluster's Probes in such a way that the imbalance IP ratio among the Probes remains at a minimum. The imbalance ratio is governed by the **imbalance threshold**.

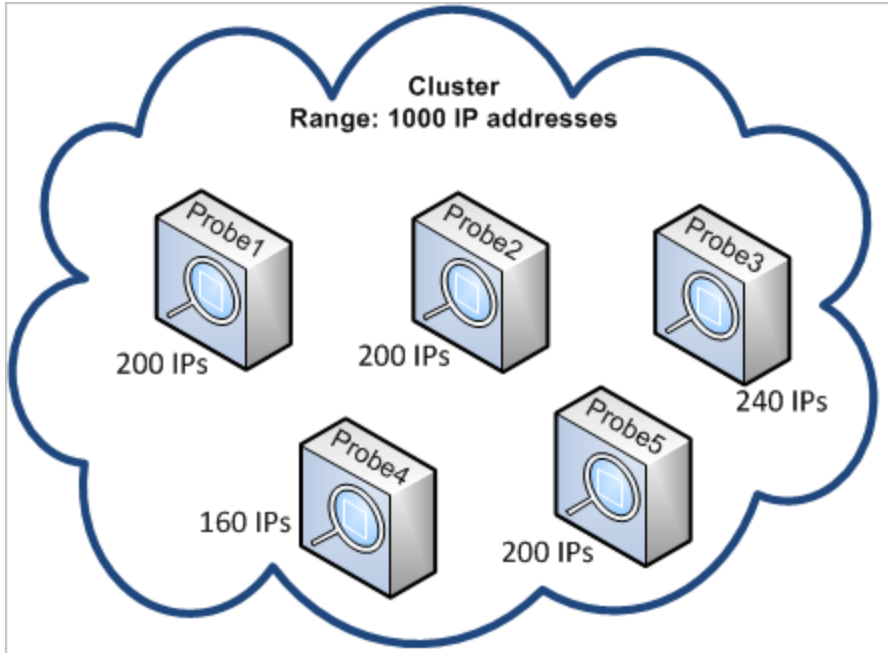
Changing the cluster's network range, changing the set of Probes associated with the cluster, or assigning a TQL constraint on a Probe in the cluster can cause an imbalance of IPs among the Probes in the cluster.

In such a situation, and depending on the IP imbalance threshold, the cluster attempts to re-balance the IPs among the cluster's Probes. That is, if one of the Probes violates the average number of IPs per Probe, as defined by the imbalance threshold, the cluster re-balances the IPs. If not, the cluster leaves the current IP distribution unchanged.

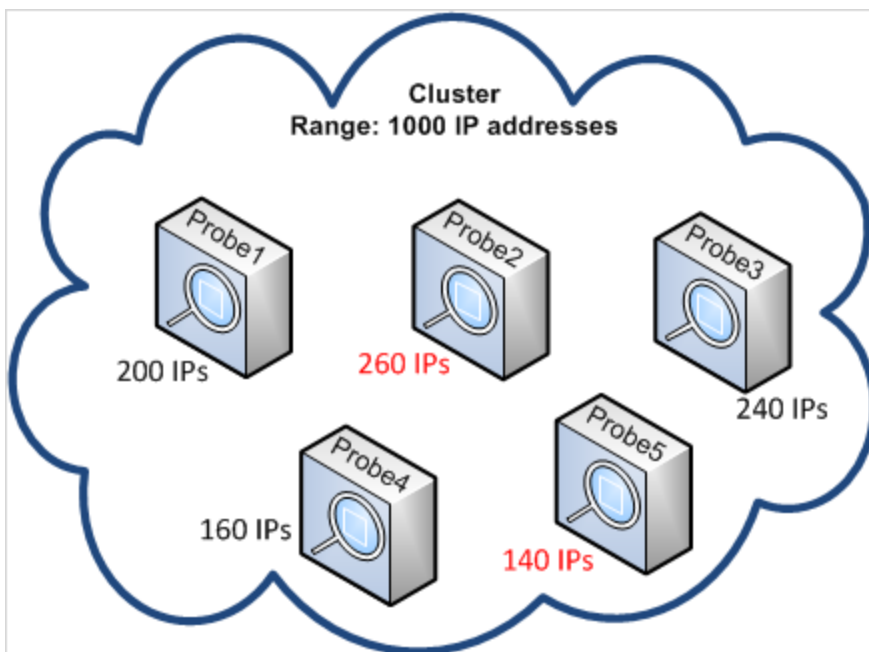
Example:

If a cluster has 5 Probes and 1000 IPs in its range, the average number of IPs per Probe should be 200.

If the imbalance threshold is set to 20%, then if each of the Probes has between 160-240 IPs, they do not violate the imbalance threshold, and no re-balancing is necessary.



If, however, there are Probes with less than 160 IPs, or more than 240 IPs (see image below)—that is, more than a 20% deviation from the average 200—the cluster attempts to re-balance the IPs among the Probes—as long as the TQL constraints on the Probes allow this.



For details on how to specify the imbalance threshold, see ["How to Limit IP Movement in a Cluster" on page 63.](#)

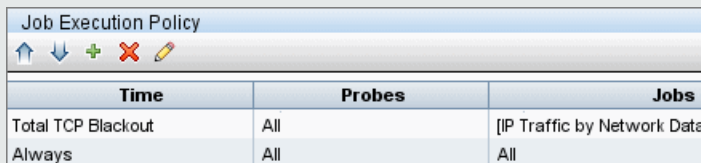
Job Execution Policies

You can define periods of time when a Probe/probe cluster may not run. You can choose to disable specific jobs running on any Probe or all jobs running on a specific Probe or on Probes in a cluster. You can also exclude jobs from a job execution policy so that they continue running as usual.

For details on defining a job execution policy, see ["New/Edit Policy Dialog Box" on page 103.](#)

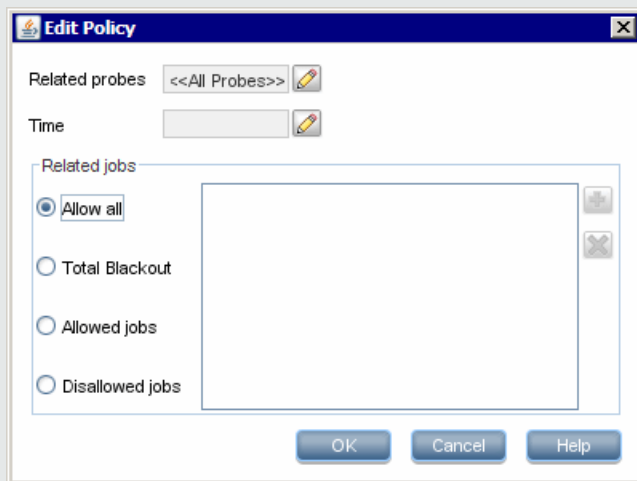
Example of Policy Ordering

Say there are two policies, **Total TCP Blackout** and **Always** (the out-of-the-box policy). **Total TCP Blackout** does not allow any TCP discovery jobs to run. The policies appear in the list as follows:

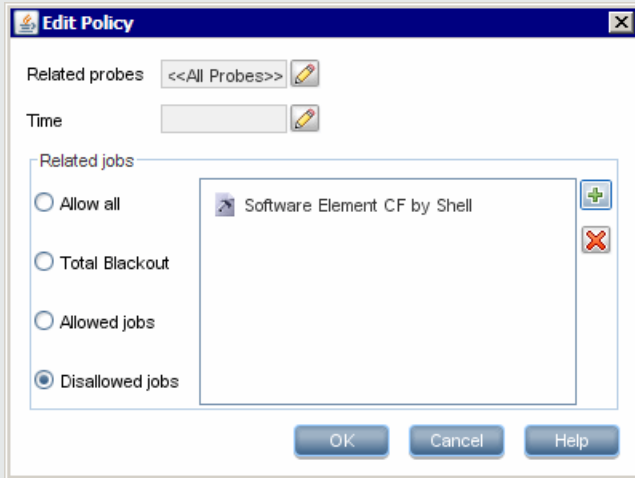


Time	Probes	Jobs
Total TCP Blackout	All	[IP Traffic by Network Date
Always	All	All

A job (**Class C IPs by ICMP**) starts running. It checks the policies in the policy list from top to bottom. It starts by checking **Total TCP Blackout**. The job does not appear in this policy, so it continues down the list and checks **Always**. The job does appear here (**Allow All** is selected in the Edit Policy dialog box) so the job runs:



The next job (**Software Element CF by Shell**) starts running. It checks the policies in the policy list from top to bottom. It starts by checking **Total TCP Blackout**. The job appears in this policy (**Disallowed Jobs** is selected in the Edit Policy dialog box), so the job does not run:



Caution: If a job is not connected to any policy, it does not run. To run these jobs, set the last policy in the list to **Allow All**.

Running Jobs When a Job Execution Policy Is Running

If a policy begins to operate while a Probe is executing a job, the job pauses. When the policy finishes, the job continues to run from where it ceased. For example, say a job contains 10,000 trigger CIs. The job finishes working on 7,000 of them and then the policy starts to operate. When the job continues (after the policy finishes), it works on the remaining 3,000 trigger CIs—the job does not start running from the beginning.

Data Flow Probe Auto Upgrade

Data Flow Probe Auto Upgrade Overview

In version 10.33, the Data Flow Probe auto upgrade mechanism is fully available. That is, once UCMDDB server is upgraded to version 10.33, the probe auto upgrade capability is in place. This capability enables you to upgrade all the connected probes of version 10.22 (or later, with or without a

CUP) in your environments with just several clicks, without having to access the probe servers anymore.

Compared to the traditional manual probe deployment approach (uninstall the old probe and then install the new probe), in general it takes 20-40 minutes to upgrade multiple probes (say, 100 or 200 probes) in parallel with the probe auto upgrade mechanism.

The time required for upgrading all the connected probes equals to that of the probe that takes the longest duration to finish upgrade among all the connected probes. The network latency would be a impact factor, which has impact on the time the probe downloads resources from the UCMDB Server. Micro Focus Software lab testing shows the following results: A total of 60 connected probes finished upgrade in 40 minutes, while the majority of them finished around 20-30 minutes with network latency less than 1 millisecond.

Supported Probes

In version 10.33, probes that satisfy the following criteria are supported for auto upgrade:

- **Supported versions.** The probe auto upgrade and deployment mechanism supports upgrading probes from any of the following versions to version 10.33 automatically:
 - 10.22 (with or without a CUP)
 - 10.30
 - 10.31
 - 10.32
- Union and non-FIPS mode probes on Windows machine

The following probes are not supported for auto upgrade in version 10.33:

- FIPS mode probes
- Separate mode probes
- Probes on Linux machine
- Integration service
- Two probes installed on a same Windows machine

Important:

- Before the upgrade, make sure that:
 - all Data Flow Probe related command line windows and probe related folders are closed. Otherwise when the probe auto upgrade agent backs up probe folders, backing up of those

files may fail as they are occupied.

- ports 5436 and 5437 are free, as these two ports will be used during the probe upgrade.
- If the **UCMDB_Probe** and the **UCMDB_Probe_DB** services run under custom account, make sure you grant full control to the user of the **<DataFlowProbe>** folder before the probe auto upgrade starts, and revert the control after the upgrade.
- If you are upgrading UCMDB, and you have Data Flow Probes in your environment that satisfy the probe auto upgrade requirements, make sure you select **No** when asked if you want to deploy the latest Content Pack, and manually deploy the latest Content Pack after you have completed upgrading the UCMDB server.

Data Flow Probe Auto Upgrade Workflow

The Data Flow Probe Auto Upgrade workflow contains the following steps:

1. The UCMDB **Administrator** upgrades UCMDB server from version 10.22 (or later, with or without a CUP) to version 10.33.

During the upgrade, the Administrator selects the **Automatically update Data Flow Probe to 10.33** option. As a result, the probe auto upgrade agent package is placed under the **<UCMDB_Server>\content\probe_patch** folder, and the Data Flow Probe installer package is placed under the **<UCMDB_Server>\content\probe_installer** folder.

2. The **probe auto upgrade agent** performs the following operations:
 - a. Performs pre-check to decide if the probe is ready for upgrade. For example, if there is enough disk space available or not, and if the probe is of a supported version.
 - b. Generates the response file required for silent installation.
 - c. Downloads **UCMDB_DataFlowProbe_10.33.exe** from the UCMDB server.
 - d. Stops the following services: **UCMDB_Probe**, **UCMDB_Probe_DB**, and **UCMDB_Probe_XmlEnricher**.
 - e. Performs silent installation with the **Update** option.

During this step, Performs post-upgrade tasks, including merging customized settings, creating and adjusting database tables, such as splitting tables (version 10.22 to version 10.33), columns, indexes, and so on.

2. The **probe auto upgrade agent** performs the following operations:
 - f. Starts all three services after the installation is done: **UCMDB_Probe**, **UCMDB_Probe_DB**, and **UCMDB_Probe_XmlEnricher**.

- g. Reports probe upgrade status to the UCMDB server, and save probe auto upgrade logs to UCMDB Server. For example: **<UCMDB_Server>\runtime\log\probeUpgradeLogs\10.22to10.33\success.**

Note: If the upgrade is successful, the log would be placed under the **success** folder; if failed, the logs would be placed under the **failed** folder.

Troubleshooting Probe Auto Upgrade

Troubleshooting Probe Auto Upgrade - General

- **Limitation:** If the auto upgrade fails, retry will not resolve the issue. You need to access the corresponding probe server and perform manual deployment of version 10.33 probe.
- **Known Issue:** The **C:\hp\UCMDB\temp** folder was created and used by the probe auto upgrade agent 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.
- **Check if resources are placed under the right place after UCMDB server is upgraded to version 10.33**
 - a. 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_10.33.exe**.
 - b. Check if the probe auto upgrade agent 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,

 - i. Go to **<UCMDB_Server>\content\probe_patch**.
 - ii. Copy the **probe-patch-10.33-windows.zip** package to the **<UCMDB_Server>\runtime\probe_upgrade** directory.
 - iii. Restart the UCMDB server. UCMDB server will then perform probe auto upgrade.
- **Probe auto upgrade log files**

Check the probe auto upgrade log files (in the **<DataFlowProbe>\runtime\log** directory) for more details:

- **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 upgrade agent upgrades a probe.

For more details about the log files, see ["Data Flow Probe Log Files" on page 99](#).

- **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\10.22to10.33\failed**. You can find the following message in **probe_auto_upgrade.log**:

```
2017-07-14 11:27:11 INFO ServiceControl:106 - Starting XML Enricher service...
2017-07-14 11:27:11 INFO ServiceControl:328 - XML EnricherStatus status:
STOPPED
2017-07-14 11:27:11 INFO ServiceControl:381 - Waiting for execution...
2017-07-14 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**.

Troubleshooting Probe Auto Upgrade - PostgreSQL Upgrade

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

In a more general way, 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.

- 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.
 - a. **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.
 - b. **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**.
 - c. **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.
 - d. **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
```

- e. **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:

- a. Stop the **UCMDB_Probe_DB** service.
- b. Remove the content of the **pgsql** folder and copy the content of the **pgsql.old** folder into the **pgsql** folder.
- c. 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%
```

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

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

Troubleshooting - Probe Auto Upgrade Agent

Before upgrading a probe, the probe auto upgrade agent checks the environment and the probe status.

- a. **Check probe version.** Only a probe of version 10.22 or higher could be upgrade. For supported probe versions, see [Supported Versions](#).
- b. **Check probe status.** Only union mode probe in non-FIPS mode could be upgraded.
- c. **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.

- **How to check if a probe has been upgraded successfully?**

You can check the **probe_auto_upgrade.log** file (in the **C:\hp\UCMDB\DataFlowProbe\runtime\log\probeUpgradeLogs** folder).

- If the probe has been upgraded successfully, you can 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 the probe upgrade failed, 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" on page 99](#).

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

Solution: You need to 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 following log files for further information:

- **probe_upgrade_conf_merge.log**
- **pg_upgrade.log**
- **probe_post_upgrade.log**

Troubleshooting - Three Way Merge Function

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 is **500**. So if your value is greater than 500, it will be modified 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\HPProbeKeyStore.jks**
- **<DataFlowProbe>\conf\security\HPProbeTrustStore.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 probe manually.

Effects of Range Type on Discovery Workflows

Depending on the type of network range defined for a discovery environment, different reconciliation rules and discovery workflows are applied.

To support different types of environments, the IP Address CI contains the **Lease Time** attribute which stores the type of network range. The type of network range the routing domain, and certain discovery options determine the reconciliation rules and workflows that are applied to that network range.

Updates to the IP Address CI occur when ranges are updated, when IP Address CIs are reported by the Data Flow Probe, or when new IP/MAC pairs are discovered. This behavior minimizes unnecessary add and delete operations for IP Address CIs.

For descriptions of typical environments for range types, and for information on how to configure range types, see ["New/Edit Range Dialog Box" on page 131](#).

For explanations on choosing the best discovery options for Client types ranges, see ["Discovery Options for Client IP Ranges" on page 538](#).

The following explains the range types and discovery options, and the effects on data reconciliation:

Range Type	Discovery Option	Discovery Workflow	Effects on Data Reconciliation
Data Center	N/A	<ol style="list-style-type: none"> Ping Sweep by ICMP job runs. <ul style="list-style-type: none"> Note: MAC addresses are not captured during a ping sweep discovery job. Node CI is created. Host Connection jobs run. Inventory Discovery jobs and Universal Discovery Agent related jobs run. 	If the IP addresses that are discovered during two unique discovery runs are identical, the data is merged into a single IP Address CI.
Client	SNMP	<ol style="list-style-type: none"> Client SNMP Discovery job runs to discover ARP-enabled devices that provide IP/MAC pair information. IP/MAC Address Harvesting job runs against SNMP devices to retrieve IP/MAC pair information. 	If the IP addresses that are discovered during two unique discovery jobs are different but the ARP/MAC values are identical, the data is merged into a single IP

Range Type	Discovery Option	Discovery Workflow	Effects on Data Reconciliation
		<ol style="list-style-type: none"> 3. New or updated IP/MAC pair information and a CallHomeEvent CI is reported to UCMDB. 4. The Host Connection job and the Call Home Processing job runs. 5. Inventory Discovery jobs and Universal Discovery Agent-related jobs run. However, if the Data Flow Probe cannot establish a connection with the discovery node or a job is waiting for other tasks to complete, the workflow is put into a parked state. <p>A CallHomeEvent CI is received by UCMDB when the Universal Discovery Agent sends a call home message to the Data Flow Probe, or when a new IP/MAC address pair is harvested from an ARP cache job. As a result, a Call Home Processing job is triggered and the parked workflow is put into an activated state. Then, the Inventory Discovery jobs and Universal Discovery Agent-related jobs run. For more information on parked workflows and other traffic cases, see "Call Home Overview" on page 167.</p>	<p>Address CI.</p> <p>If the IP addresses that are discovered during two unique discovery jobs are different and the ARP/MAC addresses are null or undetermined, the data is merged into a single IP Address CI if the Interface IDs are identical.</p>
	Without SNMP	<ol style="list-style-type: none"> 1. Ping Sweep by ICMP job runs. <p>Note: MAC addresses are not captured during a ping sweep discovery job.</p> <ol style="list-style-type: none"> 2. Host Connection jobs run. 3. Inventory Discovery jobs and Universal Discovery Agent-related jobs run. 	<p>Standalone (i.e., not connected to any CIs) IP addresses without ARP/MAC values are reported to UCMDB. However, IP addresses that are connected to a CI (i.e., not standalone) and without ARP/MAC values are not reported to UCMDB.</p> <p>If an IP address without an IP/MAC value is discovered, and there is another instance of the same IP address together with the same domain name, the two instances are reconciled. This behavior occurs</p>

Range Type	Discovery Option	Discovery Workflow	Effects on Data Reconciliation
			whether there are IP/MAC values or not.

Using HTTPS Port 8453 as Default for Data Flow Probe

Starting with version 10.31, to provide secure access to the Data Flow Probe JMX console, for fresh installed Probes, by default the **jettyHttpsEnabled** setting in the Probe configuration file **DataFlowProbe.properties** is **true** and the HTTPS port 8453 (**jettyGtwHttpsPort**) is used for the Probe server, with the HTTP port 1977 being disabled.

To access the Probe JMX console, on the probe machine, launch the Web browser and enter the following address: **https://localhost:8453**. For more information about accessing probe JMX console, see "Introduction" in the *Universal CMDB JMX Reference Guide*.

Note:

- For off-site scan file saving, only the HTTPS port 8453 can be used. If you want to use HTTP port 1977 for scan files saving, set **jettyHttpsEnabled** to **false**.
- For probes and Integration Service upgraded from a previous version, your custom settings are retained. This default port change only applies to fresh installed probes of version 10.31.
- Separate mode probes (whether in FIPS mode or not) do not support HTTPS communication. You need to set **jettyHttpsEnabled** to **false** after installing probes in separate mode.

How to Install a Second Data Flow Probe on a Windows Machine

Notes before you install

- Supported combination: An existing Probe (of any version, separate or union mode) on Windows + a second Probe (of version 10.30 or later, union mode), reporting to two different UCMDDB Servers

That is to say, when installing a second Probe, you can

- install it on Windows machine only
- install a union mode Probe only
- ignore the version of the existing Probe, as two Probes report to two different UCMDB servers
- On the same Windows machine, you can have two Probes at most.

Even if you run the Data Flow Probe installer once again in an attempt to install a third Probe, it just overrides the second Probe.

- Multi network card is not supported
- You can change the ports manually after the installation.

The following procedure explains how to install a second Data Flow Probe on a Windows machine.

Note:

- Ensure that you have read the important notes and considerations above before you install the Data Flow Probe.
- The passwords that you specify during the Data Flow Probe installation must meet the following requirements:

The password must contain 8 to 16 characters and include at least one of each of the following four types of characters:

- Uppercase alphabetic characters
- Lowercase alphabetic characters
- Numeric characters
- Special characters: , \ : / . _ = + - [] (

Caution: (PostgreSQL only) Do not include any of the following special characters in the PostgreSQL user account password as they are regarded as sensitive characters: = ? % | &). Otherwise probe cannot be started after installation.

To install a second Data Flow Probe:

1. Insert the **UCMDB10.33WIN** DVD into the drive from which you are installing the Probe. If you are installing from a network drive, connect to the drive.
2. In the root folder of the DVD, double-click **UCMDB_DataFlowProbe_10.33.exe**.
3. A progress bar is displayed. After the initial process is complete, the splash screen opens.

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

4. The Introduction page opens. A prompt pops up reminding you that an existing Data Flow Probe installation is detected, and asking you if you would like to install a second Data Flow Probe. Click **Yes** to proceed, or click **Cancel** to cancel the installation.

5. The License Agreement page opens.

Accept the terms of the end-user license agreement and click **Next**.

6. The Setup Type page opens.

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

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

Click **Next**.

7. The Select Installation Type page opens.

Select **New Installation** if you are installing a new probe.

Note: Select **Upgrade** when you upgrade an existing probe.

8. The Select Installation Folder page opens.

Specify a different installation folder or click **Choose** to select a different installation folder for the second probe.

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

9. The UCMDB Data Flow Probe Configuration page opens, enabling you to configure the details of the application server to which the second Data Flow Probe will report.

- o Under **Application to report to** select **Universal CMDB** and in the **Application Server address** box, enter the name or the IP address of a different Universal CMDB server (other than the UCMDB server for the existing Probe) with which the second Probe is to connect.

Note:

- Two Probes installed on the same Windows machine should report to two different UCMDB servers respectively. For the second Probe you install, make sure you specify a different Universal CMDB server.

- In a High Availability environment, use the Writer virtual IP address of the load balancer.
- In the **Data Flow Probe address** box, enter the IP address or DNS name of the machine on which you are currently installing the Probe, or accept the default.

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

Click **Next**.

Note: If you do not enter the address of the application server, or if there is no TCP connection to the application server via default ports (8080,8443,80) (possibly because the application server has not fully started yet), a message is displayed. You can choose to continue to install the Probe without entering the address, or return to the previous page to add the address.

10. A second UCMDB Data Flow Probe Configuration page opens, enabling you to configure an identifier for the Probe.
 - In the **Data Flow Probe Identifier** box, enter a name for the second Probe that is used to identify it in your environment.

Note:

- The Probe identifier is case sensitive, must be unique for each Probe in your deployment, and it must not exceed 50 characters.
- Make sure you enter a unique identifier for the second Probe.
- To use the default UCMDB IP address or machine name, as defined in the UCMDB Server installation, select **Use Default CMDB Domain**.

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

Click **Next**.

11. The UCMDB Data Flow Probe Memory Size page opens.

Note: For the second Probe you install, the Probe Domain Config and Probe Working Mode pages are skipped.

Define the minimum and maximum memory, in megabytes, to be allocated to the second Probe.

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

Click **Next**.

12. The PostgreSQL Account Configuration page opens.

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

Enter the password for the PostgreSQL Data Flow Probe account and enter it a second time for confirmation.

Note: Changing this password requires an update to the **DataFlowProbe.properties** file.

Caution: (PostgreSQL only) Do not include any of the following special characters in the PostgreSQL user account password as they are regarded as sensitive characters: = ? % | &). Otherwise probe cannot be started after installation.

Click **Next**.

13. A second PostgreSQL Account Configuration page opens where you configure the PostgreSQL root account. The PostgreSQL root account is the account used to administer the PostgreSQL database. When set, it may need to be provided while executing scripts under the Probe's installation.

Enter the password for the PostgreSQL Data Flow Probe account, and enter it a second time for confirmation.

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

Click **Next**.

14. The Configuration for System Administrator Password page opens.

Enter the password for the **sysadmin** account. Make sure the password meets the default password.

15. The Account Configuration for Uploading Scan Files page opens. This is used for Manual Scanner Deployment mode. It enables uploading scan files directly to the XML Enricher's **incoming** directory on the Data Flow Probe using HTTP or HTTPS.

Enter the user name and password for this account, and enter the password a second time for confirmation. The default user name is **UploadScanFile**.

Click **Next**.

16. The Pre-Installation Summary page opens.

Review the selections you have made and click **Install** to complete the installation of the second Probe.

17. When the installation is complete, the Install Complete page opens.

Note:

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

C:\hp\UCMDB*DataFlowProbe_2_InstallDir*\UninstallerData\Logs\UCMDB_Data_Flow_Probe_Install_<i>install date and time

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

C:\hp\UCMDB*DataFlowProbe_2_InstallDir*\runtime\log\postgresql.log

Click **Done**.

18. If you customized the **key.bin** file, copy the **key.bin** file that you saved earlier to **C:\hp\UCMDB\DataFlowProbe\conf\security**.
19. Start the second Probe: Select **Start > All Programs > UCMDB (2) > Start Data Flow Probe**.

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

C:\hp\UCMDB*DataFlowProbe_2_InstallDir*\bin\gateway.bat console.

Note:

- o In order for the Probe to connect to the application server, the application server must be fully started.
- o The Probe is displayed in UCMDB in the **Data Flow Management** module, under **Data Flow Probe Setup > <Domain> > Probes**.

How to Set Master Key for Password Encryption on Data Flow Probe

This section explains how to set a master key for password encryption on Data Flow Probe. This key is updated with a new pass. The updated pass is stored in the **DataFlowProbe.properties** file.

To set the master key for password encryption on Data Flow Probe,

1. Access the Data Flow Probe JMX console. On the probe machine, launch a Web browser and enter the following address: **https://localhost:8453**.

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

Note: If you have not created a user, use the default user name sysadmin to log in.

2. Locate the **type=MainProbe** service and click the link to open the Operations page.
3. Locate the **changeMasterKey** operation.
4. In the **pass** field, enter the new pass to change master key.
5. In the **repass** field, enter the new pass again to double confirm.
6. Click **Invoke**.

The result of the invocation is a message like the following:


The key is changed successfully.

Note: For Data Flow Probes installed in separate mode, you need to change the master key on both probe gateway and probe manager.

How to Add Data Flow Probes to UCMDB

This task describes how to add a Data Flow Probe to UCMDB.

1. Prerequisites
 - Verify that the Probe is installed and make a note of its IP address.
For details about installing a Data Flow Probe, see the interactive *Universal CMDB Deployment Guide*.
 - Ensure that the probe's domain is defined in UCMDB. For details, see ["Add New Domain Dialog Box" on page 104](#).
2. Add a Data Flow Probe
 - a. In the Data Flow Management module, go to the Data Flow Probe Setup window.
 - b. In the Domains and Probes tree, select the domain to which to add the probe.

- c. Select the **Data Flow Probes** node, click , and select **New Data Flow Probe**.
- d. Define the Probe name and provide a description if desired.
- e. Select the new Probe and define its network range. For details, see "[New/Edit Range Dialog Box](#)" on page 131.

Note: Two Probes in the same domain cannot have the same IP address in their range.

3. Results


To verify that the Probe is connected, select the Domains and Probes tree, and in the details pane on the right, verify that the **Status** is **Connected**.

Note: When you install and start the Probe, it automatically connects to UCMDB.


How to Add Probe Clusters to UCMDB

This task describes how to add a probe cluster to UCMDB.

1. Create a cluster

- a. In **Data Flow Management**, go to **Data Flow Probe Setup**.
- b. In the **Domains and Probes** tree, select the **Data Flow Probes** node.
- c. Click , and select **New Cluster**.
- d. Enter a name and a description for the cluster.


2. Define a network range for cluster

Select the cluster in the Domains and Probes tree on the left, and in the **Ranges** pane on the right, click **New Range**  to define a network range for the cluster.


For details, see "[New/Edit Range Dialog Box](#)" on page 131.

3. Add Data Flow Probes to the cluster

- a. Select the cluster in the Domains and Probes tree.

- b. In the **Associated Probes** pane on the right, click **Add Probe to Cluster** , and select Data Flow Probes to add to the cluster.

Note:

- A Data Flow Probe can belong to one cluster only.
- You can define a Data Flow Probe in a cluster even before the Data Flow Probe has actually been installed and connects to the UCMDB Server. To do this, select the cluster in the Domains and Probes tree, click **New Data Flow Probe** , and give the Probe a name and a description.
- When a Data Flow Probe is added to a cluster its whole network range becomes part of the cluster's range. If you remove the Probe from the cluster, the Probe will have no defined network ranges because all of them remain part of cluster's range.

Exception: If the Probe was added, and then removed without making any changes to its range, and before saving the cluster, then its range is not merged with the cluster's range, but remains with the Probe.

- If management zones are used on the Probe that you are adding to the cluster, and those management zones contain IP ranges, add the IP ranges to the management zones again using the Edit Management Zones dialog box.

- c. (Optional). Set TQL constraints for one or more Probes. For details, see [Set TQL Constraint](#) on page 119.

4. Save the cluster

Click **OK** at the bottom of the Details pane to save the cluster.

5. Results

The cluster balances its network ranges among its Probes. For details, see "[Cluster Range Distribution Policy](#)" on page 31.

How to Start a Data Flow Probe

This task describes how to start the Data Flow Probe service.

Note:

- A Data Flow Probe running on a Linux platform is intended for the CMS Sync integration only, and not for discovery.
- The managed environment is defined by the ranges of the domains. However, with some discovery adapters it is possible to override this behavior and discover CIs that are out of a Probe's range.

1. Prerequisite

- Ensure that the UCMDB Server is installed and running.
- Ensure that the Data Flow Probe is installed.

For installation instructions, see the interactive *Universal CMDB Deployment Guide*.

2. Start the Probe

Start the Probe on the machine on which the Probe is installed:

- **Windows: Start > All Programs > UCMDB > Start Data Flow Probe**

Note: To start the second Probe (of version 10.30 or later) you installed on a Windows machine, click **Start > All Programs > UCMDB (2) > Start Data Flow Probe**.

- **Linux: /opt/hp/UCMDB/DataFlowProbe/bin/ProbeGateway.sh start**

The Probe is started as a service.

To verify that the Probe has been launched successfully (Windows Probe only):

- a. In UCMDB select **Data Flow Management > Data Flow Probe Setup**.
- b. Select the Probe and, in the Details pane, verify that the status is **Connected**.

Note:


- The user running the Probe service must be a member of the Administrators group.
- You can also configure the Probe so that it opens in a console. In this case, the command prompt window is displayed. To open the console, on the Probe machine select **Start > All Programs > UCMDB > Start Data Flow Probe (console)**.

How to Stop a Data Flow Probe

- To stop a Probe when it is running as a service, on the machine where the Data Flow Probe is installed select:
 - **Windows:** **Start > All Programs > UCMDB > Stop Data Flow Probe**
 - **Linux:** **/opt/hp/UCMDB/DataFlowProbe/bin/probegateway.sh stop**
- To stop a Probe when it is running in a command prompt window (the console), on the machine where the Data Flow Probe is installed press **CTRL+c**, then **y**.

How to Change the Data Flow Probe Default Domain

This task describes how to change a Data Flow Probe's default domain.

1. Stop the Probe. For details, see "[How to Stop a Data Flow Probe](#)" above.
2. Remove the Probe from UCMDB:
 - If the Probe appears in the **Data Flow Probe Setup > Domains and Probes** tree, select the Probe and click **Remove Domain, Probe or Cluster** .
 - If the Probe does not appear in the **Data Flow Probe Setup > Domains and Probes** tree (in the case of a Probe on Linux/Probe configured for Integration only), you must delete it from the UCMDB JMX console:
 - i. Log in to the UCMDB JMX Console. For details, see *How to Access the JMX Console in the Universal CMDB Administration Guide*.
 - ii. If you do not know the exact name of the Probe that you want to remove, you can generate a list of the Probes on UCMDB by invoking the **getAllRegisteredProbes** operation.
 - iii. Locate the **removeProbeOrCluster** operation, enter your customer ID (default: **1**) and the name of the Probe you are removing, and invoke the operation.

The Probe is removed from UCMDB.

3. Update the Probe default domain property.

a. On the Probe machine, open the **DataFlowProbe.properties** file, located in:

- **Windows:** C:\hp\UCMDB\DataFlowProbe\conf
- **Linux:** /opt/hp/UCMDB/DataFlowProbe/conf

b. Update the following property with the new domain name:

- **appilog.collectors.domain**

For more details about this property, see ["DataFlowProbe.properties Parameters" on page 84](#).

4. Clear the data from the Probe.

Note: The **clearProbeData** script resets the Data Flow Probe's DB schemas and file system state. After running this script the Data Flow Probe re-sends all discovered data to UCMDB. This could potentially create a significant load on the UCMDB Server.

For details, see ["How to Clear Data Flow Probe Data" on page 73](#).

5. Restart the Probe. For details, see ["How to Start a Data Flow Probe" on page 56](#).

How to Change the Data Flow Probe Port

This task describes how to change a Data Flow Probe's port number.

1. Stop the Probe. For details, see ["How to Stop a Data Flow Probe" on the previous page](#).

2. Update the Probe's port property.

a. Open the **DataFlowProbe.properties** file, located in:

- **Windows:** C:\hp\UCMDB\Data Flow Probe\conf
- **Linux:** /opt/hp/UCMDB/Data Flow Probe/conf

b. Open the **DataFlowProbeOverride.properties** file located in the same folder.

c. Copy the following property from **DataFlowProbe.properties** to **DataFlowProbeOverride.properties** (if not exist), and set the new port number in **DataFlowProbeOverride.properties**:

- If HTTP communication is configured: **serverPort**
- If HTTPS communication (SSL) is configured: **serverPortHttps**

For more details about these properties, see ["DataFlowProbe.properties Parameters" on page 84](#).

Note: Starting with version 10.33, if you want to edit or update any property in the **DataFlowProbe.properties** file, if the property also exists in the **DataFlowProbeOverride.properties** file, we highly recommend you to make sure the property is updated in both files to keep consistency.

3. Clear the data from the Probe.

Note: The **clearProbeData** script resets the Data Flow Probe's DB schemas and file system state. After running this script the Data Flow Probe re-sends all discovered data to UCMDDB. This could potentially create a significant load on the UCMDDB Server.

For details, see ["How to Clear Data Flow Probe Data" on page 73](#).

4. Restart the Probe. For details, see ["How to Start a Data Flow Probe" on page 56](#).

How to Move Resources From One Domain to Another Domain


This task describes how to move credentials, Data Flow Probes, and Probe ranges from one domain (the source domain) to another domain (the target domain).


1. Prerequisite: Deactivate all running jobs and all activities running in all the Management Zones.
2. Stop each Data Flow Probe in the source domain that you want to move to the target domain. For details, see ["How to Stop a Data Flow Probe" on page 58](#).
3. On each Probe machine, open `..\hp\UCMDDB\DataFlowProbe\conf\dataFlowProbe.properties`, and locate the following line:

```
appilog.collectors.domain =
```

Set the parameter's value to `#{DefaultDomain}`.

Save the changes, but do not yet restart the Probe.

4. In UCMDDB, go to **Data Flow Management > Data Flow Probe Setup** and for each Probe under your source domain:
 - a. Select the Probe and click **Export To CSV**  to export the Probe's ranges to a CSV file.
 - b. Delete the Probe from the source domain.

5. Create a new domain—the target domain—with **Type = Customer**.
6. In the source domain, select each credential, click **Copy selected credential to another domain** , and select the target domain that you created above.
7. In UCMDB, go to **Administration > Infrastructure Settings Manager**.
 - a. From the **Filter by column** drop-down list, select **Name**, and in the adjacent box, type **domain**.
 - b. Among others, the **Default Domain Property Value** setting is displayed. In the **Value** column of this setting, enter the name of the target domain you created above.
 - c. Save your changes.
8. Delete all the **ipaddress** and **ipsubnet** CIs from your CMDB.
9. On each Probe:
 - a. Run **clearProbeData.bat**. For details, see ["How to Clear Data Flow Probe Data" on page 73](#).
 - b. Start the Probe. For details, see ["How to Start a Data Flow Probe" on page 56](#).

Note: Ensure that the Probe started properly.
10. In UCMDB, go to **Data Flow Management > Data Flow Probe Setup**:
 - a. Check that all the Probes from the source domain now appear under the target domain you created above.
 - b. For each Probe, import the corresponding CSV with the Probe ranges that you exported earlier.

How to Change the UCMDB Integration Service Default Domain

This task describes how to change the default domain of the UCMDB Integration Service.

1. Stop the Integration Service.

Windows	Start > All Programs > UCMDB > Stop Universal CMDDB Integration Service
Linux	/opt/hp/UCMDB/UCMDBServer/integrations/bin/service.sh stop

2. Update the domain properties.

- Open the **DataFlowProbe.properties** file, located in:

Windows	c:\hp\UCMDB\UCMDBServer\integrations\conf
Linux	/opt/hp/UCMDB/UCMDBServer/integrations/conf

- Update the following property with the new domain name:

appilog.collectors.domain

For more details about this property, see ["DataFlowProbe.properties Parameters" on page 84](#).

3. Clear the data from the Integration Service.

For details, see ["How to Clear UCMDB Integration Service Data" on page 74](#).

Note: The **clearProbeData** script resets the Integration Service's DB schemas and file system state. After running this script the Integration Service re-sends all discovered data to UCMDB. This could potentially create a significant load on the UCMDB Server.

4. Restart the Integration Service.

Windows	Start > All Programs > UCMDB > Start Universal CMDDB Integration Service
Linux	/opt/hp/UCMDB/UCMDBServer/integrations/bin/service.sh start

How to Check the UCMDB Integration Service Status

If your remote managed data repositories are accessible from the UCMDB server machine, you can use the UCMDB Integration Service for non-Jython-based integrations instead of a Data Flow Probe.

Note: The UCMDB Integration Service is supported in a standalone UCMDB environment only.

To ensure that the service is running:

1. Check the status on the UCMDB Server machine:

Windows	Control Panel > Administration Tools > Services
Linux	/opt/hp/UCMDB/UCMDBServer/integrations/bin/service.sh status

2. If the service is not running:

- a. Check if there is a Data Flow Probe installed and running on the UCMDB Server machine. If so, you must first stop the Data Flow Probe before you can start the UCMDB Integration Service.

To stop the Data Flow Probe:

Windows	Select Start > All Programs > UCMDB > Stop Data Flow Probe
Linux	Enter the following command: /opt/hp/UCMDB/DataFlowProbe/bin/probegateway.sh stop

- b. Start the UCMDB Integration Service:

Windows	Use one of the following: <ul style="list-style-type: none">• Select Start > All Programs > UCMDB > Start Universal CMDB Integration Service• Select Start > Control Panel > Administration Tools > Services, and start the UCMDB Integration Service
Linux	Enter the following command: /opt/hp/UCMDB/UCMDBServer/integrations/bin/service.sh start

How to Limit IP Movement in a Cluster

This task describes how to set the IP imbalance threshold for probe clusters to minimize IP movement in the cluster.

To set the imbalance threshold:

1. Go to **Administration > Infrastructure Settings Manager > General Settings > Maximum allowed cluster imbalance**.
2. Enter the imbalance threshold (in percentage).

Default: 20% The cluster must distribute the IPs among its Probes so that they are balanced. That is, by default no Probe may have 20% more or less than the average number of IPs. If the number of IPs on any Probe deviates from this threshold, the cluster attempts to redistribute the IPs among its Probes.

For an example, see "[Limiting IP Movement in a Cluster](#)" on page 34.

Note: If minimal IP movement is more critical than cluster imbalance, then minimize the IP movement by making this threshold higher. The higher the imbalance threshold, the less the IPs will be moved around.

How to Update the Data Flow Probe's IP Address

This task describes how to configure a Data Flow Probe if its IP address has changed.

Note: If the IP address of a Data Flow Probe has changed, it is advisable to re-install the Probe. For information about installing the Data Flow Probe, see the interactive *Universal CMDB Deployment Guide*. If it is not possible to reinstall the Probe, perform the procedure below.

To change the IP address of a Data Flow Probe:

1. Update the Probe properties

In `C:\hp\UCMDB\Data Flow Probe\conf` folder:

- Open the `DataFlowProbe.properties` file and update the following properties:
 - `appilog.collectors.local.ip`
 - `appilog.collectors.probe.ip`

For more details about these properties, see "[DataFlowProbe.properties Parameters](#)" on page 84.

- Open the `probeMgrList.xml`, locate the line that starts with `<probeMgr ip=` and update the Probe Manager machine name or IP address, for example:

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

2. Stop the Probe

- To stop the Probe when it is running as a service, select

Start > All Programs > UCMDB > Stop Data Flow Probe

- To stop the Probe when it is running in a command prompt window (the console), press **CTRL+c**, then **y**.

3. Clear the data from the Probe

For details, see ["How to Clear Data Flow Probe Data" on page 73](#).

Note: The **clearProbeData** script resets the Data Flow Probe's DB schemas and file system state. After running this script the Data Flow Probe re-sends all discovered data to UCMDB. This could potentially create a significant load on the UCMDB Server.

4. Restart the Probe

To restart the Probe from the Start window or from the console, see ["How to Start a Data Flow Probe" on page 56](#).

How to Update the Data Flow Probe Memory Size

The Data Flow Probe Memory Size is defined during installation.

This task describes how to change the maximum heap size.

1. Open the **WrapperEnv.conf** located in

Windows	C:\hp\UCMDB\DataFlowProbe\bin\
Linux	/opt/hp/UCMDB/DataFlowProbe/bin

2. Update the following parameters:

- **set.GATEWAY_MAX_MEM**
- **set.MANAGER_MAX_MEM**

Note:

- For Probes on Linux machine, update only **set.GATEWAY_MAX_MEM**
- If the enriched scan file contains the **hwOSUserProfiles** attribute that has about 300,000

values, increase these parameters by one gigabyte (GB).

3. Restart the Data Flow Probe process.

How to Define Owner Tenants on Data Flow Probes

In multi-tenancy environments, all discovered CIs/relationships are assigned an owner tenant. If no owner tenant is defined in the discovery adapter parameters, but an owner tenant is defined in the Data Flow Probe properties, the discovered CIs/relationships are assigned this owner tenant.

This task describes how to define an owner tenant in the Data Flow Probe properties.

Note: This section is relevant for multi-tenancy environments only.

1. Prerequisite

The owner tenant that you want to define in the Data Flow Probe properties must already be defined in UCMDB. For details on creating owner tenants in UCMDB, see *New Tenant/Edit Tenant Dialog Box* in the *Universal CMDB Administration Guide*.

2. On the Data Flow Probe open the **DataFlowProbe.properties** file, located in the Data Flow Probe's installation folder under `..\UCMDB\DataFlowProbe\conf`.
3. Define the owner tenant parameter by adding the following line:

```
com.hp.ucmdb.discovery.Probe.DefaultTenant=<owner_tenant>
```

where **owner_tenant** is the name of the owner tenant, as defined in the **Security > Tenants Management** module.

4. Save the **DataFlowProbe.properties** file.
5. Restart the Data Flow Probe.
6. Result

The owner tenant is displayed in the Data Flow Probe Setup module.

How to Configure the Number of Connections to Other Machines

This task describes how to configure the number of connections per second that a Data Flow Probe is allowed to create to other machines. You configure these settings in the **globalsettings.xml** file which is located in the Adapter Management module under **Resources** pane > **Packages** > **AutoDiscoveryContent** > **Configuration Files**.

To configure the number of connections per second created by the Probe to other machines:

1. In the **globalsettings.xml** file, configure the properties listed below as follows:

Property	Description
maximumConnectionsPerSecond	<p>Enables limiting the number of new connections per second created by the Probe to other machines.</p> <ul style="list-style-type: none">○ 0. Unlimited number of connections allowed.○ > 0. The maximum number of connections. If this limit is reached, any job trying to create a new connection will wait for a period of time that is determined in the timeToSleepWhenMaximumConnectionsLimitReached property (see below) <p>Default: 0 (unlimited)</p>
timeToSleepWhenMaximumConnectionsLimitReached	<p>Determines how long (in milliseconds) a job needs to wait until a new connection can be created, assuming the "maximumConnectionsPerSecond" limit has been reached.</p> <p>Default: 1000 milliseconds (1 second)</p> <p>Note: If maximumConnectionsPerSecond = 0, this property is ignored.</p>

2. Save your changes.

For more details about the **globalsettings.xml** file, see the *Universal CMDB Discovery and Integrations Content Guide*.

How to Configure Periodic Data Flow Task Updates

When a data flow job is activated, the input TQL of the adapter is calculated once and is sent to the Data Flow Probe. If trigger CI data changes (for example, a laptop acquires a different IP address) the Data Flow Probe needs to be updated with the modified trigger CI data. As long as the Data Flow Probe is not updated with any changes, the query continues to run with out-of-date information.

To ensure that the Data Flow Probe is always kept up-to-date with possible changes in trigger CI data, you can configure UCMDB to recalculate trigger CI data and send any changes to the Data Flow Probe.

There are rare situations where triggers appear as part of a Service Discovery activity, although they are not part of the discovered service or CIs related to the service. In this case, the periodic data flow task updates will dispatch and undispatch these triggers to return the activity to its valid state.

This section includes:

- ["Global Configuration" below](#)
- ["Adapter Configuration" on the next page](#)
- ["Ad Hoc Updates" on page 70](#)

Global Configuration

Data flow tasks for all adapters are updated per the global setting configured in the Infrastructure Settings.

Note: Where necessary, you can configure updates for a particular adapter to behave differently. For details, see ["Adapter Configuration"](#) below.

To configure global data flow task updates:

1. Select **Administration > Infrastructure Settings Manager**.
2. Select the **General Settings** category.
 - a. Locate **Enable periodic update of data flow tasks** parameter and set the value to **true**.
 - b. Locate **Periodic data flow task update interval (in hour)** and **Periodic data flow task**

update start time and specify how often (in hours) to update the data flow tasks, and the time (01-24) at which to start the update.

By default, this option is enabled, and the data flow tasks are updated once a day, at midnight.

Adapter Configuration

This task describes how to configure a particular adapter so that updates to its data flow tasks are periodically sent to the Data Flow Probe.

Note:

- The setting in the adapter file overrides the global setting (**Enable periodic update of data flow tasks**) described above.

For example, if the setting in the adapter file is set to **true**, but the global setting is set to **false**, the adapter's tasks are still updated on the Data Flow Probe (and vice versa).
- This setting should be configured for an adapter only in the case where updates for the adapter should behave differently to configuration in the global settings.

To configure data flow task updates for a particular adapter:

1. Open the adapter's xml file in an editor.
2. Locate the **<dispatchMechanism>** tag. If it does not exist, create it.
3. Add the following parameter:

```
<dispatchOnChanges isEnabled = "<true or false>" />
```

Example:

```
<pattern>
..
    <dispatchMechanism type = "IpAddress">
        <dispatchOnChanges isEnabled = "true" />
    </dispatchMechanism>
..
</pattern>
```

Ad Hoc Updates

1. Log in to the UCMDB JMX console. (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=Discovery Manager** to open the JMX MBEAN View page.
3. Run one of the following methods, depending on which is relevant:

JMX Method	Description
recalculateAndUpdateDFMTasks	Updates data flow tasks for all the adapters for which data flow task update is enabled. Note: Data flow task updates are enabled in the adapter's configuration file.
recalculateAndUpdateDFMTasksForAdapter	Updates data flow tasks for selected adapters without checking the adapter configurations. That is, even if the data flow task update is not enabled for a selected adapter, the updates are run.

How to Prevent Probes from Sending Touch Information Simultaneously

When multiple Data Flow Probes send touch information simultaneously to the UCMDB Server, the Server may become overloaded. To enable a manual load balancing between the multiple Data Flow Probes running against the UCMDB Server, you can set the time at which each Probe reports the touch:

1. Open the **DataFlowProbe.properties** file in a text editor.
2. Locate the lines beginning with **# Is touch window mechanism active**:

```
"# Is touch window mechanism active  
appilog.agent.probe.touchWindowMechanism.isActive = false  
"# Defines the time when the touch window starts (HH:MM - 00:00-23:59)  
appilog.agent.probe.touchWindowMechanism.startTime = 10:00
```

```
"# Defines the time when the touch window ends (HH:MM - 00:00-23:59)  
appilog.agent.probe.touchWindowMechanism.endTime = 23:59
```

3. Change the **appilog.agent.probe.touchWindowMechanism.isActive** parameter to **true**.
4. Set the time at which the Probe should report the touch.
5. Save the file.

These parameters enable the Probes to perform "touching" in non-overlapping time frames.

How to Encrypt/Decrypt IP Ranges Information on the Probes

In version 10.31, a new attribute **domain_encrypt** is added in the **domainScopeDocument.xml** file to act as a flag to tell the probe whether to encrypt or decrypt the IP ranges related information in the **domainScopeDocument.xml** and **domainRangesDocument.xml** files on the Data Flow Probe. There is no need to manually modify the attribute. You can invoke the new JMX method **setDomainEncrypt** to control this attribute.

To encrypt/decrypt IP ranges information on the probe:

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. Locate **UCMDB:service=Discovery Manager** and click the link to jump to the Operations table.
3. Click the **setDomainEncrypt** operation.
4. To encrypt the IP ranges related information in the **domainScopeDocument.xml** and **domainRangesDocument.xml** files on all the Data Flow Probes connected to this UCMDB Server, provide customer ID (default: 1) and select **True**.

Note: By default, the IP ranges related information in the **domainScopeDocument.xml** and **domainRangesDocument.xml** files are not encrypted.

To decrypt the encrypted IP ranges information, provide customer ID and select **False**.

5. Click **Invoke**.


The **domain_encrypt** attribute value in the **domainScopeDocument.xml** is successfully changed.

Then the Probes connected to the UCMDB server will encrypt or decrypt IP ranges related information in the **domainScopeDocument.xml** and **domainRangesDocument.xml** accordingly. Specifically, the following will be encrypted/decrypted:

- The following sections containing IP ranges information in **domainScopeDocument.xml**:
domain_probes, **domain_scopelist**, and **domain_probeclusters**
- All content in the root element **DomainsRangeDocument** in **domainRangesDocument.xml**.

How to Configure the Data Flow Probe to Automatically Delete CIs

This task explains how to configure a job so that CI instances of specific CITs are automatically deleted.

1. Select the CIs to be deleted
 - a. Select an adapter.
 - b. In the **Adapter Configuration** tab > **Results Management** pane, select **Enable Automatic Deletion** and in the adjacent drop-down box, select when to enable automatic deletion: **Always**, **On Success or Warnings**, or **Only on Success**.
 - c. In the **Automatic Deletion** box, click .
 - d. In the Choose Discovered Class dialog box that opens, select CITs for deletion. For details, see ["Choose Discovered Class Dialog Box" on page 268](#).
 - e. In the **Automatic Deletion** box, in the Deletion Method column, select the deletion method for the CIT: **Auto Delete** or **Candidate for Deletion**. For details on the deletion methods, see ["Automatically Deleted CIs and Relationships and Candidates for Deletion CIs" on page 226](#).
 - f. Click the **Save** button at the bottom of the page.
2. Results

To view the deleted CIs, access the **Deleted** column in the Discovery Results pane. For details, see ["Discovery Results Tab/Pane" on page 678](#).

How to Delete Unsent Probe Results

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

1. Access the Data Flow Probe JMX console: On the probe machine, launch a Web browser and enter the following address: **https://localhost:8453**.

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

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

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

How to Clear Data Flow Probe Data

This task describes how to clear the data from the Data Flow Probe.

Note: For details on clearing the data from the UCMDB Integration Service, see "[How to Clear UCMDB Integration Service Data](#)" on the next page.

1. Stop the Data Flow Probe service. To do this, see "[How to Stop a Data Flow Probe](#)" on page 58.
2. Run the **clearProbeData** script

Note: The **clearProbeData** script resets the Data Flow Probe's DB schemas and file system state. After running this script the Data Flow Probe resends all the discovered data to UCMDB. This could potentially create a significant load on the UCMDB Server.

Windows	<ol style="list-style-type: none">a. On the Data Flow Probe machine, go to: c:\hp\UCMDB\DataFlowProbe\toolsb. At the command prompt, type:
---------	--

	clearProbeData.bat
Linux	/opt/hp/UCMDB/DataFlowProbe/tools/clearProbeData.sh

- Restart the Data Flow Probe service

Start the Data Flow Probe service. For details, see ["How to Start a Data Flow Probe" on page 56](#).

- Results

All the data is deleted from the Data Flow Probe.

How to Clear UCMDB Integration Service Data

This task describes how to clear the data from the UCMDB Integration Service.

Note: For details on clearing the data on a Data Flow Probe, see ["How to Clear Data Flow Probe Data" on the previous page](#).

- Stop the Integration Service.

Windows	Start > All Programs > UCMDB > Stop Universal CMDDB Integration Service
Linux	/opt/hp/UCMDB/UCMDBServer/integrations/bin/service.sh stop

- Run the **clearProbeData** script.

Note: The **clearProbeData** script resets the Integration Service's DB schemas and file system state. After running this script the Integration Service resends all the discovered data to UCMDB. This could potentially create a significant load on the UCMDB Server.

On the UCMDB Server machine, run the script as follows:

Windows	c:\hp\UCMDB\UCMDBServer\integrations\tools\clearProbeData.bat
Linux	/opt/hp/UCMDB/UCMDBServer/integrations/tools/clearProbeData.sh

- Restart the Integration Service:

Windows	Start > All Programs > UCMDB > Start Universal CMDDB Integration Service
Linux	/opt/hp/UCMDB/UCMDBServer/integrations/bin/service.sh start

4. Results

All the data is deleted from the Integration Service.


How to Deploy a Data Flow Probe CUP

This task describes how to deploy a cumulative update package (CUP) for Data Flow Probes (Windows/Linux) connected to UCMDB.

Note:

- This task describes how to deploy the Probe CUP from within the UCMDB user interface. For instruction on deploying the Data Flow Probe CUP manually on an individual Probe, see ["How to Deploy a Data Flow Probe CUP Manually" on the next page](#).
- Upgrading Data Flow Probes that operate in separate mode is not supported. To perform an upgrade, see ["How to Deploy a Data Flow Probe CUP Manually" on the next page](#).
- Download CUPs from the [ITOM Marketplace](#) site. For more information, see ["Universal Discovery Community" on page 416](#). For detailed instructions on how to install CUPs, see the release notes document that is included in the CUP package.

To deploy a Data Flow Probe CUP on all the connected Data Flow Probes:

1. In Data Flow Management, go to the Data Flow Probe Setup module.
2. Click the **Deploy Probe Update**  button.
3. Select a CUP version to deploy, and click **OK**.
4. **Linux only:**
 - a. Extract the upgrade package by running:

```
/opt/hp/UCMDB/DataFlowProbe/tools/upgrade/extractUpgradePackage.sh
```
 - b. Restart the Data Flow Probe.
5. **Windows Probe only:** Verify that the Probes is connected and that the Probe version is updated: Go to **Data Flow Management > Data Flow Probe Setup**, and select the domain. For details, see ["<Domain> Details Pane" on page 111](#).

Note:

- During the CUP deployment process, all compatible Data Flow Probes are automatically restarted. If an integration is running on a Data Flow Probe while it is restarting, the integration stops running, and starts over when the Data Flow Probe restarts. If an integration is almost finished running, or a significant part has already run, to avoid starting the integration over, we recommend letting it complete its run, and, thereafter, updating the CUP.
- To undeploy a Data Flow Probe CUP for the purpose of aligning the CUP version with the UCMDB Server's CUP version, see ["How to Align the Data Flow Probe CUP with the UCMDB Server CUP" on the next page.](#)

How to Deploy a Data Flow Probe CUP Manually

This task describes how to manually deploy a Data Flow Probe CUP on an individual Data Flow Probe.

Note:

- This procedure can be used if you are upgrading Data Flow Probes that operate in separate mode. If your Data Flow Probe is not operating in this mode, see ["How to Deploy a Data Flow Probe CUP" on the previous page.](#)
- Download CUPs from the [ITOM Marketplace](#). For more information, see ["Universal Discovery Community" on page 416](#). For detailed instructions on how to install CUPs, see the release notes document that is included in the CUP package.

1. Prerequisites

To avoid loss of data, deactivate all discovery jobs before running the update.

2. Install the UCMDB CUP

Run the installation wizard to install the UCMDB server CUP only.

3. Copy files from UCMDB server to Data Flow Probe

Copy the CUP package file from the following source locations on the UCMDB server to the following destination locations on the Data Flow Probe as follows, depending on the OS platform you are using:

Note: When the Data Flow Probe is operating in separate mode, copy the file to both the

Data Flow Probe gateway and Data Flow Probe manager.

Windows:

Source: C:\hp\UCMDB\UCMDBServer\content\probe_patch\probe-patch-10.<VersionNumber>.CUP<VersionNumber>-windows.zip

Destination: C:\hp\UCMDB\DataFlowProbe\runtime\upgrade\ probe-patch-10.<VersionNumber>.CUP<VersionNumber>-windows.zip

Linux:

Source: C:\hp\UCMDB\UCMDBServer\content\probe_patch\probe-patch-10.<VersionNumber>.CUP<VersionNumber>-linux.zip

Destination: /opt/hp/UCMDB/DataFlowProbe/runtime/upgrade/probe-patch-10.<VersionNumber>.CUP<VersionNumber>-linux.zip

4. Restart the Data Flow Probe

Restart the Probe.

5. Result

(Windows only) Verify that the Probe is connected and that the Probe version is updated: Go to **Data Flow Management > Data Flow Probe Setup**, select the domain select the Probe. For details, see "[<Domain> Details Pane](#)" on page 111.

Note:

- If this process fails, uninstall the Probe, reinstall a new Probe, and then deploy the relevant Probe CUP.
- For details on installing the Probe, see the interactive *Universal CMDB Deployment Guide*.

How to Align the Data Flow Probe CUP with the UCMDB Server CUP


The cumulative update package (CUP) version of Data Flow Probes connected to the UCMDB Server must always be aligned with the corresponding CUP version of the UCMDB Server.

This task describes how to align the CUP version on the Data Flow Probes with the corresponding UCMDB Server's CUP.


Note:


- Aligning Data Flow Probe CUPs is necessary only if any of the connected Data Flow Probes in your system are installed with CUP versions that are later than the UCMDB Server CUP version.
- This option is available only for Probes that were **updated** with a CUP version (manually or using the Deploy Probe Update feature).
- If a Probe installation includes a CUP, you cannot uninstall the CUP. To uninstall the CUP, you need to uninstall the Probe, and then reinstall the Probe with the correct CUP version.


To align the Data Flow Probe CUP version:

1. In Data Flow Management module, go to **Data Flow Probe Setup**.
2. Click the **Undeploy Probe Update**  button. The CUP version on each Data Flow Probe is downgraded by one CUP version, relative to the CUP version installed on each Data Flow Probe.

Note: If this button is not enabled, the CUP on each of the Probes is aligned with UCMDB, and nothing further needs to be done.

3. As long as the **Undeploy Probe Update**  button is enabled, this indicates that there is one or more Probe whose CUP version is not aligned with the UCMDB Server's CUP version. Click this button again to align the CUP version on those Probes.

When the **Undeploy Probe Update**  button becomes disabled, this indicates that the CUP version on all of the Probes is aligned with the UCMDB Server's CUP version.

4. Remove the CUP resource from UCMDB to ensure that it is not deployed again:
 - a. In **Administration > Package Manager**, select the **probeUpdate** package, and click **Undeploy Resources** .
 - b. In the Undeploy Package Resources dialog box that opens, select the CUP resource.
 - c. Click **Next** and then **Finish**.

Example

Consider the following deployment:

- UCMDB Server has CUP1 installed
- Probe1 has CUP1 installed.
- Probe2 has CUP2 installed.
- Probe3 has CUP3 installed.

Aligning the CUP versions will have the following effect:

- Probe1 remains untouched because its CUP version is aligned with that of the UCMDB Server.
- Probe2 is downgraded to CUP1.
- Probe3 is downgraded to CUP2.

In order for Probe3 to be compatible with the UCMDB Server, aligning the CUP versions again will have the following effect:


- Probe1 and Probe2 remain untouched because their CUP versions are aligned with that of the UCMDB Server.
- Probe3 is downgraded to CUP1.

How to Uninstall Probe CUPs Manually

This task describes how to uninstall a Data Flow Probe CUP that was deployed manually. This can be done using manual methods only.

To uninstall a Probe CUP manually:

1. Stop the Probe.
2. Copy `${PROBE_INSTALL}\UninstallCUP\CUP_NUMBER\ probeUninstallCup<CUP_number>.zip` to the `${PROBE_INSTALL}\runtime\upgrade\` directory.
3. From the command prompt, navigate to the `${PROBE_INSTALL}\tools\upgrade\` directory.
4. Run:
 - **Windows:** `extractUpgradePackage.bat`
 - **Linux:** `extractUpgradePackage.sh`
5. Ensure that the CUP resource was removed from UCMDB so that it is not deployed again:

- a. In **Administration > Package Manager**, select the **probeUpdate** package, and click **Undeploy Resources** .
- b. In the Undeploy Package Resources dialog box that opens, if the CUP resource is displayed, select it.
- c. Click **Next** and then **Finish**.

How to Set Maximum Objects for Insert Results

Starting with version 10.32, when there are more Data Flow Probes in your environment, the database performance (Oracle or Microsoft SQL server) during discovery can be improved with the introduction of a new configurable infrastructure setting **Set Max Objects For Insert Results**.

This setting allows you to set the maximum number of merge queries in a transaction for the CCM_DISCOVERY_DESTS_RESULTS table (default value: **50**) from UCMDB UI. It takes effect immediately and does not require server restart. You can adjust the value according to your environment.

Note: As a result of this change, the **-DmaxObjectsForInsertResults** parameter in the **wrapper.conf** file becomes invalid.

Data Flow Probe Process Ports

- ["Data Flow Probe Machine Ports" below](#)
- ["Remote Machine Ports" on page 82](#)

Data Flow Probe Machine Ports

The following ports are used by the Data Flow Probe process on the Data Flow Probe machine:

Port	Description
1977	Data Flow Probe's web application port. Used for JMX console and other web services.
1978	If the Data Flow Probe is installed in separate mode (Probe Manager and Probe Gateway are running in separate processes), this port is used by the Probe Manager process for the web

Port	Description
	application port (Manager's JMX console).
1979	Web application port for the second Data Flow Probe (if installed). Used for JMX console and other web services.
8453	Data Flow Probe's secured web application port. Same as 1977, and is used for the JMX console and other web services if the Jetty HTTPS mode is enabled. Also used to redirect Credential Manager requests when the Data Flow Probe is installed in separate mode.
8454	Data Flow Probe's secured web application port. If the Data Flow Probe is installed in separate mode and Jetty HTTPS mode is enabled, this port is used by the Probe Manager process for the web application port (Manager's JMX console).
8455	Secured web application port for the second Data Flow Probe (if installed). It is used to share the Incoming and Original directories via HTTPs.
1741	Port opened by the Probe Gateway to enable RMI (Remote Method Invocation) between Gateway and Managers.
1742	Port opened by the Probe Manager to enable RMI (Remote Method Invocation) between Gateway and Managers.
80	Opened by a CallHome service for Universal Discovery Agents.
81	Opened by a CallHome service for Universal Discovery Agents. This port is used by the second Data Flow Probe (if installed).
5432	Port used by the PostgreSQL database.
5433	Port used by the PostgreSQL database for the second Data Flow Probe (if installed).
1777	Port used by the Tanuki wrapper.
2055	Port opened when the Collect Network Data by Netflow job has been activated. Used for connecting netflow data reported by nProbe software.
34545	Port used by the XML Enricher. Note: The port 34545 only listens on localhost if Data Flow Probe is newly installed. However, if Data Flow Probe is upgraded to the latest version, you need to add the following setting to the wrapperEnricher.conf file manually. <pre># Make rmi listen on localhost only wrapper.java.additional.<the number>=- Djava.rmi.server.hostname=localhost</pre>
34645	Port used by the XML Enricher for the second Data Flow Probe (if installed).

Remote Machine Ports

The following ports are used by the Data Flow Probe process on remote machines:

Port	Description
5672	Used for AMQP-based discovery.
5989	Used for CIM-based discovery.
8080	Data Flow Probe uses this port to communicate with the UCMDB server (if the communication is configured to HTTP).
8443	Data Flow Probe uses this port to communicate with the UCMDB server (if the communication is configured to HTTPS).
22	Used for SSH-based discovery.
23	Used for Telnet-based discovery.
80/81	Used for HTTP, NetApp SANscreen/OnCommand, NNM, PowerShell, UDDI, VMware VIM discoveries. If the second Data Flow Probe is installed, port 81 will be used.
135, 137, 138, 139, 445 + DCOM ports	Used for WMI and NTCMD discoveries. Note: It is recommended that you use port 445. This is because, by default, Windows 2000 and later versions use SMB over TCP/IP via port 445 rather than over NetBIOS whenever possible. If port 445 is disabled, it will fall back to NetBIOS using port 137, 138, or 139.
161	Used for SNMP discovery.
389	Used for LDAP discoveries.
1521, 1433, 6789, 3306, 2048, 5432	Used for SQL (Database)-based discoveries.
2738, 7738	Used for Universal Discovery Agent-based discoveries.
443	Used for UCS, UDDI, VMWare VIM, NetApp, PowerShell discoveries.
280	Used for HPE SIM discovery.
1099	Used for Network Automation Java, JBoss discoveries.
5985, 5986	Used for PowerCmd, PowerShell discoveries. Note: These ports depend on the Microsoft Windows operating system configuration.
3200, 3300-3303, 33xx, where xx is the SAP server instance number	Used for SAP discovery.

Port	Description
50004, 50104, 50204, 50304, 50404, 5xx04 where xx is the SAP J2EE server instance number	Used for SAP JMX discovery.
2320	Used for Siebel Gateway discovery.
7001, 7002	Used for WebLogic discovery.
8880	Used for WebSphere discovery.
50001	Used for HPE SIM discovery (secure communication).

DataFlowProbe.properties File

A DFM process needs several parameters to be activated. These parameters specify the method to be used (for example, ping five times before declaring a failure) and against which CI a method should be run. If parameters have not been defined by the user, the DFM process uses the default parameters defined in the **DataFlowProbe.properties** file. If parameters have been defined by the user, the DFM process uses the custom parameters defined in the **DataFlowProbeOverride.properties** file first, and then the **DataFlowProbe.properties** file.

The **DataFlowProbe.properties** file is located in the following folder:

C:\hp\UCMDB\DataFlowProbe\conf.

Note: Starting with version 10.33, if you want to edit or update any property in the **DataFlowProbe.properties** file, if the property also exists in the **DataFlowProbeOverride.properties** file, we highly recommend you to make sure the property is updated in both files to keep consistency.

Probe restart is required for the changes to take effect.

The **DataFlowProbe.properties** file is divided into the following sections:

- **Server Connection Definitions.** Contains parameters that are needed to set up the connection between the server and the Probe, such as the protocol to be used, machine names, default Probe and domain names, time-outs, and basic authentication.
- **Data Flow Probe Definitions.** Contains parameters that define the Probe, such as root folder location, ports, and Manager and Gateway addresses.

- **Probe Gateway Configurations.** Contains parameters that define time intervals for retrieving data.
- **Probe Manager Configurations.** Contains parameters that define Probe Manager functionality, such as scheduled intervals, touching, result grouping, chunking, threading, time-outs, filtering, and reporting multiple updates.
- **I18N Parameters.** Contains parameters that define language settings.
- **Internal Configurations.** Contains parameters that enable DFM to function efficiently, such as thread pool size.

Caution: Internal configuration parameters should not be changed without an advanced knowledge of Data Flow Management.

DataFlowProbe.properties Parameters

This section describes the parameters of the **DataFlowProbe.properties** file.

These include:

- ["Server Connection Definitions" below](#)
- ["Data Flow Probe Definitions" on page 87](#)
- ["Probe Gateway Configurations" on page 91](#)
- ["Probe Manager Configurations" on page 92](#)
- ["I18N Parameters" on page 97](#)

Server Connection Definitions

Parameter Name (A-Z)	Description	Type	Value
appilog.agent.Probe.DownloadingTimeout	Timeout (in ms.) for download configuration files and userExt files (that is, serverData files).	long	Default: 300000
appilog.agent.probe.protocol	Defines the protocol used to communicate between the Probe Gateway and the	string	HTTP or HTTPS (SSL) Default: HTTPS

Parameter Name (A-Z)	Description	Type	Value
	Server.		
appilog.agent.Probe. ServerTimeout	Timeout (in ms.) for Probe requests going to the server.	long	Default: 180000
appilog.agent.Probe. ServerTimeoutForTouch	Timeout (in ms.) for touch requests going to the server.	long	Default: 300000
appilog.agent.Probe. BasicAuth.User appilog.agent.Probe. BasicAuth.Pwd	Basic authentication feature of Probe to Server. These properties are supplied by the admin who configured the Web server. Deprecated: certificate-based, mutual SSL authentication should be used instead.	string	All keys must be used to indicate usage of this feature. Values can be empty to represent non-values. Password has to be encrypted. Encrypt password using the Probe JMX (that is, the getEncryptedKey Password operation in the MainProbe MBean).
appilog.agent.Probe. JMX.BasicAuth.User	Authentication data for the Probe JMX - user name.	string	All keys must be used to indicate usage of this feature. Values can be empty to represent non-values.
appilog.agent.Probe. JMX.BasicAuth.Pwd	Authentication data for the Probe JMX - password.	bytes	Password has to be encrypted. Encrypt password using the Probe JMX (that is, the getEncryptedKey Password operation in the MainProbe MBean).
appilog.agents.probemgr. progressSleepTime	"Sleeping" time of the thread that is responsible for sending the progress to gateway.	long	Default: 40000
appilog.collectors. domain	The domain which the Probe Gateway belongs to (formerly known as the Domain of the Probe).	string	Default: \${DefaultDomain}
appilog.collectors. domain.type	The type of the domain.	string	customer (default); external
appilog.collectors. probe.name	The Probe Gateway name used for identification by the UCMDB server	string	Uses the value defined during installation.

Parameter Name (A-Z)	Description	Type	Value
	The server uses this name to pass tasks to the appropriate Probe Gateway.		The default value is the machine name.
com.hp.ucmdb.discovery.Probe.JMX.UploadAuth.User	Authentication data for the discovery Probe JMX - user name.	string	Default: UploadScanFile
com.hp.ucmdb.discovery.Probe.JMX.UploadAuth.Pwd	Authentication data for the discovery Probe JMX - password.	bytes	Password has to be encrypted. Encrypt password using the Probe JMX (that is, the getEncryptedKeyPassword operation in the MainProbe MBean).
httpConnectionLimit	The max number of connections probe establish with server. This value must be greater than 0.	int	Default: 5
jettyGtwHttpPort	The port of the jetty server used by Probe Gateway (in separate mode), or the Probe (in union mode).	int	Default: 1977 ; 1979 for the second probe (if installed)
jettyGtwHttpsPort	The https port of the jetty server used by Probe Gateway (in separate mode), or the Probe (in union mode).	int	Default: 8453 ; 8455 for the second probe (if installed)
jettyMgrHttpPort	The port of the jetty server used by Probe Manager (in separate mode).	int	Default: 1978 ; 1980 for the second probe (if installed)
jettyMgrHttpsPort	The https port of the jetty server used by Probe Manager (in separate mode).	int	Default: 8454 ; 8456 for the second probe (if installed)
jettyHttpsEnabled	Enables using the default https server. Starting with version 10.31, the default value for this setting is true for fresh installed probes of version 10.31 (or later). The HTTPS port 8453 is enabled for the	Boolean	Default: true

Parameter Name (A-Z)	Description	Type	Value
	<p>Probe by default, and the HTTP port 1977 disabled. For details, see "Using HTTPS Port 8453 as Default for Data Flow Probe" in <i>Universal CMDB Hardening Guide</i>.</p> <p>Note: For off-site scan file saving, only the HTTPS port 8453 can be used. If you want to use HTTP port 1977 for scan files saving, set jettyHttpsEnabled to false.</p>		
reuseHttpConnection	Probe reuses the connection with the server.	boolean	Default: false
server.webApp.name	Name of the server Web application (.war file) responsible for the Probe.	string	Default: mam-collectors
server.webApp.root.context	UCMDB server's root context, will be used by server.webApp.name and com.hp.ucmdb.discovery.common.security.cmRestContext .	string	Default: /
serverName	Defines the Server DNS name to which the Probe Gateway connects.	string	The DNS name
serverPort	The port number for HTTP communication.	int	Default: 8080
serverPortHttps	The port number for HTTPS communication.	int	Default: 8443

Data Flow Probe Definitions

Parameter Name	Description	Type	Value
appilog.agent.	Communication port used by	int	Default: 80; 81 for the second

Parameter Name	Description	Type	Value
callhome.port	the Universal Discovery Agent Call Home functionality		probe (if installed)
appilog.collectors.storeDomainScopeDocument	Specifies whether the (encrypted) DomainScope document should be stored on the Data Flow Probe's DB and file system (true) or be retrieved each time the Probe comes up and stored in memory only (false).	boolean	Default: true
appilog.agent.local.jdbc.user	PostgreSQL user name	string	Default: mamprobe
appilog.agent.local.jdbc.pwd	PostgreSQL password	bytes	To change the DB password: <ol style="list-style-type: none"> 1. The out-of-the-box script set_dbuser_password.cmd can be used in order to change the password of the default PostgreSQL user. 2. The password value in the properties file should be encrypted. Encrypt the password using the Probe JMX (that is, getEncryptedKeyPassword operation in MainProbe MBean).
appilog.agent.probe.jdbc.driver	Probe Gateway database information	string	Default: org.postgresql.Driver
appilog.agent.probe.jdbc.uri	Probe Gateway database information	string	Default: jdbc:postgresql://localhost/dataflowprobe jdbc:postgresql://localhost:5433/dataflowprobe for the second probe (if installed)
appilog.agent.probe.jdbc.useCmdbSchema	Probe Gateway database information	boolean	Default: false

Parameter Name	Description	Type	Value
appilog.agent.probe.jdbc.user	Probe Gateway user name	string	Default: mamprobe
appilog.agent.probe.jdbc.pwd	Probe Gateway password	bytes	Password has to be encrypted. Encrypt password using the Probe JMX (that is, getEncryptedKeyPassword operation in MainProbe MBean).
appilog.agent.local.jdbc.driver	Probe Manager database information	string	Default: org.postgresql.Driver
appilog.agent.local.jdbc.uri	Probe Manager database information	string	Default: jdbc:postgresql://localhost/dataflowprobe jdbc:postgresql://localhost:5433/dataflowprobe for the second probe (if installed)
appilog.agent.local.jdbc.useCmdbSchema	Probe Manager database information	boolean	Default: false
appilog.agent.normalization.jdbc.user	Normalization database info	string	Default: mamprobe
appilog.agent.normalization.jdbc.pwd	Normalization database info	bytes	Password has to be encrypted. Encrypt password using the Probe JMX (that is, getEncryptedKeyPassword operation in MainProbe MBean).
appilog.agent.normalization.jdbc.driver	Normalization database info	string	Default: org.postgresql.Driver
appilog.agent.normalization.jdbc.uri	Normalization database info	string	Default: jdbc:postgresql://localhost/dataflowprobe jdbc:postgresql://localhost:5433/dataflowprobe for the second probe (if installed)
appilog.agent.normalization.jdbc.	Normalization database info	boolean	Default: false

Parameter Name	Description	Type	Value
useCmdbSchema			
appilog.agent.netflow.jdbc.uri	Netflow database info	boolean	Default: jdbc:postgresql://localhost/dataflowprobe jdbc:postgresql://localhost:5433/dataflowprobe for the second probe (if installed)
appilog.collectors.probeLocalUnion	true : Probe GW process should also run a Probe Manager on same JVM. false : Probe manager runs separately	boolean	Default: true
appilog.collectors.rmi.gw.port	Communication port between Probe GW and Probe Managers in case they are installed on separate processes	int	Default: 1742 ; 1744 for the second probe (if installed) Note : This value should be the same for all installed Probe Managers belonging to this Probe Gateway.
appilog.collectors.rmi.port	Internal communication port	int	Default: 1741 ; 1743 for the second probe (if installed) Note : This value should be the same for all installed Probe Managers belonging to this Probe Gateway.
appilog.collectors.storeDomainScopeDocument	true : Encrypted DomainScope document is stored on file system and internal DB. false : Encrypted DomainScope document is retrieved from server each startup and stored only in memory.	boolean	Default: true
appilog.collectors.local.ip	The Probe Manager IP address or DNS name	string	DNS Name

Parameter Name	Description	Type	Value
appilog.collectors.probe.ip	The Probe Gateway IP address or DNS name	string	DNS Name
probe.fips.status	<p>Indicates which stage the probe is on in FIPS mode: 0 = NON-FIPS 1 = JCE is ready 2 = FIPS</p> <p>Note: Not present in the DataFlowProbe.properties file by default. It has no value until after users change the probe master key manually.</p>	int	Default: 0

Probe Gateway Configurations

Parameter Name	Description	Type	Value
appilog.agent.probe.integrationsOnlyProbe	Mark this probe to run integration tasks only. Intended to SaaS and local probe installations only.	boolean	Default: false
appilog.agent.probe.reconnection.interval	The interval in ms. between reconnection attempts of the Probe Gateway to its Probe Managers.	long	Default: 30000
appilog.agent.probe.retrieveTasksFromServer.interval	The interval in ms. between task requests from the server by the Probe Gateway.	long	Default: 15000
appilog.agent.probe.saveResultsInBKPTable	<p>true: Results sent to the Server are stored in the database in a backup table.</p> <p>false: Results are not stored in a backup table.</p>	boolean	Default: false
appilog.agent.probe.restartProbeAfterJarDownload.interval	Downloaded jar file resources can cause the Data Flow Probe to restart before all the other resources of an adapter package have downloaded. This parameter prevents the restart from occurring.	long	Default: 180000 msec (3 minutes) <p>Note: The delay until a restart on the</p>

Parameter Name	Description	Type	Value
			first resource download (that is, for a first start or after clearing the Probe data) is 10 milliseconds.
appilog.agent.probe.sendtouchResultsToServer.maxObjects	The maximum objects of the touch results to be sent to the server each time. Note: Setting this parameter higher than 500 may cause communication exceptions.	int	Default: 500
probe.master.key	Specifies probe master key for password encryption purpose. Note: For a probe that is upgraded to version 10.21 or later, this parameter is not present by default. You can manually add this parameter and set the value for the parameter by using the changeMasterKey JMX method. For details, see the <i>Universal CMDB JMX Reference Guide</i> .	string	Default: appilog.common.system.types.vectors.ObjectStateHolderVector

Probe Manager Configurations

Parameter Name	Purpose	Type	Value Description
jettyMgrHttpsPort	The https port of the jetty server used by Probe Manager (in separate mode).	int	Default: 8454 ; 8456 for the second probe (if installed)
appilog.agent.local.max.worker.runtime	Maximal time (in msec) which a worker thread is allowed to run.	long	Default: 900000
appilog.agent.local.	After this period it is considered as stuck.	int	Default: 8

Parameter Name	Purpose	Type	Value Description
max.worker.stuck			
appilog.agent.local.check.stuckThreads	Maximal number of worker threads which can be considered as stuck at the same time. When the number is reached, the Probe schedules a restart to release these threads. true - the Probe Manager should detect stuck threads. false - otherwise.	boolean	Default: true
appilog.agent.local.discoveryAnalyzerFromEclipse	Setting to true enables that DiscoveryAnalyzer is executed from Eclipse.	boolean	Default: false
appilog.agent.local.process.result.checkMultiUpdate	Defines whether to check data consistency on objects.	boolean	Default: true
appilog.agent.local.services.maxRemoteProcesses	The maximum number of remote processes allowed to be created during discovery. Remote processes are used to separate specific discovery from Probe process to prevent the Probe from possible memory issues. Used, for example, in J2EE Discovery.	int	Default: -1 (no limit)
appilog.agent.local.services.maxRemoteProcessesPerJob	The maximum number of remote processes per job that are allowed to run simultaneously.	int	Default: 3
appilog.agent.local.process.result.dataValidation	Checks results for invalid data.	boolean	Default: true
appilog.agent.local.process.result.dataValidation.content	Defines whether to validate data reported to the UCMDB server by content. Deals mainly with reported values (that is, attribute value), rather than metadata of objects.	boolean	Default: true
appilog.agent.local.process.result.autoDelete	true - send auto-delete notification to Server for aged objects, not discovered by the Probe. false - do not send Note: This can be enabled only if appilog.agent.local.process .	boolean	Default: true

Parameter Name	Purpose	Type	Value Description
	<code>result.filterRedundant</code> is enabled.		
appilog.agent.local.process.result.dataValidation.validLinks	true - validate links are legal. false - do not validate links.	boolean	Default: true
appilog.agent.local.process.result.filterCI	true - filter results be predefined rules (CI types). false - otherwise	boolean	Default: true
appilog.agent.local.process.result.filterRedundant	true - filter results which have been already sent to server. false - disable filter.	boolean	Default: true
appilog.agent.local.process.result.filterRedundant.filterIgnoredCIs	<ul style="list-style-type: none"> true. If CIs were ignored by reconciliation on a discovery cycle, as long as they have not undergone any changes, they are filtered by the Probe on subsequent discovery cycles, and a warning is displayed on the trigger CI level. To resend these objects, you must clear the results cache. false. Even if CIs that were ignored by reconciliation, they are still sent to the UCMDB on each discovery cycle, together with new and updated CIs. 	boolean	Default: true
appilog.agent.local.process.result.fixLinksDirection	true - fix direction of illegal links. false - otherwise.	boolean	Default: true
appilog.agent.local.process.result.storedata	Store the result data in probe manager database when a new record is inserted.	boolean	Default: true
appilog.agent.local.process.result.updateClassModel	Update class model (change classes and attributes name) as part of results processing chain.	boolean	Default: true
appilog.agent.local.process.result.warnOnMultiUpdate	true - Reports multiple update warnings to the UCMDB server. Note: This parameter is global. It can be overridden on the adapter level by the warnOnDuplicates parameter which is	boolean	Default: true

Parameter Name	Purpose	Type	Value Description
	absent by default, but gets its value from the global parameter.		
appilog.agent.local.services.poolThreads	Maximal number of concurrent threads allocated for the multi-threaded job's execution activity.	int	Default: 80
appilog.agent.local.services.defaultMaxJobThreads	Maximal number of concurrent threads running on a specific job.	int	Default: 8
appilog.agent.local.services.adHocMaxThreads	Maximal number of threads for ad hoc tasks.	int	Default: 20
appilog.agent.local.discoveryAnalyzerFromEclipse	True: DiscoveryAnalyzer is executed from Eclipse. False: DiscoveryAnalyzer is not executed from Eclipse.	boolean	Default: false
appilog.agent.local.download.erroneous.configuration.documents.interval	Interval before re-download of erroneous configuration document from server.	int	Default: 1440
appilog.agent.local.maxTaskResultSize	Chunk maximal size of results being sent to the server.	int	Default: 20000 Note: Lowering this value lowers the number of CIs sent to the CMDB in a single bulk.
appilog.agent.local.maxTaskResultPrint	Probe mgr - Bulk with more results that set on this parameter will not be printed to task	int	Default: 2000

Parameter Name	Purpose	Type	Value Description
LogSize	results log.		
appilog.agent.local.probe.restart.interval	Interval (in ms) before auto-restarts of the Probe Manager.	long	Default: 900000
appilog.agent.local.serverdata.sync.timeout	Timeout (in msec) for the Probe to sync with Server data before starting executing tasks.	long	Default: 60000
appilog.agent.local.specialCharacters Remove	Filter characters from string attributes of result objects which are reported to server by Probe.	string	Default: empty string (do not filter)
appilog.collectors.probemgr.DefaultResult GroupMinTime appilog.collectors.probemgr.DefaultResult GroupMaxObjs	Probe Mgr - Result Grouping defaults (used when DFM adapter does not override). Grouping means holding on to results and sending them to the Gateway only upon meeting one of the grouping thresholds. This is used to control the rate of data flowing from Probes to the Server.	long	Default min: 5000 Default max: 30000 (in ms.) Relation between two keys: OR
appilog.collectors.listenertaskmgr.load.jars.recursive	When building the class path, probe manager looks for jar/class files only in # listed directories (recursive=false) or search recursively (true).	Default: false	Default: false
appilog.agent.probe.touchWindowMechanism.isActive	The touch window defines the period when touch process is allowed . The parameter defines whether the touch window mechanism is active.	boolean	Default: false
appilog.agent.probe.touchWindowMechanism.startTime	Defines the time, in hours and minutes, when the touch window starts	string	Format: HH:MM Values: 00:00-23:59 Default: 00:00
appilog.agent.probe.touchWindowMechanism.endTime	Defines the time, in hours and minutes, when the touch window ends	string	Format: HH:MM Values: 00:00-23:59 Default: 00:00

I18N Parameters

Parameter Name	Description	Type	Value
appilog.collectors.encoding.ANSI	Default encoding used for Windows applications (requiring ANSI encoding)	string	Default: empty (ANSI encoding is chosen from the Data Flow Probe operating system)
appilog.collectors.encoding.OEM	Default encoding used for DOS/UNIX Shells/IBM encoded applications.	string	Default: empty (OEM encoding is chosen from the Data Flow Probe operating system)
chcpCodeTo CharasetName.xxx	Mapping entry between chcp code page to specific encoding name (used for cases where the cp+<code> rule is not followed)	string	Syntax: chcpCodeTo CharasetName.<code>=<encoding_name> Example: chcpCodeTo CharasetName.932=MS932
collectors_language	Language settings (must be manually configured for non-English environments).	string	Default: English Options: get=German rus=Russian

DataFlowProbeOverride.properties File

Starting with UCMDB version 10.31, a new configuration file **DataFlowProbeOverride.properties** is available in the **C:\hp\UCMDB\DataFlowProbe\conf** folder to hold all custom input during probe installation/upgrade as well as customized changes you made to probe properties through UCMDB UI or via the JMX console. The **DataFlowProbe.properties** file holds all out-of-the-box (OOTB) properties values.

Starting with version 10.33, if you want to edit or update any property in the **DataFlowProbe.properties** file, if the property also exists in the **DataFlowProbeOverride.properties** file, we highly recommend you to make sure the property is updated in both files to keep consistency.

Data Flow Probe Database Scripts

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:
 - **Windows:** C:\hp\UCMDB\DataFlowProbe\tools\dbscripts
 - **Linux:** /opt/hp/UCMDB/DataFlowProbe/tools/dbscripts
- 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 data_flow_probe_export.bin in the current directory
importPostgresql [Export file name] [PostgreSQL root account password]	Imports data from a file created by the exportPostgresql 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

Data Flow Probe Log Files

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

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

Note: Alternatively, to access the Data Flow Probe's log files, log in to the JMX console (<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

WrapperProbeGateway.log	Records all the Probe's console output in a single log file. <ul style="list-style-type: none">• Levels:<ul style="list-style-type: none">◦ Error. Any error that occurs within the Probe Gateway.◦ Information. Important information messages, such as the arrival or removal of a new task.◦ Debug. N/A• Basic Troubleshooting: Use this file for any Probe Gateway problems to verify what occurred with the Probe Gateway at any time as well as any important problems it encountered.
probe-error.log	Summary of the errors from the Probe. <ul style="list-style-type: none">• Levels:<ul style="list-style-type: none">◦ Error. All errors in the Probe components.◦ Information. N/A◦ Debug. N/A• Basic Troubleshooting: Messages from the Probe's infrastructure only.
wrapperLocal.log	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. <ul style="list-style-type: none">• Levels:

	<ul style="list-style-type: none"> ○ Error. Any error that occurs within the Probe Manager. ○ Information. Important information messages such as received tasks, task activation, and the transferring of results. ○ Debug. N/A ● Basic Troubleshooting: Use this file for any Probe Manager problems to verify what occurred with the Probe Manager at any time as well as any important problems it encountered.
postgresql.log	<p>Displays database related error during the installation.</p> <p>Note: If this log is empty check in the Event Viewer logs.</p>
pg_upgrade.log	<p>Shows the running details of the pg_upgrade.bat script, including the details about PostgreSQL upgrade and table splitting.</p> <p>The log does not appear in the log folder by default. It appears only when you manually run the pg_upgrade.bat script or may appear when you select the upgrade option during probe installation.</p> <ul style="list-style-type: none"> ● Levels: <ul style="list-style-type: none"> ○ Error. Any error that occurs when PostgreSQL upgrade or table splitting fails. ○ Information. Shows the console output and suggestions when it fails. ○ Debug. N/A ● Basic Troubleshooting: Check this log file when PostgreSQL upgrade or table splitting fails.
probe_upgrade_conf_merge.log	<p>Shows the related information when probe installer merger configuration files.</p> <ul style="list-style-type: none"> ● Levels: <ul style="list-style-type: none"> ○ Error. Any error that occurs when merging configuration files. ○ Information. Shows the console output of normal information. ○ Debug. N/A ● Basic Troubleshooting: Check this log file when the probe installer has problems.
probe_auto_upgrade.log	<p>Shows the related information when the probe auto upgrade agent upgrades a probe.</p> <p>It shows in the C:\hp\UCMDB\DataFlowProbe\runtime\log\probeUpgradeLogs\<source_version>to<target_version> folder. For example: C:\hp\UCMDB\DataFlowProbe\runtime\log\probeUpgradeLogs\10.32t</p>

	<p>o10.33.</p> <p>This log file is also sent to the UCMDB server and shows as <domain_name>_probename_auto_upgrade.log in the C:\hp\UCMDB\UCMDBServer\runtime\log\probeUpgradeLogs\<source_version>to<target_version>\failed success folder.</p> <ul style="list-style-type: none"> • Levels: <ul style="list-style-type: none"> ◦ Error. Any error that occurs when the probe auto upgrade agent upgrades a probe. ◦ Information. Shows the console output of normal information. ◦ Debug. N/A • Basic Troubleshooting: Check this log file when the probe upgrade fails.
--	--

Probe Gateway Logs

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

	<ul style="list-style-type: none"> • Basic Troubleshooting: <ul style="list-style-type: none"> ◦ If the Probe Gateway tasks are not synchronized with the server tasks, check this log to determine which tasks the Probe Gateway received. ◦ You can view the current task's state through the JMX console (use the Discovery Scheduler MBean).
--	--

Probe Manager Logs

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

Discovery Rules Engine Log Files

normalization.audit.log	<p>Logs information about the processing of the Discovery Rules Engine.</p> <ul style="list-style-type: none"> • Levels: <ul style="list-style-type: none"> ◦ Error. N/A ◦ Information. Audits the number of element processed and the number of CIs that were changed. Example: <div style="background-color: #f0f0f0; padding: 5px; margin: 5px 0;"> Normalization (OSHV: 8 elements) (Time: 125 ms) (Modified CIs: 1) </div> ◦ Debug. N/A
normalization.log	<p>Logs detailed information about the processing of the Discovery Rules Engine, enabling you to trace detailed information of the Discovery Rule</p>

	<p>Engine process.</p> <ul style="list-style-type: none"> • Levels: <ul style="list-style-type: none"> ◦ Error. All discovery rule processing errors. ◦ Information. Logs all levels of information about the processing of the Discovery Rules Engine. ◦ Debug. Logs mainly for debugging purposes. • Basic Troubleshooting. Check this log when you need to analyze why a CI was not enriched by the Discovery Rules Engine.
--	---



Data Flow Probe Setup User Interface

This section includes:

New/Edit Policy Dialog Box	103
Add New Domain Dialog Box	104
Data Flow Probe Setup Window	105
New/Edit Range Dialog Box	131





New/Edit Policy Dialog Box

Enables you to create a job execution policy, to disable jobs from running at specific times.

To access	Go to Data Flow Management > Data Flow Probe Setup > Domains and Probes > Details pane > Job Execution Policy section. Select an existing policy and click the Edit Policy  button, or click the New Policy  button.
See also	<ul style="list-style-type: none"> • "Job Execution Policies" on page 36 • "Domains and Probes Details Pane" on page 110


User interface elements are described below:

UI Element (A–Z)	Description
Related jobs	<ul style="list-style-type: none"> • Allow all. Run the job execution policy on all jobs. • Total blackout. The policy does not run on any jobs.

UI Element (A–Z)	Description												
	<ul style="list-style-type: none"> • Allowed jobs. Choose jobs to run even during the configured blackout time. • Disallowed jobs. Choose jobs that do not run during the configured blackout time. <p>For allowed and disallowed jobs, clicking the Add job  button opens the Choose Discovery Jobs dialog box enabling to you choose specific jobs to be included/excluded on the policy.</p> <p>To remove selected jobs, click the Remove job  button.</p> <p>Tip: Use the SHIFT or CTRL key to select multiple jobs or packages.</p>												
Related Probes	The Probes on which to run the policy. Click the  button to open the Edit Related Probes dialog box to define which Probes are included in the policy.												
Time	<p>The date and time during which the policy is active. Click the  button to open the Edit Timetable dialog box.</p> <ul style="list-style-type: none"> • Description. Add a description of the specific policy. This field is mandatory. <p>Tip: The text you enter here appears in the Time column in the Job Execution Policy pane, so it is recommended that the description be informative:</p> <table border="1" data-bbox="435 1087 1125 1245"> <thead> <tr> <th colspan="3">Job Execution Policy</th> </tr> <tr> <th>Time</th> <th>Probes</th> <th>Jobs</th> </tr> </thead> <tbody> <tr> <td>Labor Day weekend</td> <td>All</td> <td>None (total blackout)</td> </tr> <tr> <td>Always</td> <td>All</td> <td>All</td> </tr> </tbody> </table> <ul style="list-style-type: none"> • Time Definition. Click a cell for a day and time to be included in the policy. To add more than one time unit, drag the pointer over the cells. <p>Note: To clear a time unit, click the cell a second time.</p>	Job Execution Policy			Time	Probes	Jobs	Labor Day weekend	All	None (total blackout)	Always	All	All
Job Execution Policy													
Time	Probes	Jobs											
Labor Day weekend	All	None (total blackout)											
Always	All	All											

Add New Domain Dialog Box

Enables you to add a domain.

To access	Go to Data Flow Management > Data Flow Probe Setup > Domains and Probes pane, click  , and select New Domain .
Important information	In a version 8.01 or later environment that has been upgraded from version 6.x, to enable data to be modeled similarly as in the previous version, you must define the

	Probes as belonging to the External domain and not to the Customer domain.
Relevant Tasks	"How to Add Data Flow Probes to UCMDB" on page 54

User interface elements are described below:

UI Element (A–Z)	Description
Description	Enter a description to appear in the Details pane of the Data Flow Probe Setup window.
Domain Type	<ul style="list-style-type: none"> • Customer. A private domain used for your site. You can define several domains and each domain can include multiple Probes. Each Probe can include IP ranges but the customer domain itself has no range definition. • External. Internet/public domain. A domain that is defined with a range. The external domain can contain only one Probe whose name equals the domain name. However, you can define several external domains in your system.
Name	Enter a unique name for the domain.

Data Flow Probe Setup Window






In this window you can manage the discovery domains, Data Flow Probes, and probe clusters in UCMDB. You can also manage connection data for each connection protocol.



To access	Select Data Flow Management > Data Flow Probe Setup .
See also	<ul style="list-style-type: none"> • "How to Add Data Flow Probes to UCMDB" on page 54 • "How to Add Probe Clusters to UCMDB" on page 55 • "How to Start a Data Flow Probe" on page 56 • "How to Stop a Data Flow Probe" on page 58 • Supported Protocols and Supported Agents in the <i>Universal CMDB Discovery and Integrations Content Guide</i>.








Domains and Probes Pane

Enables you to view, define or edit domains, connection credentials, probe clusters, Data Flow Probes, and passive discovery probes. Also enables you to automatically upgrade all the Data Flow Probes with the latest cumulative patch (CUP).

User interface elements are described below (unlabeled elements are shown in angle brackets>):

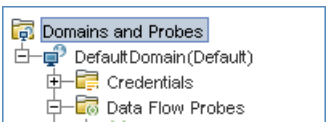
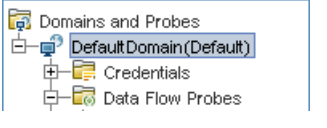
UI Element (A-Z)	Description
	<ul style="list-style-type: none"> • New Domain. Opens the Add New Domain dialog box, enabling you to define a discovery domain in UCMDB. For details, see "Add New Domain Dialog Box" on page 104. Available when: Domains and Probes root is selected • New Data Flow Probe. Opens the Add New Probe dialog box, enabling you to add a Data Flow Probe to UCMDB. Available when: The Data Flow Probes node or a cluster is selected. • New Cluster. Opens the Add New Cluster dialog box, enabling you to define a new probe cluster. For details, see "How to Add Probe Clusters to UCMDB" on page 55. Available when: The Data Flow Probes node is selected.
	<p>Remove Domain/Probe/Cluster. Removes the selected domain, Data Flow Probe/probe cluster, or passive discovery probe.</p> <p>Note:</p> <ul style="list-style-type: none"> • When you remove a Data Flow Probe from a cluster, its network range remains part of the cluster's network range, and a new network range needs to be defined for the Data Flow Probe. Exception: If the Probe was added to a cluster , and then removed without making any changes to its range and before saving the cluster, then its range is not merged with the cluster's range, but remains with the Probe. • If you remove a probe cluster, and its Probes are still up and running, the Probes automatically reconnect to UCMDB server, and, after a few minutes, reappear in the Data Flow Probe Setup under their defined domain.
	<p>Find Probe Range by IP. If a Probe has many defined ranges, you can locate a specific range on the Probe.</p> <p>To do this, select the Probe and click Find Probe Range by IP. In the Find Probe Range dialog box, enter the IP address (in IPv4 or IPv6 format, as appropriate) and click the Find button. The range is highlighted in the Ranges pane.</p>
	<p>Reload Domain Information from Server. Updates all domain and probe information from the server.</p>
	<ul style="list-style-type: none"> • Suspend Probe/Cluster. Suspends the selected Data Flow

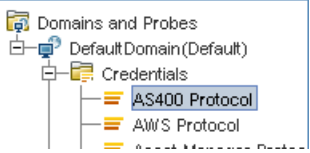
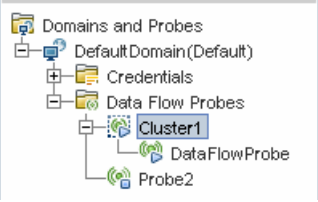
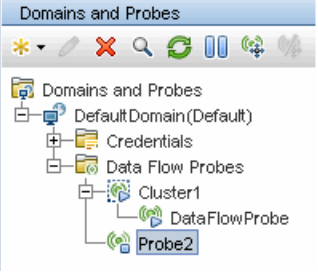
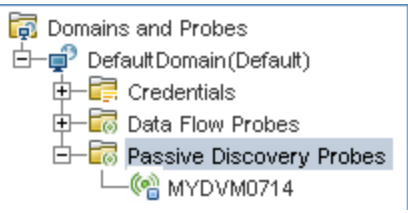
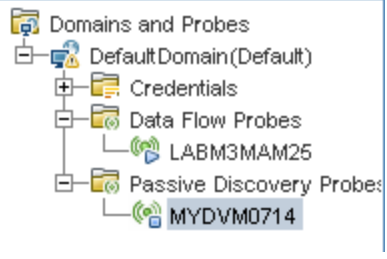
UI Element (A–Z)	Description
	<p>Probe/probe cluster from the UCMDB Server such it cannot run discovery and integration jobs.</p> <ul style="list-style-type: none"> • Resume Probe/Cluster. Resumes the Data Flow Probe/probe cluster's ability to run discovery and integration jobs. <p>Note: When a Data Flow Probe/probe cluster is suspended, only the ability to run jobs is suspended. All other processes continue to run as usual.</p> <p>The suspend feature is used to just create a job execution policy for a particular probe, and dispatch the policy to that particular probe. Once the job execution policy takes effect, all of the jobs dispatched to the particular probe are switched to the Total blackout state. It does not block the process of job dispatching from UCMDB server to the probe. The effect of the suspend feature equals to creating a job execution policy rule in the Domains and Probes Details pane directly.</p>
	<p>Deploy Probe Update. Opens the Deploy Probe Update dialog box, enabling you to automatically update the CUP version of all the Data Flow Probes connecting to the UCMDB Server to the CUP version compatible with the UCMDB CUP version.</p> <p>In the Deploy Probe Update dialog box, navigate to the Probe CUP .zip file.</p> <p>Note: During the CUP deployment process, all compatible Data Flow Probes are automatically restarted. If an integration is running on a Data Flow Probe while it is restarting, the integration stops running, and starts over when the Data Flow Probe restarts. If an integration is almost finished running, or a significant part has already run, to avoid starting the integration over, we recommend letting it complete its run, and, thereafter, updating the CUP.</p>
	<p>Undeploy Probe Update. Enables you to undeploy CUP versions of the Data Flow Probes connecting to the UCMDB Server, and thereby align them with the CUP version of the UCMDB Server.</p> <p>For details, see "How to Align the Data Flow Probe CUP with the UCMDB Server CUP" on page 77.</p>
<p><Domain and Probes tree></p>	<p>Displays the domains defined in the system, along with the credential per supported protocol and the probe clusters, Data Flow Probes, and passive discovery probes in each domain.</p> <p>Note: Integration Probes—that is Probes on Linux machines, and Windows Probes configured for integration only—are not displayed in the tree. To verify if an integration Probe is connected, create a dummy integration point</p>

UI Element (A-Z)	Description
	<p>and verify that the Probe is listed among the Probes that can be selected for the integration point. For details, see "How to Set Up an Integration Point" on page 324.</p>
<Credential status icons>	<p> . Indicates that an active discovery job or activity wants to connect using the protocol, but no protocol credential information is defined.</p>
<Data Flow Probe status icons>	<ul style="list-style-type: none">  . Indicates the Probe is connected.  . Indicates the Probe is suspended.  . Indicates the Probe is disconnected.
<Probe Cluster status icons>	<ul style="list-style-type: none">  . Indicates the probe cluster is connected.  . Indicates the probe cluster is suspended. <p>Note: A red exclamation mark on the cluster icon () indicates an warning or error that needs attention.</p>

Details pane

Displays details relevant to the node selected in the Domains and Probes tree.

Selected Node	Information Pane
<p>Domains and Probes</p> 	<p>Displays details of all the Data Flow Probes. You can also define and edit job execution policies.</p> <p>For details, see "Domains and Probes Details Pane" on page 110.</p>
<p>A specific domain</p> 	<p>Displays a list of probe clusters, Data Flow Probes, and passive discovery probes defined and running in the selected domain.</p> <p>You can add a description for the domain in this pane.</p> <p>For details, see "<Domain> Details Pane" on page 111.</p>
<p>A specific protocol</p>	<p>Displays the details on the protocol, including user credentials. You can add/edit protocol parameters in this pane.</p> <p>For details, see "<Protocol> Details Pane" on page 113.</p>

Selected Node	Information Pane
	<p>For a list of supported protocols, see the <i>Universal CMDB Discovery and Integrations Content Guide</i>.</p>
<p>A probe cluster</p> 	<p>Displays details of the selected probe cluster, including range information. You can also add ranges to, or exclude ranges from, the cluster.</p> <p>For details, see "Cluster Details Pane" on page 119.</p>
<p>A Data Flow Probe</p> 	<p>Displays the details of the Data Flow Probe, including range information. You can also add ranges to, or exclude ranges from, the Data Flow Probe.</p> <p>For details, see "Data Flow Probe Details Pane" on page 122.</p>
<p>Passive Discovery Probes</p> 	<p>You can view and globally configure notification types and verification policies for all passive discovery probes that integrate with the Data Flow Probes of the same domain.</p> <p>For details, see "Passive Discovery Probes Pane" on page 126.</p>
<p>A specific passive discovery probe</p> 	<p>Displays the details of a passive discovery probe, including the Data Flow Probe to which it connects, and its IP range information. You can also configure the IP ranges to be monitored by the passive probe, and you can remove a passive probe from the domain.</p> <p>For details, see "Passive Discovery Probe Details Pane" on page 128.</p>

Domains and Probes Details Pane

To access	Select Data Flow Probe Setup > Domains and Probes pane > Domains and Probes root node.
------------------	---

Domains and Probes Pane

Displays all of the Probes connected to the UCMDB Server.

User interface elements are described below:

UI Element (A–Z)	Description
IP	The main IP address with which the Probe communicates with the UCMDB server.
Last Access Time	The last time that the Probe requested tasks from the server.
Name	The name given the Probe when it was added to UCMDB.
Probe Version	The version of the Probe. If the version of the Probe is not compatible with the version of the UCMDB server, this is indicated. Moreover, if the incompatible Probe tries to connect to the UCMDB server, the server sends a shutdown instruction to the Probe. To ensure compatibility, you must update the Probe. For details, see "How to Deploy a Data Flow Probe CUP" on page 75 .
Status	<ul style="list-style-type: none">• Connected. The Probe is connected to the server (the Probe connects every few seconds).• Connected (suspended). The Probe is connected, but it is suspended such that no jobs can run on the Probe.• Disconnected. The Probe is not connected to the server.





Job Execution Policy Pane

Enables you to configure the periods of time when jobs should or should not run on selected Probes/clusters.

Important	<ul style="list-style-type: none">• The default job execution policy is Always. This policy allows all jobs to run on
------------------	--

information	<p>any Probe/cluster at any time.</p> <ul style="list-style-type: none"> Jobs that have a listening functionality—that is, they do not perform discovery, for example, they listen to SNMP traps—are not included in a policy.
See also	"Job Execution Policies" on page 36

User interface elements are described below:

UI Element (A–Z)	Description
	Move priority up/down. Move the priority for the policy up or down. Universal Discovery executes all the policies in the list with the first policy taking priority. If a job is included in two policies, only the first policy for that job is executed.
	New Policy. Opens the New Policy dialog box, enabling you to add a job execution policy.
	<p>Remove Policy. Removes the selected job execution policy.</p> <p>Note: If a job affected by the policy is active when the Remove command is executed, UCMDB removes the policy but any of the job's triggers that are currently running remain unaffected.</p>
	Edit Policy. Opens the Edit Policy dialog box, enabling you to edit the selected job execution policy.
Jobs	The jobs that are affected by the policy.
Probes	The Probes/clusters that are affected by the policy.
Time	The schedule of the policy.

<Domain> Details Pane

This pane displays the details of the selected domain and the probes defined in the domain.

To access	Select Data Flow Probe Setup > Domains and Probes pane > Domains and Probes root node > a domain.
------------------	--

Domain Details

User interface elements are described below:

UI Element (A–Z)	Description
Description	The description that was given to the domain when it was defined in UCMDB. Note: This field is editable.
Domain Type	<ul style="list-style-type: none"> • Customer. A private domain used for your site. You can define several domains and each domain can include multiple Probes. Each Probe can include IP ranges but the customer domain itself has no range definition. • External. Internet/public domain. A domain that is defined with a range. The external domain can contain only one Probe whose name equals the domain name. However, you can define several external domains in your system.

Data Flow Probes Details

Lists all of the probes in the selected domain.

User interface elements are described below:








UI Element (A–Z)	Description
IP	The main IP address with which the Probe communicates with the UCMDB server.
Last Access Time	The last time that the Probe requested tasks from the server.
Name	The name given the Probe when it was added to UCMDB.
Probe Version	The version of the Probe. If the version of the Probe is not compatible with the version of the UCMDB server, this is indicated. Moreover, if the incompatible Probe tries to connect to the UCMDB server, the server sends a shutdown instruction to the Probe. To ensure compatibility, you must update the Probe. For details, see "How to Deploy a Data Flow Probe CUP" on page 75 .
Status	<ul style="list-style-type: none"> • Connected. The Probe is connected to the server (the Probe connects every few seconds). • Connected (suspended). The Probe is connected, but it is suspended such that no jobs can run on the Probe. • Disconnected. The Probe is not connected to the server.



Passive Discovery Probes Details

For details, see ["Passive Discovery Probes Pane" on page 126](#).

<Protocol> Details Pane

Enables you to manage protocol connection credentials.




UI Element (A–Z)	Description
	Create New Connection Details. Opens the Protocol Parameters dialog box, enabling you to define a connection credential for the selected protocol type. For details, see "Protocol Parameter Dialog Box" on page 115 .
	Remove Connection Details. Removes the selected connection credential.
	Edit Connection Details. Opens the Protocol Parameters dialog box, enabling you to edit the selected connection credential. For details, see "Protocol Parameter Dialog Box" on page 115 .
	Copy/Move selected credential to another domain. Enables you to copy/move the selected credential to another domain in the Domains and Probes tree.
	Export Certificate for Manual Agent Deployment. Enables you to export the Universal Discovery Agent certificate when installing the Universal Discovery Agent manually. For details, see "How to Install the Universal Discovery Agent Manually" on page 174 . Available for: Universal Discovery Protocol only.
	Import DDMI Certificates. Opens the Universal Discovery Protocol Parameters dialog box, enabling you to import certificates during a migration from DDMI to Universal Discovery. For details on the dialog box, see "Protocol Parameter Dialog Box" on page 115 . For details on DDMI migration, see the <i>DDMI to Universal Discovery Migration Walkthrough Guide</i> . Available for: Universal Discovery Protocol only.
	Move entry up/Move entry down. Enables you to move credential connections up or down to set the order in which credential sets are attempted. UCMDDB tries to connect using all the credential sets in the list, with the first set taking priority.
<Protocol connection details grid>	Displays the connection credentials defined for the protocol type selected in the Domains and Probes tree on the left. The details displayed in this section vary from protocol type to protocol type. For details, see the relevant protocol information as described in the Supported Protocols section in the <i>Universal CMDB Discovery and Integrations Content Guide</i> .

UI Element (A–Z)	Description
	<p>All protocol credentials include the following parameters:</p> <ul style="list-style-type: none"> Index. Indicates the order in which credential instances are selected to make a connection attempt. The lower the index, the higher the priority. Default: Credentials are added with an auto-increasing index value. To update the index, use the arrows buttons ( ). Scope. To change the range that a protocol must discover or to select a Probe or probe cluster, click Edit. For details, see "Protocol Parameter Dialog Box" on the next page. Default: ALL User Label. Enables you to enter a label to help you identify the protocol credential when you use it later. Syntax: Maximum of 50 characters
<right-click menu>	<p>When you right-click connection credential, choose from the following options:</p> <ul style="list-style-type: none"> Edit. Enables you to enter protocol parameters, such as user name and password, that enable connection to an application on a remote machine. Edit using previous interface. Choose this option under any of the following circumstances: <ul style="list-style-type: none"> In a previous version of UCMDB, you added parameters to this protocol that do not exist in this version. Values in this version cannot be deleted. For example, in this version you cannot configure Generic DB (SQL) Protocol credentials with an empty port number. Select this option to open the previous Edit Protocol Parameter dialog box and delete the port number. Copy/Move to another domain. Enables you to copy/move the selected protocol credential to another domain in the Domains and Probes tree. Check credential. Opens the Check Credential dialog box, where you specify the host name or IP address (in IPv4/IPv6 format) of the remote machine on which the protocol must run, and specify a connection timeout (in milliseconds). <ul style="list-style-type: none"> If you enter an IP address, the system populates the Data Flow Probe field with the Probe whose ranges include the IP address. If the system cannot find a Probe associated with the IP address, you must select a Probe manually from the Data Flow Probe drop-down list. If you enter a host name, you must select a Probe in the Data Flow Probe drop-down list. The Probe tries to resolve the name to a valid IP address using the DNS server specified on the Probe. <p>The selected Probe attempts to connect to the remote machine within the</p>

UI Element (A–Z)	Description
	<p>specified timeout and returns an answer as to whether the connection succeeded or not. If the connection is not successful, click Details for a description of the error.</p> <ul style="list-style-type: none"> • Export public certificates. Opens the Export dialog box, enabling you to export the UD Agent certificate when deploying the UD Agent manually. For details, see "How to Install the Universal Discovery Agent Manually" on page 174. <p>Available for: Universal Discovery Protocol only.</p>
<right-click a column heading>	<p>Choose from the following options:</p> <ul style="list-style-type: none"> • Hide Column. Displayed when a column is shown. • Show All Columns. Displayed when a column is hidden. • Select Columns. Select to choose which columns to display or to change the display order of the columns. • Auto-resize Column. Select to change the column width to fit the contents.

Protocol Parameter Dialog Box

Displays the attributes that can be defined for a protocol.

To access	<p>Select Data Flow Probe Setup > Domains and Probes pane > Domains and Probes root node > a domain > Credentials > a protocol.</p> <p>In the right-hand pane:</p> <ul style="list-style-type: none"> • To add new connection details, click the Create new connection details for selected protocol type  button. • To remove an existing credential, click the Remove connection details for selected protocol type  button. • To edit an existing credential, click the Edit connection details for selected protocol type  button.
See also	<ul style="list-style-type: none"> • "Data Flow Probe Setup Window" on page 105 • "<Protocol> Details Pane" on page 113 • Supported Protocols in the <i>Universal CMDB Discovery and Integrations Content Guide</i>.

User interface elements are described below:



UI Element (A–Z)	Description
General	<ul style="list-style-type: none"> • Network Scope. Opens the Scope Definition dialog box enabling you to define the network scope for the credential. <ul style="list-style-type: none"> ◦ Selected Probes. Clicking the Edit button opens the Select Probes dialog box, where you select specific Probes/probe clusters whose IP range must be changed. ◦ Selected Ranges. <ul style="list-style-type: none"> • All. Discovery runs on all ranges in the domain (default). • Selected Range. Enables you to select a specific range on which to run discovery. You can also define ranges to exclude from the range. For more details, see "Ranges Pane" below. • User Label. The display name for the credential.
<Protocol attributes>	<p>Enables you to define/edit the protocol attributes for the credential. The fields displayed are based on the protocol selected.</p> <p>For details about the protocol attributes, see the section about the supported protocols in the <i>Universal CMDB Discovery and Integrations Content Guide</i>.</p>




Ranges Pane






Enables you to define network IP addresses on which a Probe/probe cluster must discover CIs.

Important Information	<ul style="list-style-type: none"> • This pane is disabled when the selected Probe is contained within a probe cluster because the Probe's range is dynamically determined by the load balancing mechanism of the probe cluster. • For details on searching for a specific range, see the Find Probe Range by IP button in "Data Flow Probe Setup Window" on page 105.
------------------------------	---

User interface elements are described below:

UI Element (A–Z)	Description
	New IP Range. Opens the New IP Range dialog box, enabling you to define a new IP range for the selected Probe/probe cluster. For details, see " New/Edit Range Dialog Box " on page 131.
	Delete IP Range. Select an IP range and click the button to delete a range from the list.

UI Element (A–Z)	Description
	<p>Note: You can also delete an excluded IP range.</p>
	<p>Edit IP Range. Opens the Edit IP Range dialog box, enabling you to edit the selected IP range for the selected Probe/probe cluster. For details, see "New/Edit Range Dialog Box" on page 131.</p> <p>Note: You can also edit an excluded IP range.</p>
	<p>Export Data To File. Enables you to export the defined ranges in the following formats:</p> <ul style="list-style-type: none">• Excel. The table data is formatted as an .xls (Excel) file that can be displayed in a spreadsheet.• PDF. The table data is exported in PDF format.• RTF. The table data is exported in Rich Text Format.• CSV. The table data is formatted as a comma-separated values (CSV) text file that can be displayed in a spreadsheet. <p>Note: For the CSV formatted table data to display correctly, the comma (,) must be defined as the list separator in your Windows Control Panel. In Linux, you can specify the list separator in the application that opens the CSV file.</p> • XML. The table data is formatted as an XML file that can be opened in a text or XML editor. <p>Tip: To extract HTML code from the report:</p> <ul style="list-style-type: none">• Save the file as HTML• Open the file in an HTML editor• Copy the relevant table into the target file <p>Note: Ranges in CIDR notation can also be exported.</p>
	<p>Import Ranges from CSV File. Opens the Import Ranges from File dialog box, enabling you to select a CSV file from which to import a set of ranges.</p> <p>Before importing ranges, verify that:</p> <ul style="list-style-type: none">• The imported file is a valid CSV file <p>The CSV file must be built using the following names for the column headings:</p> <ul style="list-style-type: none">◦ Range. The range to import. This can be an IP range (IPv4 only) or in CIDR notation (IPv4/IPv6).




UI Element (A-Z)	Description																																																																						
	<ul style="list-style-type: none"> Excluded Ranges. The IP ranges to exclude from the imported range. <p>Note: The excluded range must be defined in the same format (IPv4/IPv6) as the full range.</p> <p>Important: See example below:</p> <ul style="list-style-type: none"> When defining an excluded IP range, always include the full range in the Ranges column as well. When a range is defined in CIDR notation, the excluded ranges must be defined in the IP range format (<start_ip_address> – <end_ip_address>) Description. A description of the range Type. The range type: 1 = Client; 0 = Data Center <p>Example</p> <table border="1" data-bbox="418 898 1378 1241"> <thead> <tr> <th></th> <th>A</th> <th>B</th> <th>C</th> <th>D</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>Range</td> <td>Excluded Ranges</td> <td>Description</td> <td>Type</td> </tr> <tr> <td>2</td> <td>16.60.133.56-16.60.133.75</td> <td></td> <td>Include IPv4 Range</td> <td>1</td> </tr> <tr> <td>3</td> <td>16.60.133.56-16.60.133.75</td> <td>16.60.133.60-16.60.133.65</td> <td>Exclude IPv4 Range 1 from IP Range</td> <td></td> </tr> <tr> <td>4</td> <td>16.60.133.56-16.60.133.75</td> <td>16.60.133.70-16.60.133.70</td> <td>Exclude IPv4 Range 2 from IP Range</td> <td></td> </tr> <tr> <td>5</td> <td>16.60.134.56/29</td> <td></td> <td>Include IPv4 CIDR</td> <td>0</td> </tr> <tr> <td>6</td> <td>16.60.134.56/29</td> <td>16.60.134.56-16.60.134.59</td> <td>Exclude IPv4 Range 1 from CIDR</td> <td></td> </tr> <tr> <td>7</td> <td>16.60.134.56/29</td> <td>16.60.134.60-16.60.134.61</td> <td>Exclude IPv4 Range 2 from CIDR</td> <td></td> </tr> <tr> <td>8</td> <td>0:0:0:0:0:1037:f418/125</td> <td></td> <td>Include IPv6 CIDR</td> <td>0</td> </tr> <tr> <td>9</td> <td>0:0:0:0:0:1037:f418/125</td> <td>0:0:0:0:0:1037:f41b-0:0:0:0:0:1037:f41b</td> <td>Exclude IPv6 Range 1 from CIDR</td> <td></td> </tr> <tr> <td>10</td> <td>0:0:0:0:0:1037:f418/125</td> <td>0:0:0:0:0:1037:f41d-0:0:0:0:0:1037:f41d</td> <td>Exclude IPv6 Range 2 from CIDR</td> <td></td> </tr> <tr> <td>11</td> <td>0:0:0:0:0:1037:f440/122</td> <td></td> <td>Include IPv6 CIDR</td> <td>0</td> </tr> <tr> <td>12</td> <td>0:0:0:0:0:1037:f440/122</td> <td>0:0:0:0:0:1037:f447-0:0:0:0:0:1037:f477</td> <td>Exclude IPv6 Range 1 from CIDR</td> <td></td> </tr> <tr> <td>13</td> <td></td> <td></td> <td></td> <td></td> </tr> </tbody> </table>		A	B	C	D	1	Range	Excluded Ranges	Description	Type	2	16.60.133.56-16.60.133.75		Include IPv4 Range	1	3	16.60.133.56-16.60.133.75	16.60.133.60-16.60.133.65	Exclude IPv4 Range 1 from IP Range		4	16.60.133.56-16.60.133.75	16.60.133.70-16.60.133.70	Exclude IPv4 Range 2 from IP Range		5	16.60.134.56/29		Include IPv4 CIDR	0	6	16.60.134.56/29	16.60.134.56-16.60.134.59	Exclude IPv4 Range 1 from CIDR		7	16.60.134.56/29	16.60.134.60-16.60.134.61	Exclude IPv4 Range 2 from CIDR		8	0:0:0:0:0:1037:f418/125		Include IPv6 CIDR	0	9	0:0:0:0:0:1037:f418/125	0:0:0:0:0:1037:f41b-0:0:0:0:0:1037:f41b	Exclude IPv6 Range 1 from CIDR		10	0:0:0:0:0:1037:f418/125	0:0:0:0:0:1037:f41d-0:0:0:0:0:1037:f41d	Exclude IPv6 Range 2 from CIDR		11	0:0:0:0:0:1037:f440/122		Include IPv6 CIDR	0	12	0:0:0:0:0:1037:f440/122	0:0:0:0:0:1037:f447-0:0:0:0:0:1037:f477	Exclude IPv6 Range 1 from CIDR		13				
	A	B	C	D																																																																			
1	Range	Excluded Ranges	Description	Type																																																																			
2	16.60.133.56-16.60.133.75		Include IPv4 Range	1																																																																			
3	16.60.133.56-16.60.133.75	16.60.133.60-16.60.133.65	Exclude IPv4 Range 1 from IP Range																																																																				
4	16.60.133.56-16.60.133.75	16.60.133.70-16.60.133.70	Exclude IPv4 Range 2 from IP Range																																																																				
5	16.60.134.56/29		Include IPv4 CIDR	0																																																																			
6	16.60.134.56/29	16.60.134.56-16.60.134.59	Exclude IPv4 Range 1 from CIDR																																																																				
7	16.60.134.56/29	16.60.134.60-16.60.134.61	Exclude IPv4 Range 2 from CIDR																																																																				
8	0:0:0:0:0:1037:f418/125		Include IPv6 CIDR	0																																																																			
9	0:0:0:0:0:1037:f418/125	0:0:0:0:0:1037:f41b-0:0:0:0:0:1037:f41b	Exclude IPv6 Range 1 from CIDR																																																																				
10	0:0:0:0:0:1037:f418/125	0:0:0:0:0:1037:f41d-0:0:0:0:0:1037:f41d	Exclude IPv6 Range 2 from CIDR																																																																				
11	0:0:0:0:0:1037:f440/122		Include IPv6 CIDR	0																																																																			
12	0:0:0:0:0:1037:f440/122	0:0:0:0:0:1037:f447-0:0:0:0:0:1037:f477	Exclude IPv6 Range 1 from CIDR																																																																				
13																																																																							
	<p>Expand All. Expands the entire hierarchical tree structure to display all of the defined IP ranges, including the excluded IP ranges.</p>																																																																						
	<p>Collapse All. Collapses the hierarchical tree structure, leaving the top-level IP ranges showing, but hiding excluded IP ranges.</p>																																																																						
	<p>Show/Hide Legend. Shows/Hides the legend for the Ranges pane.</p> <ul style="list-style-type: none"> . Denotes the range of IP addresses included for the selected Probe/probe cluster. . Denotes a range of IP addresses to exclude from the defined IP range. 																																																																						
<p><Ranges grid></p>	<p>The network range where the Probe/probe cluster discovers CIs. For details, see "New/Edit Range Dialog Box" on page 131.</p>																																																																						

Cluster Details Pane

Enables you to view the details of the probe cluster selected in the Domains and Probes tree.

To access	Select Data Flow Probe Setup > Domains and Probes pane > Domains and Probes root node > a domain > Data Flow Probes > a cluster.
Relevant task	<ul style="list-style-type: none"> • "How to Add Probe Clusters to UCMDB" on page 55 • "How to Limit IP Movement in a Cluster" on page 63
See also	<ul style="list-style-type: none"> • "Data Flow Probes and Probe Clusters" on page 30 • "Cluster Range Distribution Policy" on page 31 • "Limiting IP Movement in a Cluster" on page 34

User interface elements are described below:

UI Element	Description
Cluster Description pane	The description of the selected cluster.
Associated Probes pane	<p>Enables you to manage Data Flow Probes associated with the cluster.</p> <ul style="list-style-type: none"> • Add Probe to Cluster . Enables you to add Data Flow Probes to the cluster. • Remove Probe from Cluster . Removes the selected Data Flow Probe from the cluster. <p>Note:</p> <ul style="list-style-type: none"> ◦ A Probe that is removed from a cluster has no network range. To define a range for the Probe, see "New/Edit Range Dialog Box" on page 131. ◦ If you add a Probe to a cluster and remove the Probe before saving the cluster then: <ul style="list-style-type: none"> • if changes were made to the Probe's range after adding the Probe, the range remains with the cluster • if no changes were made to the Probe's range after adding the Probe, the range remains with the Probe <ul style="list-style-type: none"> • View Constraint . Opens the Trigger Query Editor dialog box and displays the defined TQL constraints for the selected Probe. • Set TQL Constraint. Opens the Choose Discovery Query dialog box, enabling you select a constraint query for the Probe. When the cluster distributes its





UI Element	Description
	network range among its Probes, it takes into account the constraints defined on the Probes.


Ranges Pane






Enables you to define network ranges over which the Data Flow Probes in the cluster should perform discovery.

Important Information	<ul style="list-style-type: none"> For details on searching for a specific range, see the Find Probe Range by IP button in "Data Flow Probe Setup Window" on page 105. When a specific Probe in a cluster is selected, its range is displayed but is not editable.
------------------------------	---

User interface elements are described below:

UI Element	Description
	New Range. Opens the New Range dialog box, enabling you to define a new network range for the selected probe cluster. For details, see " New/Edit Range Dialog Box " on page 131.
	Delete Range. Enables you to delete the selected range. Note: You can also delete an excluded IP range.
	Edit Range. Opens the Edit Range dialog box, enabling you to edit the selected range for the probe cluster. For details, see " New/Edit Range Dialog Box " on page 131. Note: You can also edit an excluded IP range.
	Export Data To File. Enables you to export the defined ranges in the following formats: <ul style="list-style-type: none"> Excel. The table data is formatted as an .xls (Excel) file that can be displayed in a spreadsheet. PDF. The table data is exported in PDF format. RTF. The table data is exported in Rich Text Format. CSV. The table data is formatted as a comma-separated values (CSV) text file that can be displayed in a spreadsheet. Note: For the CSV formatted table data to display correctly, the comma (,) must be defined as the list separator. In Windows, to verify or modify the list separator

UI Element	Description
	<p>value, open Regional Options from the Control Panel, and on the Numbers tab ensure that the comma is defined as the List Separator value. In Linux, you can specify the list separator in the application that opens the CSV file.</p> <ul style="list-style-type: none"> • XML. The table data is formatted as an XML file that can be opened in a text or XML editor. <p>Tip: To extract HTML code from the report:</p> <ul style="list-style-type: none"> ◦ Save the file as HTML ◦ Open the file in an HTML editor ◦ Copy the relevant table into the target file <p>Note: Ranges in CIDR notation can also be exported.</p>
	<p>Import Ranges from CSV File. Opens the Import Ranges from File dialog box, enabling you to select a CSV file from which to import a set of ranges.</p> <p>Before importing ranges, verify that:</p> <ul style="list-style-type: none"> • The imported file is a valid CSV file <p>The CSV file must be built using the following names for the column headings:</p> <ul style="list-style-type: none"> ◦ Range. The range to import. This can be an IP range (IPv4 only) or in CIDR notation (IPv4/IPv6). ◦ Excluded Ranges. The IP ranges to exclude from the imported range. <p>Note: The excluded range must be defined in the same format (IPv4/IPv6) as the full range.</p> <p>Important: See example below:</p> <ul style="list-style-type: none"> • When defining an excluded IP range, always include the full range in the Ranges column as well. • When a range is defined in CIDR notation, the excluded ranges must be defined in the IP range format (<start_ip_address> – <end_ip_address>) ◦ Description. A description of the range ◦ Type. The range type: 1 = Client; 0 = Data Center <p>Example</p>

UI Element	Description																																																																						
	<table border="1"> <thead> <tr> <th></th> <th>A</th> <th>B</th> <th>C</th> <th>D</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>Range</td> <td>Excluded Ranges</td> <td>Description</td> <td>Type</td> </tr> <tr> <td>2</td> <td>16.60.133.56-16.60.133.75</td> <td></td> <td>Include IPv4 Range</td> <td>1</td> </tr> <tr> <td>3</td> <td>16.60.133.56-16.60.133.75</td> <td>16.60.133.60-16.60.133.65</td> <td>Exclude IPv4 Range 1 from IP Range</td> <td></td> </tr> <tr> <td>4</td> <td>16.60.133.56-16.60.133.75</td> <td>16.60.133.70-16.60.133.70</td> <td>Exclude IPv4 Range 2 from IP Range</td> <td></td> </tr> <tr> <td>5</td> <td>16.60.134.56/29</td> <td></td> <td>Include IPv4 CIDR</td> <td>0</td> </tr> <tr> <td>6</td> <td>16.60.134.56/29</td> <td>16.60.134.56-16.60.134.59</td> <td>Exclude IPv4 Range 1 from CIDR</td> <td></td> </tr> <tr> <td>7</td> <td>16.60.134.56/29</td> <td>16.60.134.60-16.60.134.61</td> <td>Exclude IPv4 Range 2 from CIDR</td> <td></td> </tr> <tr> <td>8</td> <td>0:0:0:0:0:1037:f418/125</td> <td></td> <td>Include IPv6 CIDR</td> <td>0</td> </tr> <tr> <td>9</td> <td>0:0:0:0:0:1037:f418/125</td> <td>0:0:0:0:0:1037:f41b-0:0:0:0:0:1037:f41b</td> <td>Exclude IPv6 Range 1 from CIDR</td> <td></td> </tr> <tr> <td>10</td> <td>0:0:0:0:0:1037:f418/125</td> <td>0:0:0:0:0:1037:f41d-0:0:0:0:0:1037:f41d</td> <td>Exclude IPv6 Range 2 from CIDR</td> <td></td> </tr> <tr> <td>11</td> <td>0:0:0:0:0:1037:f440/122</td> <td></td> <td>Include IPv6 CIDR</td> <td>0</td> </tr> <tr> <td>12</td> <td>0:0:0:0:0:1037:f440/122</td> <td>0:0:0:0:0:1037:f447-0:0:0:0:0:1037:f477</td> <td>Exclude IPv6 Range 1 from CIDR</td> <td></td> </tr> <tr> <td>13</td> <td></td> <td></td> <td></td> <td></td> </tr> </tbody> </table>		A	B	C	D	1	Range	Excluded Ranges	Description	Type	2	16.60.133.56-16.60.133.75		Include IPv4 Range	1	3	16.60.133.56-16.60.133.75	16.60.133.60-16.60.133.65	Exclude IPv4 Range 1 from IP Range		4	16.60.133.56-16.60.133.75	16.60.133.70-16.60.133.70	Exclude IPv4 Range 2 from IP Range		5	16.60.134.56/29		Include IPv4 CIDR	0	6	16.60.134.56/29	16.60.134.56-16.60.134.59	Exclude IPv4 Range 1 from CIDR		7	16.60.134.56/29	16.60.134.60-16.60.134.61	Exclude IPv4 Range 2 from CIDR		8	0:0:0:0:0:1037:f418/125		Include IPv6 CIDR	0	9	0:0:0:0:0:1037:f418/125	0:0:0:0:0:1037:f41b-0:0:0:0:0:1037:f41b	Exclude IPv6 Range 1 from CIDR		10	0:0:0:0:0:1037:f418/125	0:0:0:0:0:1037:f41d-0:0:0:0:0:1037:f41d	Exclude IPv6 Range 2 from CIDR		11	0:0:0:0:0:1037:f440/122		Include IPv6 CIDR	0	12	0:0:0:0:0:1037:f440/122	0:0:0:0:0:1037:f447-0:0:0:0:0:1037:f477	Exclude IPv6 Range 1 from CIDR		13				
	A	B	C	D																																																																			
1	Range	Excluded Ranges	Description	Type																																																																			
2	16.60.133.56-16.60.133.75		Include IPv4 Range	1																																																																			
3	16.60.133.56-16.60.133.75	16.60.133.60-16.60.133.65	Exclude IPv4 Range 1 from IP Range																																																																				
4	16.60.133.56-16.60.133.75	16.60.133.70-16.60.133.70	Exclude IPv4 Range 2 from IP Range																																																																				
5	16.60.134.56/29		Include IPv4 CIDR	0																																																																			
6	16.60.134.56/29	16.60.134.56-16.60.134.59	Exclude IPv4 Range 1 from CIDR																																																																				
7	16.60.134.56/29	16.60.134.60-16.60.134.61	Exclude IPv4 Range 2 from CIDR																																																																				
8	0:0:0:0:0:1037:f418/125		Include IPv6 CIDR	0																																																																			
9	0:0:0:0:0:1037:f418/125	0:0:0:0:0:1037:f41b-0:0:0:0:0:1037:f41b	Exclude IPv6 Range 1 from CIDR																																																																				
10	0:0:0:0:0:1037:f418/125	0:0:0:0:0:1037:f41d-0:0:0:0:0:1037:f41d	Exclude IPv6 Range 2 from CIDR																																																																				
11	0:0:0:0:0:1037:f440/122		Include IPv6 CIDR	0																																																																			
12	0:0:0:0:0:1037:f440/122	0:0:0:0:0:1037:f447-0:0:0:0:0:1037:f477	Exclude IPv6 Range 1 from CIDR																																																																				
13																																																																							
	Expand All. Expands the entire hierarchical tree structure to display all of the defined IP ranges, including the excluded IP ranges.																																																																						
	Collapse All. Collapses the hierarchical tree structure, leaving the top-level IP ranges showing, but hiding excluded IP ranges.																																																																						
	<p>Show/Hide Legend. Shows/Hides the legend for the Ranges pane.</p> <ul style="list-style-type: none"> . Denotes the range of IP addresses included for the selected Probe. . Denotes a range of IP addresses to exclude from the defined IP range. 																																																																						
<Ranges grid>	Lists the network ranges where the Data Flow Probes in the cluster perform discovery. For details, see "New/Edit Range Dialog Box" on page 131 .																																																																						

Data Flow Probe Details Pane

To access	Select Data Flow Probe Setup > Domains and Probes pane > Domains and Probes root node > a domain > Data Flow Probes > a Data Flow Probe.
Relevant tasks	"How to Add Data Flow Probes to UCMDB" on page 54
See also	"Data Flow Probe Status" on page 147

Probe Details Pane

Displays the details of the selected Data Flow Probe.

User interface elements are described below:

UI Element (A–Z)	Description
Default Tenant	<p>Displays the default tenant for the Data Flow Probe.</p> <p>Note: When working in multi-tenancy mode, the best practice is for all Data Flow Probes in a probe cluster to have the same default tenant defined for them. If Data Flow Probes have different default tenants and a re-distribution of the ranges occurs, the tenant of the already discovered CIs is not changed.</p> <p>Available: In multi-tenancy environments only.</p>
Last time probe accessed UCMDB	<p>The last time that the Probe accessed the server machine.</p>
Probe Description	<p>The description given to the Probe when it was added to UCMDB.</p> <p>Note: This field is editable.</p>
Probe IPs	<p>The IPs of the Probe machine.</p> <p>Note: If the Probe machine has more than one network card, all the IP addresses are displayed.</p>
Status	<p>The status of the selected Probe:</p> <ul style="list-style-type: none"> • Connected. The Probe has successfully connected to the server. (The Probe connects every few seconds.) • Disconnected (being restarted). The Probe gateway service is restarting. This may be because, for example, the Probe has downloaded a Content Pack Update, or detected a job that is stuck. • Disconnected (stopped). The Probe gateway service is stopped by the server administrator. • Disconnected (reason unknown). The Probe gateway service is stopped for some other reason. <p>Note: When the Probe is suspended, (suspended) is also displayed together with the status.</p>
Version	<p>The version of the Probe.</p> <p>Note: If the version of the Probe is not compatible with the version of the UCMDB server, this is indicated. Moreover, if the incompatible Probe tries to connect to the UCMDB server, the server sends a shutdown instruction to the</p>





UI Element (A–Z)	Description
	<p>Probe. To ensure compatibility:</p> <ul style="list-style-type: none"> • If the Probe version is correct but the CUP version is not aligned with the UCMDB Server CUP version, see "How to Align the Data Flow Probe CUP with the UCMDB Server CUP" on page 77. • If the Probe is an old version, you need to uninstall the Probe, and reinstall the correct version. For details, see the interactive <i>Universal CMDB Deployment Guide</i>.


Ranges Pane






Enables you to define network IP addresses on which a Probe must discover CIs.

<p>Important Information</p>	<ul style="list-style-type: none"> • This pane is read-only when the Probe is associated with a probe cluster because the Probe's range is dynamically determined by the load balancing mechanism of the probe cluster. • For details on searching for a specific range, see the Find Probe Range by IP button in "Data Flow Probe Setup Window" on page 105.
-------------------------------------	--

User interface elements are described below:

UI Element (A–Z)	Description
	<p>New IP Range. Opens the New IP Range dialog box, enabling you to define a new IP range for the selected Probe. For details, see "New/Edit Range Dialog Box" on page 131.</p>
	<p>Delete IP Range. Select an IP range and click the button to delete a range from the list.</p> <p>Note: You can also delete an excluded IP range.</p>
	<p>Edit IP Range. Opens the Edit IP Range dialog box, enabling you to edit the selected IP range for the selected Probe. For details, see "New/Edit Range Dialog Box" on page 131.</p> <p>Note: You can also edit an excluded IP range.</p>
	<p>Export Data To File. Enables you to export the defined ranges in the following formats:</p> <ul style="list-style-type: none"> • Excel. The table data is formatted as an .xls (Excel) file that can be displayed in a

UI Element (A–Z)	Description
	<p>spreadsheet.</p> <ul style="list-style-type: none">• PDF. The table data is exported in PDF format.• RTF. The table data is exported in Rich Text Format.• CSV. The table data is formatted as a comma-separated values (CSV) text file that can be displayed in a spreadsheet. <p>Note: For the CSV formatted table data to display correctly, the comma (,) must be defined as the list separator. In Windows, to verify or modify the list separator value, open Regional Options from the Control Panel, and on the Numbers tab ensure that the comma is defined as the List Separator value. In Linux, you can specify the list separator in the application that opens the CSV file.</p> <ul style="list-style-type: none">• XML. The table data is formatted as an XML file that can be opened in a text or XML editor. <p>Tip: To extract HTML code from the report:</p> <ul style="list-style-type: none">• Save the file as HTML• Open the file in an HTML editor• Copy the relevant table into the target file <p>Note: Ranges in CIDR notation can also be exported.</p>
	<p>Import Ranges from CSV File. Opens the Import Ranges from File dialog box, enabling you to select a CSV file from which to import a set of ranges.</p> <p>Before importing ranges, verify that:</p> <ul style="list-style-type: none">• The imported file is a valid CSV file <p>The CSV file must be built using the following names for the column headings:</p> <ul style="list-style-type: none">◦ Range. The range to import. This can be an IP range (IPv4 only) or in CIDR notation (IPv4/IPv6).◦ Excluded Ranges. The IP ranges to exclude from the imported range. <p>Note: The excluded range must be defined in the same format (IPv4/IPv6) as the full range.</p> <p>Important: See example below:</p> <ul style="list-style-type: none">• When defining an excluded IP range, always include the full range in the Ranges column as well.

UI Element (A-Z)	Description																																																																						
	<ul style="list-style-type: none"> When a range is defined in CIDR notation, the excluded ranges must be defined in the IP range format (<start_ip_address> – <end_ip_address>) Description. A description of the range Type. The range type: 1 = Client; 0 = Data Center <p>Example</p> <table border="1"> <thead> <tr> <th></th> <th>A</th> <th>B</th> <th>C</th> <th>D</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>Range</td> <td>Excluded Ranges</td> <td>Description</td> <td>Type</td> </tr> <tr> <td>2</td> <td>16.60.133.56-16.60.133.75</td> <td></td> <td>Include IPv4 Range</td> <td>1</td> </tr> <tr> <td>3</td> <td>16.60.133.56-16.60.133.75</td> <td>16.60.133.60-16.60.133.65</td> <td>Exclude IPv4 Range 1 from IP Range</td> <td></td> </tr> <tr> <td>4</td> <td>16.60.133.56-16.60.133.75</td> <td>16.60.133.70-16.60.133.70</td> <td>Exclude IPv4 Range 2 from IP Range</td> <td></td> </tr> <tr> <td>5</td> <td>16.60.134.56/29</td> <td></td> <td>Include IPv4 CIDR</td> <td>0</td> </tr> <tr> <td>6</td> <td>16.60.134.56/29</td> <td>16.60.134.56-16.60.134.59</td> <td>Exclude IPv4 Range 1 from CIDR</td> <td></td> </tr> <tr> <td>7</td> <td>16.60.134.56/29</td> <td>16.60.134.60-16.60.134.61</td> <td>Exclude IPv4 Range 2 from CIDR</td> <td></td> </tr> <tr> <td>8</td> <td>0:0:0:0:0:1037:f418/125</td> <td></td> <td>Include IPv6 CIDR</td> <td>0</td> </tr> <tr> <td>9</td> <td>0:0:0:0:0:1037:f418/125</td> <td>0:0:0:0:0:1037:f41b-0:0:0:0:0:1037:f41b</td> <td>Exclude IPv6 Range 1 from CIDR</td> <td></td> </tr> <tr> <td>10</td> <td>0:0:0:0:0:1037:f418/125</td> <td>0:0:0:0:0:1037:f41d-0:0:0:0:0:1037:f41d</td> <td>Exclude IPv6 Range 2 from CIDR</td> <td></td> </tr> <tr> <td>11</td> <td>0:0:0:0:0:1037:f440/122</td> <td></td> <td>Include IPv6 CIDR</td> <td>0</td> </tr> <tr> <td>12</td> <td>0:0:0:0:0:1037:f440/122</td> <td>0:0:0:0:0:1037:f447-0:0:0:0:0:1037:f477</td> <td>Exclude IPv6 Range 1 from CIDR</td> <td></td> </tr> <tr> <td>13</td> <td></td> <td></td> <td></td> <td></td> </tr> </tbody> </table>		A	B	C	D	1	Range	Excluded Ranges	Description	Type	2	16.60.133.56-16.60.133.75		Include IPv4 Range	1	3	16.60.133.56-16.60.133.75	16.60.133.60-16.60.133.65	Exclude IPv4 Range 1 from IP Range		4	16.60.133.56-16.60.133.75	16.60.133.70-16.60.133.70	Exclude IPv4 Range 2 from IP Range		5	16.60.134.56/29		Include IPv4 CIDR	0	6	16.60.134.56/29	16.60.134.56-16.60.134.59	Exclude IPv4 Range 1 from CIDR		7	16.60.134.56/29	16.60.134.60-16.60.134.61	Exclude IPv4 Range 2 from CIDR		8	0:0:0:0:0:1037:f418/125		Include IPv6 CIDR	0	9	0:0:0:0:0:1037:f418/125	0:0:0:0:0:1037:f41b-0:0:0:0:0:1037:f41b	Exclude IPv6 Range 1 from CIDR		10	0:0:0:0:0:1037:f418/125	0:0:0:0:0:1037:f41d-0:0:0:0:0:1037:f41d	Exclude IPv6 Range 2 from CIDR		11	0:0:0:0:0:1037:f440/122		Include IPv6 CIDR	0	12	0:0:0:0:0:1037:f440/122	0:0:0:0:0:1037:f447-0:0:0:0:0:1037:f477	Exclude IPv6 Range 1 from CIDR		13				
	A	B	C	D																																																																			
1	Range	Excluded Ranges	Description	Type																																																																			
2	16.60.133.56-16.60.133.75		Include IPv4 Range	1																																																																			
3	16.60.133.56-16.60.133.75	16.60.133.60-16.60.133.65	Exclude IPv4 Range 1 from IP Range																																																																				
4	16.60.133.56-16.60.133.75	16.60.133.70-16.60.133.70	Exclude IPv4 Range 2 from IP Range																																																																				
5	16.60.134.56/29		Include IPv4 CIDR	0																																																																			
6	16.60.134.56/29	16.60.134.56-16.60.134.59	Exclude IPv4 Range 1 from CIDR																																																																				
7	16.60.134.56/29	16.60.134.60-16.60.134.61	Exclude IPv4 Range 2 from CIDR																																																																				
8	0:0:0:0:0:1037:f418/125		Include IPv6 CIDR	0																																																																			
9	0:0:0:0:0:1037:f418/125	0:0:0:0:0:1037:f41b-0:0:0:0:0:1037:f41b	Exclude IPv6 Range 1 from CIDR																																																																				
10	0:0:0:0:0:1037:f418/125	0:0:0:0:0:1037:f41d-0:0:0:0:0:1037:f41d	Exclude IPv6 Range 2 from CIDR																																																																				
11	0:0:0:0:0:1037:f440/122		Include IPv6 CIDR	0																																																																			
12	0:0:0:0:0:1037:f440/122	0:0:0:0:0:1037:f447-0:0:0:0:0:1037:f477	Exclude IPv6 Range 1 from CIDR																																																																				
13																																																																							
	Expand All. Expands the entire hierarchical tree structure to display all of the defined IP ranges, including the excluded IP ranges.																																																																						
	Collapse All. Collapses the hierarchical tree structure, leaving the top-level IP ranges showing, but hiding excluded IP ranges.																																																																						
	<p>Show/Hide Legend. Shows/Hides the legend for the Ranges pane.</p> <ul style="list-style-type: none"> . Denotes the range of IP addresses included for the selected Probe. . Denotes a range of IP addresses to exclude from the defined IP range. 																																																																						
<Ranges grid>	The network range where the Probe discovers CIs. For details, see "New/Edit Range Dialog Box" on page 131 .																																																																						

Passive Discovery Probes Pane

This pane enables you to globally configure notification types for all passive discovery probes that integrate with the Data Flow Probes of the same domain. The passive discovery probes notify UCMDB of changes in traffic, such as an unseen IP address or software not running.

To access	Select Data Flow Management > Data Flow Probe Setup > Domains and Probes pane > a domain > Passive Discovery Probes .
Important	The definitions defined here are valid for all of the passive discovery probes that

information	integrate with the Data Flow Probes of the same domain.
Relevant task	"How to Configure Just-In-Time Discovery" on page 655
See also	<ul style="list-style-type: none"> • "Just-In-Time Discovery Overview" on page 655 • "Data Flow Probe Setup Window" on page 105 • "Passive Discovery Probe Details Pane" on the next page

Notification Types Pane

Note: By default all types of notifications are enabled.

User interface elements are described below :

UI Element	Description
Report IP notifications	<ul style="list-style-type: none"> • Reports new IP addresses seen on the network. • Reports unseen IP addresses. <ul style="list-style-type: none"> ◦ Select the amount of time that the passive probe should wait before triggering a notification that the IP address was not seen. ◦ After this notification is sent, the Data Flow Probe performs a verification. Select an action that should be taken upon verification: <ul style="list-style-type: none"> • set the IP address as a candidate for deletion • remove the IP address from UCMDB
Report running software notifications	<ul style="list-style-type: none"> • Reports new running software seen on the network • Reports unseen running software. <ul style="list-style-type: none"> ◦ Select the amount of time that the passive probe should wait before triggering a notification that the software is not running. ◦ After this notification is sent, the Data Flow Probe performs a verification. Select an action that should be taken upon verification: <ul style="list-style-type: none"> • set the RunningSoftware CI as a candidate for deletion • remove the RunningSoftware CI from UCMDB
Report dependency link notifications	Enables notification of dependency relationships.

Removal Verification Policy Pane

User interface elements are described below:

UI Element	Description
Verify ports by scanning	Enables verification of listening ports by scanning.
Ping configuration for verification process	Enables you to specify the number and frequency of pings to verify unseen IP addresses before removal, as well as the overall number of simultaneous pings allowed.

Passive Probes Pane

Lists the passive discovery probes that are connected to Data Flow Probes.

User interface elements are described below:

UI Element (A - Z)	Description
Data Flow Probe	The name of the Data Flow Probe to which the passive discovery probe reports.
IP Address	The IP address of the passive discovery probe (RUM Engine) machine.
Last access time	The date and time the passive discovery probe was last accessed.
Name	The name given to the passive discovery probe (RUM Engine) when it was defined in RUM.
Status	Indicates the status of the passive discovery probe: <ul style="list-style-type: none"> • Connected. The passive discovery probe is connected and available to report information to the Data Flow Probe. • Suspended. The passive discovery probe is connected but not available to report information to the Data Flow Probe. • Disconnected. The passive discovery probe is not connected.
Version	The RUM version.

Passive Discovery Probe Details Pane

This pane enables you to configure the passive discovery probes (Micro Focus RUM Engines) to monitor the IP address ranges and ports that you specify.

To access	Select Data Flow Management > Data Flow Probe Setup > Domains and Probes pane > a domain > Passive Discovery Probes > a passive probe.
------------------	--

Important information	The passive discovery probes can be configured to monitor the IP address ranges in the domain of the Data Flow Probe only.
Relevant task	"How to Configure Just-In-Time Discovery" on page 655
See also	<ul style="list-style-type: none"> • "Just-In-Time Discovery Overview" on page 655 • "Passive Discovery Probes Pane" on page 126 • "Data Flow Probe Setup Window" on page 105

Passive Discovery Probe Details Pane

User interface elements are described below :

UI Element	Description
Name	The name given to the passive discovery probe (RUM Engine) when it was defined in RUM.
Data Flow Probe	The name of the Data Flow Probe to which the passive discovery probe reports.
IP	The IP address of the passive discovery probe (RUM Engine) machine.
Version	The RUM version.
Status	Indicates the status of the passive discovery probe: <ul style="list-style-type: none"> • Connected. The passive discovery probe is connected and available to report information to the Data Flow Probe. • Suspended. The passive discovery probe is connected but unavailable to report information to the Data Flow Probe. • Disconnected. The passive discovery probe is not connected.
Last access time	The date and time the passive discovery probe was last accessed.

Passive Discovery Ranges Pane

This pane lists the RUM Probes that report to the RUM Engine. This information is obtained from the RUM Server.


User interface elements are described below :

UI Element	Description
Passive	The name of the RUM Probe.

UI Element	Description
Discovery Agent Name	
Range	<p>The IP address range defined for the RUM Probe. Information from within this range is reported to the RUM Engine (passive discovery probe).</p> <p>Note: The range can be displayed here either according to the IP range format or the CIDR notation, as explained in "New/Edit Range Dialog Box" on the next page.</p>
Ports	The ports defined for the RUM Probe over which information is reported.












Passive Discovery Integrated Ranges Pane

User interface elements are described below :

UI Element	Description
Use All Ranges Of Data Flow Probe <Data Flow Probe name>	<p>Enables passive discovery over all address ranges of the connected Data Flow Probe, over selected ports:</p> <ul style="list-style-type: none"> • All available ports. Enables passive discovery over all available ports. • Selected ports Enables passive discovery over ports that you select from the Global Ports List. Click  to select ports to monitor.
Use Selected Ranges Of Data Flow Probe <Data Flow Probe name>	<p>Enables passive discovery over the Ranges Definition area where you can select existing Data Flow Probe ranges over which to perform passive discovery. See below.</p> <p>Note:</p> <ul style="list-style-type: none"> • Ranges must be a subset of both the connected Data Flow Probe's ranges and Passive Discovery ranges. • Ranges can be displayed here either according to the IP range format or the CIDR format, as explained in "New/Edit Range Dialog Box" on the next page.





Ranges Definition Area

User interface elements are described below :

UI Element (A–Z)	Description
	<p>New Range. Enables you to define a new range for the passive discovery probe to monitor.</p> <p>Note: This range must be a subset of one of the Data Flow Probe's ranges. For details about defining Probe ranges, see "New/Edit Range Dialog Box" below.</p>
	<p>Delete Range. Enables you to remove a range defined for passive discovery.</p>
	<p>Select Range Enables you to select defined ranges for the passive discovery probe to monitor from the ranges defined for the connected Data Flow Probe.</p>
	<p>Edit Range. Enables you to modify a selected range.</p> <p>For example, you can select one of the Data Flow Probes ranges, and then exclude some IP addresses from that range for passive discovery.</p>
	<p>Export Data To File.</p> <p>Note: Not enabled for passive discovery probes.</p>
	<p>Import Ranges from CSV File.</p> <p>Note: Not enabled for passive discovery probes.</p>
	<p>Expand All. Expands the hierarchical tree structure to display all of the defined ranges, including the excluded IP ranges.</p>
	<p>Collapse All. Collapses the hierarchical tree structure, hiding excluded IP ranges.</p>
	<p>Show/Hide Legend. Shows/Hides the legend for the Ranges pane.</p> <ul style="list-style-type: none"> . Denotes a range included for the selected passive discovery probe. . Denotes an IP range to exclude from the parent range.
<Ranges grid>	<p>Lists the ranges and ports selected for the passive discovery probe to monitor.</p>

New/Edit Range Dialog Box

Enables you to set network ranges for Data Flow Probes, a probe clusters, or passive discovery probes. The results are retrieved from the addresses in the range you define. You can also define IP addresses that must be excluded from a range.




To access	<p>Select Data Flow Management > Data Flow Probe Setup > Domains and Probes > <Domain>.</p> <ul style="list-style-type: none"> • Data Flow Probes/Clusters: Select Data Flow Probes > a probe/cluster, and in the Ranges pane click the New Range  or Edit Range  button. • Passive discovery probes: Select Passive Discovery Probes > a passive probe, and in the Passive Discovery Integrated Ranges pane click the New Range  or Edit Range  button.
Important information	<ul style="list-style-type: none"> • An IP address can belong to only one probe or probe cluster's range in the same domain. That is, two Probes in the same domain cannot have the same IP address in their ranges. • For a passive discovery probe, the range must fall within the range of the Data Flow Probe it is reporting to. • If you define a range that is out of the scope of the network on which the probe/cluster is installed, a warning message informs you that the probe is not included in the range. <ul style="list-style-type: none"> ◦ Click Yes to save the current range without including the probe in the range. ◦ Click No to continue editing without saving the current range.
Relevant tasks	<ul style="list-style-type: none"> • "How to Add Data Flow Probes to UCMDB" on page 54 • "How to Run Module/Job-based Discovery" on page 470 • "How to Configure Just-In-Time Discovery" on page 655 • "How to Configure Probe IP Ranges with Active Directory" on page 333


User interface elements are described below:

UI Element	Description
IPv4/6	Enables you to define the IP range in IPv4 or IPv6 format.
Definition Type	<ul style="list-style-type: none"> • IP Range. (IPv4 format only) Enables you to define an IP address range for the probe/cluster. You define a start IP address and an end IP address. • CIDR. Enables you to define an address range using the CIDR (Classless Inter-Domain Routing) notation, where each IP address has a network prefix that identifies either an aggregation of network gateways or an individual gateway. The length of the network prefix is also specified as part of the IP address and varies depending on the number of bits that are needed. <p>Available: When creating a new range only</p>
Range	Enables you to select a range over which the probe or cluster should perform discovery. IPv4

UI Element	Description
	<ul style="list-style-type: none"> • IP Range. Define a range of IPv4 addresses using the following rules: <ul style="list-style-type: none"> ◦ The IP address range must have the following format: start_ip_address – end_ip_address For example: 10.0.64.0 - 10.0.64.57 ◦ The first decimal value (octet) of the start IP address and the end IP address must be identical. For example, 10.1.2.3 - 10.4.5.6 ◦ The range can include an asterisk (*), representing any number in the range of 0-255. <ul style="list-style-type: none"> • If you use an asterisk, you do not need to enter a second IP address. For example, you can enter the range pattern 10.0.48.* to cover the range from 10.0.48.0 to 10.0.48.255. • Use an asterisk in the lower bound IP address of the IP range pattern only. If you use an asterisk in the lower bound IP address and also enter an upper bound IP address, the upper bound IP address is ignored. • You can use more than one asterisk (*) in an IP address as long as they are used consecutively. The asterisks cannot be situated between two numbers in the IP address, nor can they be substituted for the first digit in the number. For example, you can enter 10.0.*.* but not 10.*.64.*. • CIDR Notation. Define a range using the CIDR notation as follows: <ol style="list-style-type: none"> a. Enter the IP address in IPv4 format. b. In the drop-down, choose the number of bits (1-32) to determine the network prefix. For example, if you enter 192.30.250.00/18, then 192.30.250.00 is the network address and 18 indicates that the first 18 bits are the network part of the address, leaving the last 14 bits for specific host addresses. <p>IPv6</p> <p>IPv6 ranges are defined in CIDR notation only:</p> <ol style="list-style-type: none"> 1. Enter the IP address in IPv6 format. You can define IPv6 ranges using the full or compressed IPv6 notation Example: <ul style="list-style-type: none"> ◦ Full IPv6 addresses: abcd:abcd:abcd:abcd:abcd:abcd:abcd:abcd ◦ Compressed IPv6 address: <ul style="list-style-type: none"> • A:B:C:D:1:2:3:4 is the compressed version of 000A:000B:000C:000D:0001:0002:0003:0004

UI Element	Description
	<ul style="list-style-type: none"> • abcd::abcd is the compressed version of abcd:0000:0000:0000:0000:0000:abcd • ::abcd is the compressed version of 0000:0000:0000:0000:0000:0000:abcd <p>2. In the drop-down, choose the number of bits (1-128) to determine the network prefix.</p> <p>For example, if you enter abcd:abcd:abcd:abcd:abcd:abcd:abcd:abcd/100, then abcd:abcd:abcd:abcd:abcd:abcd:abcd:abcd is the network address and 100 indicates that the first 100 bits are the network part of the address, leaving the last 28 bits for specific host addresses.</p> <p>Note: IPv6 ranges cannot include IPv4-mapped IPv6 addresses (0.0.0.0 - 255.255.255.255). If your IPv6 range includes IPv4-mapped IPv6 addresses, these addresses must be defined separately in IPv4 ranges.</p> <p>For example, the IPv6 range, 0:0:0:0:ffe:0:0/60, must be defined as a number of ranges as follows:</p> <ul style="list-style-type: none"> • IPv6 range: 0:0:0:0:0:0:0 – 0:0:0:0:ffe:fff:fff • IPv4-mapped IPv6 range, 0:0:0:0:fff:0:0 - 0:0:0:0:fff:fff:fff, must be defined in IPv4 format: 0.0.0.0 - 255.255.255.255, per network class • IPv6 range: 0:0:0:1:0:0:0 – 0:0:0:f:fff:fff:fff
Type	<p>Defines the IP address lease time setting for the range.</p> <p>Available when: Defining a range for a Data Flow Probe or a probe cluster.</p> <p>Note: It is important to select the appropriate IP Address type to ensure that discovery is performed as expected. For more information, see "Effects of Range Type on Discovery Workflows" on page 46.</p> <ul style="list-style-type: none"> • Data Center. For permanent or long IP address lease times. This type is suitable for environments that have the following characteristics: <ul style="list-style-type: none"> ◦ IP addresses are stable due to long lease times or due to the consistent availability characteristics of the nodes and network ◦ Nodes connect to the network using the same interfaces due to a single access technology ◦ Few or no mobile users ◦ Single domain environment • Client. For short IP address lease times. This type is suitable for environments that have the following characteristics: <ul style="list-style-type: none"> ◦ IP addresses are not stable due to short lease times or due to the inconsistent availability characteristics of the nodes and network.

UI Element	Description
	<ul style="list-style-type: none"> ◦ Nodes connect to the network using different interfaces due to multiple access technologies. Therefore, the same IP address is bound to different interfaces at different times. ◦ Mobile users access the network from different domains in a multi-domain environment. <p>Note: Enable SNMP on all networking devices.</p>
Description (Optional)	A description about the selected range. <p>Note:</p> <ul style="list-style-type: none"> • Maximum number of characters allowed: 150 • No new lines or tabs may be inserted
Excluded IP Ranges	Enables you to define a range of IP addresses to exclude from the full network range specified above. <p>Note:</p> <ul style="list-style-type: none"> • The rules for entering an excluded range are the same as for entering a range. For details, see Range (on page 132). • The excluded range must be defined in the same format (IPv4/IPv6) as the full network range. • Even when a network range is defined using CIDR notation, the excluded ranges can still only be defined in <start_ip_address> – <end_ip_address> format. <p>New Excluded IP Range . Enables you to define a range of IP addresses to exclude from the full range, and enter a description about the excluded range if desired.</p> <p>Delete Excluded IP Range . Deletes an excluded IP range.</p> <p>Edit Excluded IP Range . Enables you to edit a defined excluded IP range.</p> <p>Example:</p> <p>You can divide a network range into several sub-ranges.</p> <p>For example, if the range is 10.0.64.0 – 10.0.64.255 and you define three excluded ranges:</p> <ul style="list-style-type: none"> • 10.0.64.45 – 10.0.64.50 • 10.0.64.65 – 10.0.64.70 • 10.0.64.89 – 10.0.64.95

UI Element	Description
	<div data-bbox="410 289 911 554" style="border: 1px solid black; padding: 10px; margin-bottom: 10px;"> <p style="text-align: center;">Network range 10.0.64.0 – 10.0.64.255</p> <div style="display: flex; justify-content: space-around;"> <div style="border: 1px solid black; border-radius: 50%; padding: 5px; text-align: center;"> 10.0.64.45 – 10.0.64.50 </div> <div style="border: 1px solid black; border-radius: 50%; padding: 5px; text-align: center;"> 10.0.64.89 – 10.0.64.95 </div> </div> <div style="text-align: center; margin-top: 10px;"> <div style="border: 1px solid black; border-radius: 50%; padding: 5px; text-align: center;"> 10.0.64.65 – 10.0.64.70 </div> </div> </div> <p>the Universal Discovery is performed over:</p> <ul style="list-style-type: none"> • 10.0.64.0 – 10.0.64.44 • 10.0.64.51 – 10.0.64.64 • 10.0.64.71 – 10.0.64.88 • 10.0.64.96 – 10.0.64.255
Ports	<p>Enables you to define ports over which passive discovery should be performed within the defined range:</p> <ul style="list-style-type: none"> • All available ports. Enables passive discovery over all available ports. • Selected ports Enables passive discovery over ports that you select from the Global Ports List. Click  to select ports to monitor. <p>Available: When defining a network range for a passive discovery probe only.</p>

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](#)" on page 124.
2. Remove the existing Probe from UCMDB. For details, see the **Remove Domain or Probe** button in "[Data Flow Probe Setup Window](#)" on page 105.
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" on page 75](#).

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" on page 76](#).

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" on page 324](#).

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:
 - **Windows:** `C:\hp\UCMDB\DataFlowProbe\tools\dbscripts`
 - **Linux:** `/opt/hp/UCMDB/DataFlowProbe/tools/dbscripts`

- 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 data_flow_probe_export.bin in the current directory
importPostgresql [Export file name] [PostgreSQL root account password]	Imports data from a file created by the exportPostgresql 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

- 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" on page 76](#).
- Data Flow Probe CUPs that were deployed manually can be uninstalled using manual methods only. For details, see ["How to Uninstall Probe CUPs Manually" on page 79](#).
- 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 Support for assistance in configuring callhome.

Troubleshooting Probe Auto Upgrade

Troubleshooting Probe Auto Upgrade - General

- **Limitation:** If the auto upgrade fails, retry will not resolve the issue. You need to access the corresponding probe server and perform manual deployment of version 10.33 probe.
- **Known Issue:** The **C:\hp\UCMDB\temp** folder was created and used by the probe auto upgrade agent 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.
- **Check if resources are placed under the right place after UCMDB server is upgraded to version 10.33**

- a. 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_10.33.exe**.

- b. Check if the probe auto upgrade agent 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,

- i. Go to **<UCMDB_Server>\content\probe_patch**.
 - ii. Copy the **probe-patch-10.33-windows.zip** package to the **<UCMDB_Server>\runtime\probe_upgrade** directory.
 - iii. Restart the UCMDB server. UCMDB server will then perform probe auto upgrade.
- **Probe auto upgrade log files**

Check the probe auto upgrade log files (in the **<DataFlowProbe>\runtime\log** directory) for more details:

- **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 upgrade agent upgrades a probe.

For more details about the log files, see ["Data Flow Probe Log Files" on page 99](#).

- **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\10.22to10.33\failed**. You can find the following message in **probe_auto_upgrade.log**:

```
2017-07-14 11:27:11 INFO ServiceControl:106 - Starting XML Enricher service...
2017-07-14 11:27:11 INFO ServiceControl:328 - XML EnricherStatus status:
STOPPED
2017-07-14 11:27:11 INFO ServiceControl:381 - Waiting for execution...
2017-07-14 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\xmlenricherWrapperEnricher.conf` file, or free the port **34545**.

Troubleshooting Probe Auto Upgrade - PostgreSQL Upgrade

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

In a more general way, 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.

- 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.

a. **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.

b. **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**.

- c. **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.

- d. **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
```

- e. **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:

- Stop the **UCMDB_Probe_DB** service.
- Remove the content of the **pgsql** folder and copy the content of the **pgsql.old** folder into the **pgsql** folder.
- 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%
```

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

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

Troubleshooting - Probe Auto Upgrade Agent

Before upgrading a probe, the probe auto upgrade agent checks the environment and the probe status.

- a. **Check probe version.** Only a probe of version 10.22 or higher could be upgrade. For supported probe versions, see [Supported Versions](#).
- b. **Check probe status.** Only union mode probe in non-FIPS mode could be upgraded.
- c. **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.

- **How to check if a probe has been upgraded successfully?**

You can check the **probe_auto_upgrade.log** file (in the **C:\hpb\UCMDB\DataFlowProbe\runtime\log\probeUpgradeLogs** folder).

- If the probe has been upgraded successfully, you can 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 the probe upgrade failed, 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](#)" on page 99.

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

Solution: You need to 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 following log files for further information:

- **probe_upgrade_conf_merge.log**
- **pg_upgrade.log**
- **probe_post_upgrade.log**

Troubleshooting - Three Way Merge Function

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 is **500**. So if your value is greater than 500, it will be modified 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\HPProbeKeyStore.jks**
- **<DataFlowProbe>\conf\security\HPProbeTrustStore.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 probe manually.

Chapter 3: Data Flow Probe Status

This chapter includes:

How to View Job Information on the Data Flow Probe	147
Data Flow Probe Status User Interface	148
Discovery Job Operation Commands	153
Job Operation Parameters	160

How to View Job Information on the Data Flow Probe

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

This task includes the following steps:

1. Access the MBean operations

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

- a. 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.

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

2. Locate the operation to invoke

On the MBean View page, select **type=JobsInformation**. Locate the required operation. For details, see "[Discovery Job Operation Commands](#)" on page 153 and "[Job Operation Parameters](#)" on page 160.

3. Run the operation

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

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


Data Flow Probe Status User Interface

This section includes:

<Job Name> Dialog Box	148
Data Flow Probe Status Window	149

<Job Name> Dialog Box

Enables you to view status and progress of a job that ran or is currently running on a Data Flow Probe.

To access	Select Data Flow Management > Data Flow Probe Status > Progress pane > a job, and click the View job progress  button.
See also	<ul style="list-style-type: none"> • "How to Add Data Flow Probes to UCMDB" on page 54 • "How to Start a Data Flow Probe" on page 56 • "How to Stop a Data Flow Probe" on page 58 • "How to Run Zone-based Discovery" on page 428 • "How to Run Module/Job-based Discovery" on page 470 • "How to Manually Activate Modules/Jobs/CIs" on page 473


User interface elements are described below:

UI Element (A–Z)	Description
Job	<ul style="list-style-type: none"> • Status. The status of the job: Scheduled, Running, Blocked, Removed.

UI Element (A–Z)	Description
Details	<ul style="list-style-type: none"> • Last updated. The last time that the job was updated. • Threads. The number of threads currently allocated to this job. • Progress. The number of Trigger CIs in the job and the number of Trigger CIs that the Probe has finished working on. • Discovered CIs in sending queue. The number of CIs/relationships discovered by the discovery job, and that are waiting to be sent to the UCMDB Server.
Schedule	<ul style="list-style-type: none"> • Previous invocation. The last time that Universal Discovery ran the job. • Next invocation. The next time that Universal Discovery is scheduled to run the job. • Last duration. The length of time, in seconds, taken to run the job in the previous invocation. This is calculated according to the start time of the first trigger until the end time of the last trigger, even if triggers were added later on. • Average duration. The average duration (in seconds) per trigger of the time it took the Probe to run this job. • Recurrence. The number of times the job ran via the scheduler (manual runs are not counted).
Discovery Results	For details, see " Data Flow Probe Status Window " below.

Data Flow Probe Status Window

Enables you to view the current status of discovered CIs and all active jobs running on the Probes.

To access	Select Data Flow Management > Data Flow Probe Status .
Important Information	<ul style="list-style-type: none"> • Depending on what you select in the Domains Browser pane, different information is displayed in the viewing pane. If you select: <ul style="list-style-type: none"> ◦ a domain, you can view details and discovery results for the domain. ◦ a Probe, you can view details on the Probe (such as the Probe IP), the progress of a job and you can view discovery results. • The view is not automatically updated. To refresh the status data, click the  button. • If a Probe is configured in Separate mode, no results are shown in this window.

Relevant tasks	<ul style="list-style-type: none"> • "How to View the Current Status of Discovered CIs" on page 661 • "How to Add Data Flow Probes to UCMDB" on page 54 • "How to Start a Data Flow Probe" on page 56 • "How to Stop a Data Flow Probe" on page 58 • "How to Run Zone-based Discovery" on page 428 • "How to Run Module/Job-based Discovery" on page 470
-----------------------	--

Domain Browser Pane

Displays the domains and Probes defined in the UCMDB system in a tree view.

Domain Details Pane

Displays the details of the domain selected in the Domains Browser pane.


User interface elements are described below:

UI Element (A–Z)	Description
Domain Type	<ul style="list-style-type: none"> • Customer. A private domain used for your site. You can define several domains and each domain can include multiple Probes. Each Probe can include IP ranges but the customer domain itself has no range definition. • External. Internet/public domain. A domain that is defined with a range. The external domain can contain only one Probe whose name equals the domain name. However, you can define several external domains in your system. <p>For details on defining domains, see "Add New Domain Dialog Box" on page 104.</p>

Data Flow Probe Details Pane

Displays the details of the Probe selected in the Domains Browser pane.

User interface elements are described below:



UI Element (A–Z)	Description
	Refreshed the data so that the most current status of the discovered CIs and jobs on the selected Probe is displayed.

UI Element (A–Z)	Description
	<p>Note: The maximum timeout for refreshing is set to 30,000 milliseconds by default. To change this setting, change the Max time out for getting probe status setting in the Infrastructure Settings Manager. For details, see "Infrastructure Settings Manager Page" in the <i>Universal CMDB Administration Guide</i>.</p>
Last updated	The date and time at which the Get snapshot button was last pressed (that is, the date and time of the data displayed in Data Flow Probe Status).
Probe IP	The IP address which the Probe communicates with UCMDB.
Running jobs	The number of jobs running on the Probe.
Scheduled jobs	The number of jobs that are scheduled to run according to the settings in the Discovery Scheduler. For details, see " Discovery Scheduler Dialog Box " on page 496 .
Status	<p>The status of the Probe:</p> <ul style="list-style-type: none"> • Connected. The Probe is connected to the server (the Probe connects every few seconds). • Connected (suspended). The Probe is connected, but it is suspended such that no jobs can run on the Probe. • Disconnected. The Probe is not connected to the server.
Threads	The sum of all threads currently allocated to the running jobs.
Total Discovered CIs in sending queue	The total number of CIs/relationships discovered by all of the discovery jobs that ran on the Probe, and that are waiting to be sent to the UCMDB Server.

Progress Pane

Displays the progress of the jobs on the selected Probe.



User interface elements are described below:

UI Element (A–Z)	Description
	<p>View Job Progress. Opens the <Job Name> dialog box, enabling you to view the details of the selected job. For details, see "<Job Name> Dialog Box" on page 148.</p> <p>Available: When a job is selected in the Progress pane.</p>
	<p>View Workflow Information. Opens the Workflow Information dialog box, enabling you to view workflow information for a selected job that is dependent on a workflow adapter and that is currently running. This dialog box shows the following information for the job: Trigger CI, current step, workflow status, workflow start time, workflow end time, parking status, current timeout period, and next invocation time.</p> <p>If you double-click on a Trigger CI in the Workflow Information dialog box, a history of all steps that have already been executed during the current execution of the selected job is displayed.</p> <p>Available when: A currently running job that is dependent on a workflow adapter is selected in the Progress pane.</p>
<p>Job List</p>	<p>List the following information about the jobs that ran or are scheduled to run on the Probe, and their progress:</p> <ul style="list-style-type: none"> • Job. The name of the job scheduled to run on the Probe. • Discovered CIs in Sending Queue. The number of CIs/relationships discovered by the selected discovery job, and that are waiting to be sent to the UCMDDB Server. • Next invocation. The next time that the Probe is scheduled to run. • Previous invocation. The last time that the Probe ran. • Progress. The progress of the job as it is running. <p> Note: If a job has not started running, the Progress column displays Scheduled.</p> <ul style="list-style-type: none"> • Thread count. The number of threads currently allocated to the selected job. • Triggered CIs. The number of CIs triggered by the job.

Discovery Results Pane

Enables you to view discovery results.

User interface elements are described below:

UI Element (A–Z)	Description
	<p>Refresh. Enables you to retrieve the latest data from the Probe.</p> <p>Note: This data is not automatically updated.</p>
	<p>Set Filter. Enables you to set the time range for which to display discovery results.</p> <ul style="list-style-type: none"> • All. Displays results for all job runs. • Last Hour/Day/Week/Month. Choose a period of time for which to display discovery results. • Custom Range. Opens the Change Timeframe dialog box customize the time range for which to display discovery results. Do one of the following: <ul style="list-style-type: none"> ◦ In the From and To boxes, click the arrow to choose a date and time from the calendar. ◦ Click Last Day to view the last 24 hours worth of results.
<Results grid>	<ul style="list-style-type: none"> • CIT. The name of the discovered CIT. • Created. The number of CIT instances created by the Probe • Deleted. The number of CIT instances deleted by the Probe. • Discovered CIs. The sum of all the CIs for all the invocations. • Updated. The number of CIT instances that have been updated.
Filter	Displays the selected filter.
Last updated	The date and time that the results data was updated for a particular Probe.

Discovery Job Operation Commands

For details on viewing job information, see ["How to View Job Information on the Data Flow Probe" on page 147.](#)

activateJob

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

Note: The following message is displayed if the job has not been activated and there is no

information about the job in the Probe's database:

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

activateJobOnDestination

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

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

start/stop

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

viewJobErrorsSummary

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

For details on the job operation parameters, see ["Job Operation Parameters" on page 160](#).

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

viewJobExecHistory

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

For details on the job operation parameters, see ["Job Operation Parameters" on page 160](#).

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

viewJobProblems

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

For details on the job operation parameters, see "[Job Operation Parameters](#)" on page 160.

Column	Description
Job ID	Displayed if the jobID field is left empty. The job name as it appears in Data Flow Management. Click a job to go to its viewJobStatus page, to view its status and scheduling information.
Trigger CI	Displayed if the triggerID field is left empty. The CMDB object ID of the trigger for a job.
ErrMsgCode	The error message hash string (error hash ID).
ErrParams	The error parameters.
Severity	The severity of the error. For details on severity levels, see "Error Severity Levels" in the <i>Universal CMDB Developer Reference Guide</i> .

viewJobResultCiInstances

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

For details on the job operation parameters, see "[Job Operation Parameters](#)" on page 160.

The **Object State Holder** column displays the code for the CI or relationship defined in the CMDB. For details on creating object state holders for common CITs, see **modeling.py** in "Jython Libraries and Utilities" in the *Universal CMDB Developer Reference Guide*. For details on the **appilog.common.system.typesClass ObjectStateHolder** method, see the **ObjectStateHolder** method in the online API documentation.

viewJobResults

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

For details on the job operation parameters, see "[Job Operation Parameters](#)" on page 160.

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

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

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

Column	Description
Job Name	<p>Displayed if the jobID field is left empty.</p> <p>The job name as it appears in Data Flow Management.</p> <p>Click a job to go to its viewJobStatus page, to view its status and scheduling information.</p>
CI Type	Click to filter the list to show results for one CIT only.
Touched CIs	Click to go to the viewJobResultCiInstances page, to view a list of those CIs discovered by the job that are Touched CIs . For details, see " Job Operation Parameters " on page 160.
Non Touched CIs	Click to go to the viewJobResultCiInstances page, to view a list of those CIs discovered by the job that are not Touched CIs.
Triggered CIs for Touched CIs	Click to go to the viewJobTriggeredCIs page, to view a list of those Trigger CIs included in a job that are Touched CIs.
Triggered CIs for Non Touched CIs	Click to go to the viewJobTriggeredCIs page, to view a list of those Trigger CIs included in the job that are not Touched CIs.
Last Discover Time	The date and time that the job was invoked.

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

viewJobsStatuses

Click the **viewJobsStatuses** button to return status and scheduling information for all jobs. You can choose to filter the results. For details, see "[Job Operation Parameters](#)" on page 160.

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

The results page displays the following information:

Column	Description
No.	The number of the job in the list.
Job Name	The job name as it appears in Data Flow Management. Click a job to go to its viewJobStatus page, to view its status and scheduling information.
Status	The severity of the job's status, as calculated by the Probe. <ul style="list-style-type: none"> • Blocked. Not in use. • Removed. The job is no longer active. • Done/Total Triggers. The number of trigger CIs that the Probe finished running on, against the total number of triggers for the job. For example, (28/69) indicates that there is a total of 69 triggers for the job, while the Probe has completed running on 28 of those triggers. • Scheduled. The job is scheduled to run. For details on scheduling jobs, see "Discovery Scheduler Dialog Box" on page 496. <p>A red background signifies that a thread has run longer than expected and may be stuck. A green background signifies that the job is running as expected.</p>
Triggered CIs	The Trigger CIs that have been run by the job. Click to go to the viewJobTriggeredCIs page.
Errors & Warnings	The number of errors and warnings for a specific job. Click to go to the viewJobErrorsSummary page, to view a list of error and warning messages reported on this job.
Last Invocation	The date and time that the job was last run.
Next Invocation	The date and time that the job is next scheduled to run.
Last Total run	The length of time, in seconds, taken to run the job in the previous invocation. This is calculated according to the start time of the first trigger until the end time of the last

Column	Description
duration (seconds)	trigger, even if triggers were added later on.
Avg run duration (seconds)	The average duration (in seconds) per trigger of the time it took the Probe to run this job.
Recurrence	The number of times that the job was invoked. Click to go to the viewJobExecHistory page, to retrieve a history of job invocations.
Results	The number of CITs that have been discovered by the job. Click to go to the viewJobResults page to view the CITs. Note: Displayed when hideResults parameter is set to False .

viewJobStatus

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

For details on the job operation parameters, see "[Job Operation Parameters](#)" on page 160.

The results page displays the following information:

Column	Description
Threading info	The total number of worker threads created by the invocation, the free worker threads, and the stuck worker threads.
Total work time	The time that the Probe took to run this job.
Tasks waiting for execution	A list of jobs together with the number of Trigger CIs that are awaiting activation.
Max. Threads	The number of threads that are serving this job.
Progress	A summary of the current run, that is, since the specific run was activated. For example, Progress: 2017 / 6851 destinations (29%) means that out of 6851 CIs, 2017 CIs have already run.
Working Threads information	<ul style="list-style-type: none"> Thread Name. The thread that is now running this job. Click to go to the viewJobThreadDump page. You use this page when a thread is running for a long time, and you must verify that this is because the thread is working hard, and not because there is a problem.

Column	Description
	<ul style="list-style-type: none"> • Curr Dest. ID. The name of the node on which the job is running. • Curr Dest. IP. The IP for which the job is discovering information. • Work Time (Sec). The length of time that this thread is running. • Communication Log. Click to go to the viewCommunicationLog page, to view an XML file that logs the connection between the Probe and a remote machine. For details, see the Create communication logs field in the "Execution Options Pane" on page 260.
Discovery Jobs Information table	<ul style="list-style-type: none"> • Status. The severity of the job's status, as calculated by the Probe. For details, see "Status" on page 157. • Triggered CIs. Click to go to viewJobTriggeredCIs page, to view a list of Trigger CIs that are part of a job. • Errors & Warnings. Click to go to viewJobErrorsSummary page, to view a list of error and warning messages reported on this job. • Last invocation. The date and time that the job was last run. • Next invocation. The date and time that the job is next scheduled to run. • Last Total run duration (seconds). The length of time, in seconds, taken to run the job in the previous invocation. This is calculated according to the start time of the first trigger until the end time of the last trigger, even if triggers were added later on. • Avg run duration (seconds). The average duration (in seconds) per trigger of the time it took the Probe to run this job. • Recurrence. The number of times that the job was invoked. Click to go to viewJobExecHistory page, to view a history of job invocations.

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

viewJobTriggeredCIs

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

For details on the job operation parameters, see "[Job Operation Parameters](#)" on the next page.

The results page displays the following information:

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

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

`viewJobTriggeredCIsWithErrorId`

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

Job Operation Parameters

The following list includes job operation parameters.

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

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

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

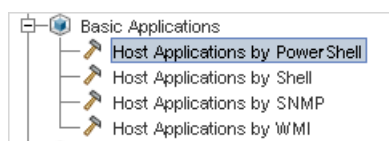
True: the table displays the total number of CIs and the total number of Trigger CIs for each CIT.

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

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

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

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



- **maxRows.** The maximum number of rows that should be displayed in the results table. The default is 100 or 1000.
- **maxTriggeredCIs.** See **maxRows**.
- **objectID.** The CMDB object ID.
- **hideRemovedJobs.** Hides information about jobs with the status, **REMOVED**. These are jobs that have run previously but that are not currently scheduled to run.
- **hideResults.** Indicates whether or not to hide the **Results** column. If the **Results** column is present, you can navigate to the job results. For more information, see "[viewJobResults](#) " on [page 155](#), and "[viewJobsStatuses](#) " on [page 157](#).
- **triggerCI.** The CMDB object ID of the trigger for a job.
- **triggeredCiID.** See **triggerCI**.

Chapter 4: Universal Discovery Agents

This chapter includes:

Universal Discovery Agent Overview	163
Universal Discovery Agent Deployment	164
Universal Discovery Agent Certificates	166
Call Home Overview	167
FDCC/USGCB Support	169
How to Create New Certificates for Universal Discovery Agent	171
How to Customize Platforms for Universal Discovery Agent Deployment	172
How to Install the Universal Discovery Agent Manually	174
How to Install Universal Discovery Agent to Run Under a Non-Root Account on UNIX	177
How to Configure Call Home	178
How to Enable Changing the Default Port Number for Call Home	179
How to Specify Data and Temp Folder Locations when Installing or Updating the Universal Discovery Agent for UNIX	180
How to Completely Uninstall the Universal Discovery Agent	181
Agent Installation Wizard Overview	182
Agent Installation User Interface	183
Discovery Node Disk Requirements	187
Universal Discovery Agent Installation Resources	188
Universal Discovery Agent File Locations	195
Software Identification Tags	197

Universal Discovery Agent Overview

Universal Discovery (UD) Agent is a program that is installed on a discovery node. The following table shows functions that the UD Agent performs:

Function
Communication. Performs job scheduling and job execution functions with the Data Flow Probe

Function
and with the Scanner.
Shell. Provides a command line interface that provides access to services. The UD Agent uses the Universal Discovery protocol.
Software Utilization. Generates files that contains application utilization data. For more information, see "Software Utilization" on page 704.

For more information about deployment methods, see ["Universal Discovery Agent Deployment" below.](#)

The UD Agent generates a **Unique ID** when it is installed on a discovery node. However, if there is a Unique ID already stored on the node, the UD Agent uses the existing Unique ID. Unique ID generation occurs when agent-based and agentless discovery methods are used. Additionally, generation might also occur when the Inventory Discovery by Scanner job and the Host Connection by Shell job run.

The Unique ID can be utilized as follows:

- **Reconciliation.** The Unique ID is used for identification and validation criterion during reconciliation operations.
- **Authentication.** The Data Flow Probe uses the Unique ID to validate that it is connecting to the correct discovery node when performing discovery.

For details about deploying the UD Agent, see ["Universal Discovery Agent Deployment" below.](#)

Universal Discovery Agent Deployment

The Universal Discovery (UD) Agent can be installed using one of the following methods:

Deployment Method	Description
Infrastructure Discovery Activity	You can use the Infrastructure Discovery activity to configure and deploy UD Agents. For more information about setting up this activity, see the <i>Universal CMDB Discovery and Integrations Content Guide</i> .
Manual	Third party software distribution tools, scripting, or any remote access technology can be used to deploy and install discovery packages. For more information, see "How to Install the Universal Discovery Agent Manually" on page 174.

Supported Platforms

When installing the agent via the Infrastructure Discovery activity, the configuration file, **AgentsSupportMatrix.xml**, located in the UDAgentManagement package controls the list of platforms on which the UD Agent can be installed. The list of platforms defined in this file matches the list of platforms officially supported by the UD agent.

Owing to the large number of platform versions, as well as new platform versions emerging all the time, the configuration file does not include every possible platform on which the corresponding UD agent may be installed and function correctly.

For example, there may be different distributions of Linux not currently officially supported, where the Linux UD Agent may indeed be deployed and work correctly. If, after internal testing, you can confirm that the UD Agent works correctly on a particular platform, you can modify the AgentsSupportMatrix.xml file to include the additional version/distribution. Any such modifications can be used only on an “as is” unsupported basis.

To edit the AgentsSupportMatrix.xml file, see ["How to Customize Platforms for Universal Discovery Agent Deployment" on page 172](#).

Note:

- For a list of out-of-the-box supported platforms and versions for the UD Agent, see the Supported Content section of the *Universal CMDB Discovery and Integrations Content Guide*. Supported platforms are added based on the growing number of tested platforms and customer requests.
- Deploying the UD Agent on a platform that is not defined among the supported platforms may result in the UD Agent not functioning properly.

UD Agent Running Modes

After deployment, you can configure the UD Agent to run in one of the following modes:

Running Mode	Description
Complete Install	The UD Agent, software utilization, and Software Identification Tags are installed on the discovery node. Note: This running mode is the default one when you use activities to install discovery packages.

Running Mode	Description
Software Utilization	Software utilization and Software Identification Tags are installed on the discovery node. Scanners are run manually using third party solutions, scripts, or other remote access technology.

Universal Discovery Agent Certificates

Universal Discovery Agent certificates are files that provide encrypted communication between the Universal Discovery Agent and Data Flow Probe.

For each Universal Discovery Agent credential that is created, there is a corresponding pair of certificate files.


- **Acstrust.cert.** This file is the public certificate file of the Data Flow Probe.
- **Agentca.pem.** This file contains the public and private certificate file of the Universal Discovery Agent.

Caution: These files are critical in maintaining communication between the Data Flow Probe and the discovery nodes.

Note: If you want to change the certificate files, you must uninstall the Universal Discovery Agents, create new credentials and perform Universal Discovery Agent deployment again.

Using Certificates

In order for Data Flow Probes to use the same Universal Discovery Agent certificates in different domains, perform the following:

1. Select your credential in the **Data Flow Probe Setup > Domains and Probes > Credentials** pane.
2. Click the **Copy selected credential to another domain**  button.

Call Home Overview

Call Home provides a way for discovery nodes to communicate with the Data Flow Probe. This option is most suited for networks that have mobile nodes, VPN clients, or for any nodes that have short DHCP lease times. Nodes regularly initiate communication with the Data Flow Probe. This **Call Home** communication occurs within ten minutes after the node is attached to the network.

Note:

- Call Home is enabled by default.
- Call Home does not work when DirectAccess is involved.

Traffic Case-Typical

The following traffic case typically occurs when a Universal Discovery Agent that is installed on a computer initiates Call Home:

1. The Universal Discovery Agent sends a request message to the Data Flow Probe.
2. The Data Flow Probe sends an acknowledgement message to the Universal Discovery Agent.

Note:

- If the Universal Discovery Agent does not receive the acknowledgement message, it sends messages to the Data Flow Probe every hour until an acknowledgement message is received.
 - The acknowledgement message is an HTTP 200 series status message.
3. The Data Flow Probe creates a Node CI, a Call Home Event CI, and a UD Agent CI.
 4. The Call Home Event CI triggers the Call Home Processing job.
 5. The Call Home Event CI for the Call Home Processing job is sent to the Data Flow Probe.
 6. The Call Home Processing job starts.
 7. The Call Home Processing job sends a notification message to workflows that are associated with the node and that are waiting to be run. These workflows are also known as **parked workflows**. After the notification message is received, the parked workflow runs. The Universal Discovery Agent continues to send the request message according to the value that is set for the

Call Home Request Frequency parameter. This parameter is configured when configuring Universal Discovery Agents for deployment. For more information on configuring this parameter, see the section about the Infrastructure discovery activity in the *Universal CMDB Discovery and Integrations Content Guide*.

Traffic Case-New Node

The following traffic case occurs when a Universal Discovery Agent that is installed on a new node initiates Call Home:

1. The Universal Discovery Agent sends a request message to the Data Flow Probe.
2. The Data Flow Probe sends an acknowledgement message to the Universal Discovery Agent.

Note: If the Universal Discovery Agent does not receive the acknowledgement message, it sends messages to the Data Flow Probe every hour until an acknowledgement message is received.

The acknowledgement message is an HTTP 200 series status message.

3. UCMDB creates a Node CI, Call Home Event CI, and UD Agent CI.
4. A new Inventory Discovery by Scanner job is triggered.

Traffic Case-Mobile Computer

The following traffic case typically occurs when a mobile computer connects to the network after a long time:

1. The computer connects to the network.
2. The IP/MAC Harvesting job runs. The job updates IP/MAC pair information, and then it creates a Call Home Event CI.
3. The Call Home Event CI triggers the Call Home Processing job.
4. The Call Home Event CI for the Call Home Processing job is sent to the Data Flow Probe.
5. The Call Home Processing job starts.
6. The Call Home Processing job sends a notification message to workflows that are associated with the node and that are waiting to be run. These workflows are also known as **parked workflows**. After the notification message is received, the parked workflow runs.

FDCC/USGCB Support

Overview

The Federal Desktop Core Configuration/United States Government Configuration Baseline (USGCB) is a list of security settings recommended by the National Institute of Standards and Technology for computers that are connected directly to the network of a United States government agency. The purpose of the initiative is to create security configuration baselines for Information Technology products.

Feature Impact

UCMDB Web Interface. To establish a web connection with the UCMDB server, the Java Runtime Environment needs to be installed.

Infrastructure Activity. Using this activity to install or upgrade Universal Discovery Agents is not supported. Alternatively, use manual methods to deploy Universal Discovery Agent installation packages to nodes. For details, see ["How to Install the Universal Discovery Agent Manually" on page 174.](#)

How to Update Security Policy Settings for FDCC

This task describes how to make security policy configurations to ensure compliancy with the FDCC mandate after you manually deploy the Universal Discovery Agent.

This task includes the following steps:

1. ["Allow firewall exceptions" below](#)
2. ["Create firewall exceptions" on the next page](#)
3. ["Results " on the next page](#)

1. Allow firewall exceptions

The FDCC security policy disables the **Firewall Exceptions** setting. Enable it either using local policy or domain policy by using the Group Policy Editor.

- a. Click **Run** and type **gpedit.msc** to open the Group Policy Editor.
 - b. Select **Local Computer Policy > Computer Configuration > Administrative Templates > Network > Network Connection > Windows Firewall > Standard Profile|Domain Profile**.
 - c. Double click **"Windows Firewall- Do not allow exceptions"**.
 - d. In the **Properties** dialog box, click **Disabled**.
2. Create firewall exceptions

The FDCC security policy disables the **Firewall Exceptions** setting. You must enable it either using local policy or domain policy by using the Policy Editor.

- a. Select **Go to Local Computer Policy > Computer Configuration > Administrative Templates > Network > Network Connection > Windows Firewall > Standard Profile|Domain Profile**.

Note: Paths may vary depending on the version of Windows.

- b. Double click **Windows Firewall-Define the Inbound Program Exceptions**.
- c. In the **Properties** dialog box, click **Enabled**.
- d. Click **Show**.
- e. In the **Show Contents** dialog box, create an entry for the Universal Discovery Agent. Follow the format conventions that are specified in the **Options** pane on the left side.

Note: Values vary depending on the configuration that you specified when deploying Scanners. The port number of the Universal Discovery Agent is 2738 or 7738. The path of the Universal Discovery Agent is **C:\Program Files\Hewlett-Packard\Discovery Agent\bin32\discagnt.exe**. For more information about Scanners and Scanner parameters, see "[Scanner Command Line Parameters Overview](#)" on page 585.

3. Results

Verify that the Universal Discovery Agent can communicate with the Data Flow Probe by invoking the **Check Credentials** option for any Universal Discovery Protocol credential. For more information, see "[<Protocol> Details Pane](#)" on page 113.

How to Create New Certificates for Universal Discovery Agent

This task describes how to regenerate and reissue certificate files that are used for communication between the Data Flow Probe and the Universal Discovery Agent.



Note:

- The Universal Discovery Agent may be upgraded during this procedure.
- The frequency that you perform this task depends on your organization's policy.

1. Prerequisites

Ensure that the UCMDB server is running.

2. Enable the parameter

- In **UCMDB**, go to **Data Flow Management > Universal Discovery > Discovery Modules/Jobs** tab.
- In the Discovery Modules tree, select **Tools and Samples > UD Agent Management**.
- Select the **Install UD Agent** or **Update UD Agent** job. Click the Properties tab and select the **UDAgentInstallCredentialID** parameter. In the Parameters pane, perform the following:
 - Select the Override check box for the parameter.
 - Click the corresponding cell in the Value column and click . The **Choose Credentials** dialog box opens.
- In the Choose Credentials dialog box, select a credential for the job to use to connect to the remote machine, or click  to create new credentials.

3. Results

The certificates are deployed to the remote machines the next time the job that you selected in [step 2](#) runs.

How to Customize Platforms for Universal Discovery Agent Deployment

The configuration file **AgentsSupportMatrix.xml** is located in the **UDAgentManagement** package and controls the list of platforms on which the Universal Discovery (UD) Agent can be installed.

Owing to the large number of platform versions, as well as new platform versions emerging all the time, the configuration file does not include every possible supported platform on which the UD Agent may be installed and function correctly.

This task describes how to modify the **AgentsSupportMatrix.xml** file to include additional versions/distributions on platforms that have been tested and confirmed to support UD Agent functionality:

Note: Any such modifications can be used only on an “as is” unsupported basis.

1. Go to **Data Flow Management > Adapter Management**.
2. Under the **UDAgentManagement** package, select **Configuration Files > AgentsSupportMatrix.xml**.
3. Go to the relevant **<operating-system>** tag.
4. Check if the version of the operating system already exists under the relevant **<architecture>** tag. If not, enter the unlisted version by copying one of the existing **<version>** tags, and replacing the **name** and **display name** values with the relevant new values.

For example:

```
ResourceDiscovery\ConfigFiles\AgentsSupportMatrix.xml
1 <agents-support-matrix parserClassName="com.hp.ucmdb.discovery.library.communication.downloader.cfgfiles.platform
2
3 <operating-system name="windows" display-name="Windows">
4 <version-identification-commands>
5 <command>ver</command>
6 </version-identification-commands>
7 <architecture name="x86">
8 <!--Uncomment to install on any version-->
9 <!--<version name="any" display-name="Any">.*</version-->
10 <version name="Microsoft Windows XP" display-name="Microsoft Windows XP">.*[Ww]indows.*5\.1.*</versio
11 <version name="Windows Server 2003" display-name="Windows Server 2003">.*[Ww]indows.*5\.2.*</version
12 <version name="Windows Server 2008/Windows Vista" display-name="Windows Server 2008/Windows Vista">.*[
13 <version name="Windows Server 2008 R2/Windows 7" display-name="Windows Server 2008 R2/Windows 7">.*[W
14 <version name="Windows 8" display-name="Windows 8">.*[Ww]indows.*6\.2.*</version>
15 </architecture>
16 <architecture name="amd64">
17 <!--Uncomment to install on any version-->
18 <!--<version name="any" display-name="Any">.*</version-->
19 <version name="Windows XP 64-Bit Edition/Windows Server 2003" display-name="Windows XP 64-Bit Editor
20 <version name="Windows Server 2008/Windows Vista" display-name="Windows Server 2008/Windows Vista">.*[
21 <version name="Windows Server 2008 R2/Windows 7" display-name="Windows Server 2008 R2/Windows 7">.*[W
22 <version name="Windows Server 2012 R2/Windows 8" display-name="Windows Server 2012 R2/Windows 8">.*[W
23 </architecture>
24 </operating-system>
25 <operating-system name="linux" display-name="Linux">
26 <version-identification-commands>
27 <command>uname -a</command>
28 <command>cat /etc/enterprise-release /etc/oracle-release /etc/redhat-release /etc/lsb-release /etc/Su
29 </version-identification-commands>
30 <architecture name="x86,x64">
31 <!--Uncomment to install on any version-->
32 <!--<version name="any" display-name="Any">.*</version-->
33 <version name="Red Hat 3" display-name="Red Hat Enterprise Linux AS/ES/WS 3">.*Red Hat[^\0-9]*3.*</ver
34 <version name="Red Hat 4" display-name="Red Hat Enterprise Linux AS/ES/WS 4">.*Red Hat[^\0-9]*4.*</ver
35 <version name="Red Hat 5" display-name="Red Hat Enterprise Linux 5 Server/Desktop">.*Red Hat[^\0-9]*5.*
36 <version name="Red Hat 6" display-name="Red Hat Enterprise Linux 6 Server/Desktop">.*Red Hat[^\0-9]*6.*
37 </architecture>
38 </operating-system>
39 </agents-support-matrix>
```

Note:

- If the relevant operating system or architecture is not listed, create new tags for these.
- To allow support for all versions of a particular architecture of an operating system, under that architecture's tag, uncomment the line: **<version name="any" display-name="Any">.*</version>**
- For a list of out-of-the-box supported platforms and versions for the UD Agent, see the Supported Content section of the *Universal CMDB Discovery and Integrations Content Guide*.
- For more information about UD Agent deployment, see "[Universal Discovery Agent Deployment](#)" on page 164.

How to Install the Universal Discovery Agent Manually

This task describes how to install the Universal Discovery (UD) Agent manually on remote machines.

1. Prerequisite

- Ensure that the platform of the remote machine on which you want to install the UD Agent is supported.
- For more information, see ["Universal Discovery Agent Deployment" on page 164](#).
- For a list of out-of-the-box supported version, see the Supported Content section in the *Universal CMDB Discovery and Integrations Content Guide*.

2. Export the UD Agent installation file and the UD Protocol certificate.

- a. Go to **Administration > Package Manager** and export the **UDAgentManagement** archive file.

For more information, see "How to Export a Package" in the *Universal CMDB Administration Guide*.

- b. Extract the UD Agent installation file or files that are appropriate for the platform of your discovery nodes from the following location in the archive file:

discoveryResources\ud_agents

For a mapping of installation files to platforms, see ["Universal Discovery Agent Installation Resources" on page 188](#).

Tip:

- The file name indicates the platform.
- **UNIX only.** Additionally, extract the **agentinstall.sh** file.

- c. In **Data Flow Management**, go to **Data Flow Probe Setup > Domains and Probes**. In the relevant domain, select the UD protocol credential whose certificate you want to export, and click **Export Public Certificates**.

3. Copy the UD Agent installation and the UD Protocol certificate.

Copy the exported UD Agent and certificate to the remote machine and install them using one of the following methods:

Note: Ensure that you distribute or copy installation files that are appropriate to the platform of the discovery node.

- o **Attended (Windows only)**

Copy the UD Agent installation file and certificate using any manual method or remote access technology to the remote Windows machine, and then perform installation by clicking the executable (.MSI) file. For more information on running or configuring this installer, see "[Agent Installation Wizard](#)" on page 183.

- o **Unattended (All platforms)**

- i. Copy the UD Agent installation file or files and the certificate file to the remote machine using any manual method or remote access technology.

UNIX only. Additionally, copy the **agentinstall.sh** file.

- ii. Perform the installation by using command line parameters. For details on parameters for all platforms, see "[Universal Discovery Agent Installation Resources](#)" on page 188.

For example, the following command is used to install the UD Agent on a Windows machine, to listen on port 7738, with a connection timeout of 900 msec, with the UD Protocol certificate located in c:\UDAgentInstall

```
c:\AgentTest>msiexec /i hp-ud-agent-win32-x86-10.10.000.xxx.msi /quiet
SETUPTYPE=Enterprise PORT=7738 TIMEOUT=900
CERTPATH=c:\UDAgentInstall PERIOD=90 SOFTWAREUTILIZATION=ON
URL0=15.178.179.124 URL1=15.178.179.125 URL2=15.178.179.126
```

Note:

- For error code information, see platform-specific information at "[Universal Discovery Agent Installation Resources](#)" on page 188.
- If an error occurs, the screen may also display a message with information about the error.

4. Generate Unique IDs for Disk Cloning- Optional

If you are using disk cloning to distribute images that contain the UD Agent, perform the following

to generate Unique IDs:

- a. **UNIX and Mac OS X only.** Log in using the user account that is used to run the UD Agent. If the location of the data files were modified with the `--home` command line option at the time of installation, type **HOME=<HOME>** and press ENTER at a command prompt.

Note: <HOME> is the home directory of the user that runs the UD Agent on the computer where the disk image was created.

- b. Navigate to the directory that contains the UD Agent executable files and run the following command:

- **Windows:** `discagnt.exe --newuniqueid`
- **UNIX:** `./discagnt --newuniqueid`

Note: Ensure that you run the command before the UD Agent runs the first time.

5. Results

When you activate the Infrastructure activity, the Data Flow Probe connects to the UD Agent installed on the remote machine.

To verify that the Data Flow Probe is able to communicate with the remote UD Agent, go to **Universal Discovery > Activity Discovery Status > Progress tab** and make sure that a UDA CI instance was discovered. For more information, see "[Zone-based Discovery View](#)" on [page 457](#).

The following events also occur as a result of installing the UD Agent:

- The UD Agent generates a Unique ID which is stored locally on the discovery node and in UCMDB as follows:
 - **Windows and UNIX.** For more information on where Unique ID is stored, see "[Universal Discovery Agent File Locations](#)" on [page 195](#).
 - **UCMDB.** Stored in the `ud_unique_id` attribute of Node CI.

For more information on Unique ID, see "[Universal Discovery Agent Overview](#)" on [page 163](#).

- Software Identification Tag files are created and stored on the discovery node. For more information about Software Identification Tags, see "[Hardware and Software Recognition](#)" on [page 532](#).

How to Install Universal Discovery Agent to Run Under a Non-Root Account on UNIX

This task describes how to install the UD Agent to run under a non-root account on UNIX systems.

1. Go to **Data Flow Management > Universal Discovery > Zone-based Discovery**, and select a Management Zone or create a new one.
2. In the Infrastructure Discovery activity, in the Define Credentials page, ensure that SSH and Universal Discovery protocol credentials are defined, as follows:
 - **SSH protocol:**
 - In the **User Name** and **Password** fields, define credentials for a non-root user for connecting to the host through the SSH network protocol.
 - In the Privileged Command Execution Properties area, define details for the Sudo prefixed command execution:
 - For the Policy, select **Sudo-like**.
 - For the Mode, select **Sudo**.
 - In the **sudo paths** field, make sure to include the full path to the sudo command on the remote machine. If the path is different on different computers/operating systems, you should provide multiple paths, separated by commas.
 - Enter the **sudo commands**. Ensure that the **agentinstall.sh** and **nohup** commands are included among these commands.
 - **Universal Discovery protocol:**
 - In the **sudo paths** field, ensure that the sudo paths defined for the SSH protocol above are also included.
 - In the **sudo commands** field, ensure that the sudo commands defined for the SSH protocol above are also included. Ensure that the **agentinstall.sh** and **nohup** commands are included among these commands.
3. On the Universal Discovery Agent Deployment page:
 - a. Select the deployment option: **Install** or **Update**.
 - b. Clear the **Install UD Agent to run under the root account on UNIX machines** option.

Note:

- After installing the UD Agent under a non-root account, the SSH credential used to install the agent must be kept in UCMDB because this credential is used to retrieve the password for the sudo command.

If, for whatever reason, the SSH credential was removed and created again, the Host Connection by Shell job must be rerun on the relevant triggers so that the other jobs can run sudo commands successfully.

- The Universal Discovery Agent will be run on the remote machine under the credential that was used for SSH in step 2.

How to Configure Call Home

This task describes how to configure the Call Home feature.

1. Configure the parameters

Call Home is configured depending on the method you use to perform deployment and installation of discovery resources.

- **Infrastructure Discovery Activity**

Configure Call Home parameters on the Agent Deployment page of the Infrastructure Discovery Activity. For details, see the *Universal CMDB Discovery and Integrations Content Guide*.

- **Manual**

If you manually deploy discovery packages, include parameters according to the target platform of your discovery nodes:

- **Windows**

- **Unattended.** For details on available parameters, see "[Universal Discovery Resources for Windows](#)" on page 189 and "[Agent Installation Wizard](#)" on page 183.
- **Attended.** For details on how to configure, see "[Agent Installation Wizard](#)" on page 183.
- **UNIX.** For details on available parameters, see "[Universal Discovery Resources for UNIX](#)" on page 191.

2. Results

- If you use the activity to configure Call Home, verify that you see configuration values on the **Summary** page of the **Infrastructure Discovery** activity. Then, verify the activity ran successfully by viewing the results summary in **Data Flow Management > Universal Discovery > Zone-based Discovery**, and select the **Progress** tab. For more information, see ["Zone-based Discovery View" on page 457](#).
- If you use manual methods to configure Call Home, see the section that describes the traffic case in ["Call Home Overview" on page 167](#).

How to Enable Changing the Default Port Number for Call Home

The Universal Discovery Agent Call Home feature uses the default port number 80 for communicating with the Data Flow Probe. However, in some organizations, port 80 might be blocked internally for security reasons.

This task describes how to enable changing the default port number for the Call Home feature to any other available port number.


1. Configure the **DataFlowProbe.properties** file

- a. On the Data Flow Probe, locate the **DataFlowProbe.properties** and **DataFlowProbeOverride.properties** files in the `C:\hp\UCMDB\DataFlowProbe\conf` folder and open them using a text editor.
- b. Locate the following line in **DataFlowProbe.properties** and copy it to **DataFlowProbeOverride.properties** (if does not exist):

```
appilog.agent.callhome.port = 80
```

- c. Change the port number value in **DataFlowProbeOverride.properties** to any other available port number.
- d. Save the file.
- e. Restart the Data Flow Probe.

Note: Starting with version 10.31, if you want to edit or update the properties in the **DataFlowProbe.properties** file, it is highly recommended that you to open the **DataFlowProbeOverride.properties** file in a text editor instead and add the updated properties into it. Otherwise your changes will be overridden by the settings (if exist) in **DataFlowProbeOverride.properties** after you restart the Probe, as the probe always loads the **DataFlowProbeOverride.properties** file first at probe startup, and then the OOTB **DataFlowProbe.properties** file.



2. Update the new port number on the Universal Discovery Agent Deployment page
 - a. Log in to the UCMDB Server, and go to **Data Flow Management > Universal Discovery > Zone-Based Discovery**.
 - b. From the navigation tree, select an existing Infrastructure Discovery activity and click **Edit**  or create a new Infrastructure Discovery activity.
 - c. In the New/Edit Infrastructure Discovery Activity dialog, go to the Universal Discovery Agent Deployment page.
 - d. In the **Primary Call Home Probe Address** or **Secondary Call Home Probe Address** field, update the port number with the new value you just specified in [step 1](#).
 - e. Click **Finish**.

For more details, see the "Universal Discovery Agent Deployment Page" section in the *HPE UCMDB Discovery and Integrations Content Guide - Discovery Activities*.

How to Specify Data and Temp Folder Locations when Installing or Updating the Universal Discovery Agent for UNIX

This task describes how to specify the location of data folders and temporary folders when installing and updating the Universal Discovery Agent on UNIX discovery nodes only.

1. Edit the XML file

- a. Locate the **AgentConfigurationbyPlatform.xml** file. To do this, choose from the following options:
 - **Data Flow Management > Universal Discovery > Discovery Modules/Jobs**, expand **Tools and Samples**, expand **Universal Discovery Agent Management** and select a job. Under the Properties tab select **AgentConfigurationbyPlatform.xml** and click **Edit** . The script editor opens.
 - **Data Flow Management > Adapter Management**, expand **Universal Discovery Agent Management**, expand **Configuration Files** and select **AgentConfigurationbyPlatform.xml**. The script editor opens.
- b. In the Script Editor, click **Find Text**  to open the Find Text dialog box. Find the **agent-install-data-folder** and **agent-install-temp-folder** parameters. Replace the **DEFAULT** value with the new value for the parameters you want to modify.

For more information on the Find Text dialog box, see ["Find Text Dialog Box" on page 273](#).

2. Results

The new values for the parameters that you modified are used when the Install UD Agent or the Update UD Agent job runs.

How to Completely Uninstall the Universal Discovery Agent

This task describes how to completely uninstall the Universal Discovery Agent and all its associated files. A complete uninstall differs from a default, or normal uninstall which retains certain files.

Note:

- Perform this task only when you will not re-install the Universal Discovery Agent.
- Configuration data files will be removed. This action cannot be undone.
- If you re-install the Universal Discovery Agent after you perform this task, reconciliation issues may occur due to the removal of the file that contains the Unique ID of the previous instance of

Universal Discovery Agent. As a result, you may notice duplicate Node CIs after inventory discovery runs.

- This task can also be performed manually. For more information, see ["Agent Installation User Interface" on the next page.](#)

1. Prerequisites

Ensure the UCMDB server is running.

2. Enable the parameter

- a. In **UCMDB**, go to **Data Flow Management > Universal Discovery > Discovery Modules/Jobs** tab.
- b. In the Discovery Modules tree, select **Tools and Samples > UD Agent Management**.
- c. Click the Properties tab and select **Uninstall UD Agent**. In the Parameters pane, perform the following:
 - i. Select the Override check box for the **RemoveAgentData** parameter.
 - ii. Click the corresponding cell in the Value column and set the value by typing **True**.

3. Results

The Universal Discovery Agent is completely uninstalled the next time the job runs. To verify that all files were removed, see ["Universal Discovery Agent File Locations" on page 195.](#)

Agent Installation Wizard Overview

This MSI package is used in manual deployments of the Universal Discovery Agent for Windows computers only. It can be used for installing, uninstalling, upgrading, or repairing the Universal Discovery Agent. Additionally, you can enable and set the options for software utilization.

For more information about deployment methods for the Universal Discovery Agent, see ["Universal Discovery Agent Deployment" on page 164.](#)

For more information about the Agent Installation Wizard, see ["Agent Installation Wizard" on the next page.](#)

Agent Installation User Interface

This chapter includes:

Agent Installation Wizard 183

Agent Installation Wizard

Enables you to install and configure the Universal Discovery Agent on a discovery node that is running Windows.

To access	<ul style="list-style-type: none"> Export the MSI package from the Package Manager. After the resource is deployed, double click hp-ud-agent-win32-x86-<VersionNumber>.msi. For details about how to export the package, see How to Export a Package in the <i>Universal CMDB Administration Guide</i>.
Important Information	<ul style="list-style-type: none"> This MSI installer can be run on Windows computers only. Additionally, the Windows computer must be running Microsoft Installer version 2.0 or above. There are two operational modes that are available-Complete Installation mode or Software Utilization mode. The mode that you select determines which pages are displayed. If the Universal Discovery Agent is already installed on the computer, the wizard starts at the "Uninstall Options Page". For more information on using command line parameters to configure unattended deployments of Universal Discovery Agents, see "Universal Discovery Resources for Windows" on page 189.
Relevant tasks	"How to Install the Universal Discovery Agent Manually" on page 174
Wizard map	The Agent Installation Wizard contains: "Set Up Type Page" > "Agent Configuration for Complete Installation Page" > "Software Utilization Page" > "Uninstall Options Page" > "Uninstall Type Page"
See also	"Universal Discovery Agent Overview" on page 163

Set Up Type Page

Enables you to select a mode of operation for Universal Agent installation.

Important Information	The Windows computer must be running Microsoft Installer version 2.0 or later.
Wizard Map	The Agent Configuration Wizard contains: Set Up Type Page > "Agent Configuration for Complete Installation Page" > "Software Utilization Page" > "Uninstall Options Page" > "Uninstall Type Page"

User interface elements are described below:

UI Element (A–Z)	Description
Set Up Type	Select a mode of operation: <ul style="list-style-type: none"> • Complete Install. This is the default mode and suggested for most client type environments. Universal Discovery Agents are installed on the discovery nodes, and then the Data Flow Probe installs the Scanner on the discovery nodes. Scanner schedules and jobs are managed by the Data Flow Probe. • Software Utilization Only. Only the Software Utilization software is installed on the discovery node. For more information, see "Software Utilization" on page 704.

Agent Configuration for Complete Installation Page

Enables you to make configurations for the Universal Discovery Agent installation when you select the Complete Installation mode.

Important information	<ul style="list-style-type: none"> • The Windows computer must be running Microsoft Installer version 2.0 or later. • This page is displayed only if you selected Complete Installation on the Set Up Page.
Wizard map	The Agent Configuration Wizard contains: "Set Up Type Page" > Agent Configuration for Complete Installation Page > "Software Utilization Page" > "Uninstall Options Page" > "Uninstall Type Page"

UI Element	Description
Port	Select the port that you want to use for communication between the Universal Discovery Agent and the Data Flow Probe. Note: This port number should be the same as the port number you specified in the UD Protocol Parameters dialog box at Data Flow Management > Data

UI Element	Description
	<p>Flow Probe Setup > Domains and Probes > Domain > Credentials. Additionally, if you change this port number manually after installation, the new port number takes effect only after the Universal Discovery Agent is upgraded.</p>
<p>Time Out</p>	<p>Enter a value that sets a time out threshold. Measured in seconds.</p> <p>Note: This parameter is called Call Home Frequency in the Infrastructure Discovery activity.</p>
<p>Primary Call Home Probe Address</p>	<p>Enter a primary address for the Data Flow Probe server that you want the Universal Discovery Agent to contact for Call Home messages.</p> <p>Use one of the following formats:</p> <ul style="list-style-type: none"> • Hostname (For example: probehost) • IP Address (the call home port is 80) <ul style="list-style-type: none"> ◦ IPv4Address (For example: 10.11.12.13) ◦ IPv6Address (For example: 2010:836b:4179::836b:4179) • Full Path (the call home port is not 80) <ul style="list-style-type: none"> ◦ http://HostNameOrIPv4Address:Port/callhome (For example: http://probehost:<port_number>/callhome) ◦ http://[IPv6Address]:Port/callhome (For example: http://[2010:836b:4179::836b:4179]:<port_number>/callhome) <p>Note: Port 80 is used by default when no port number is specified. If port 80 is occupied, use a format that specifies a customer port.</p>
<p>Secondary Call Home Probe Address</p>	<p>Enter a secondary address for the Data Flow Probe server that you want the Universal Discovery Agent to contact for Call Home messages. See Primary Call Home Probe Address (above) for formatting information.</p>
<p>Certificate Path</p>	<p>Select a credential to use.</p> <p>For more information on exporting certificate files, see "Universal Discovery Agent Certificates" on page 166.</p> <p>Note: The path must be a folder that contains the asctrust.cert file and agentca.pem file.</p>

Software Utilization Page

Enables you to make configurations for the software utilization feature.

Important Information	The Windows computer must be running Microsoft Installer version 2.0 or later.
Wizard Map	The Agent Configuration Wizard contains: "Set Up Type Page" > "Agent Configuration for Complete Installation Page" > Software Utilization Page > "Uninstall Options Page" > "Uninstall Type Page"

UI Element (A–Z)	Description
Software Utilization	Select this option if you want to enable this feature. For more information, see "Software Utilization" on page 704 .
Software Utilization Period	Choose the range to retain the software utilization data: <ul style="list-style-type: none"> • 31 days • 90 days • 365 days

Uninstall Options Page

Enables you to select options for the uninstall operation.

Important Information	<ul style="list-style-type: none"> • The Windows computer must be running Microsoft Installer version 2.0 or later. • This page is available only if the Universal Discovery Agent is already installed on the computer.
Wizard Map	The Agent Configuration Wizard contains: "Set Up Type Page" on page 183 > "Agent Configuration for Complete Installation Page" on page 184 > "Software Utilization Page" above > Uninstall Options Page > "Uninstall Type Page" on the next page

UI Element	Description
Repair	Select this option if you want to install the installation files again.

UI Element	Description
	<p>Note: All configuration options are preserved.</p>
Remove	Select this option to remove the Universal Discovery Agent.

Uninstall Type Page

Enables you to select the type of uninstall operation.

Important Information	<ul style="list-style-type: none"> The Windows computer must be running Microsoft Installer version 2.0 or later. This page is available only if you selected Remove on the "Uninstall Options Page".
Wizard Map	<p>The Agent Configuration Wizard contains:</p> <p>"Set Up Type Page" > "Agent Configuration for Complete Installation Page" > "Software Utilization Page" > "Uninstall Options Page" > Uninstall Type Page</p>

UI Element	Description
Default	<p>Select this option if you want perform a typical uninstall operation that deletes agent executable files and configuration files.</p> <p>Note:</p> <ul style="list-style-type: none"> Use this option when upgrading the Universal Discovery Agent. The Universal Discovery Agent log and software utilization files are not deleted.
Complete	<p>Select this option if you want to perform a complete uninstall and remove most Universal Discovery Agent and scanner files.</p> <p>Note:</p> <ul style="list-style-type: none"> Use this option when you do not plan on installing the Universal Discovery Agent again. Temporary files that are associated with the scanner are not deleted.

Discovery Node Disk Requirements

The estimated minimum disk space requirements for a discovery node are as follows:

Type of Node	Universal Discovery Agent and Scanner	Inventory Data	Utilization Data
Desktop/Workstation/Laptop	25 MB	250 KB- 3 MB	5-10 MB
Servers	25 MB	3-100 MB	50-100 MB

Note:

- The size of the **inventory data** heavily depends on the scanner configuration and the size of the file system on the target computer being inventoried. These are guideline figures for typical computers scanned using default scanner configuration. If the scanners are configured to collect information on all files (not just executables) or for computers hosting very large amount of files that are being scanned and the information on which is captured into the scan file, the space required could be larger.
- The size of the software **utilisation data** heavily depends on the amount of processes being executed and the length of the software utilization collection period. These are guideline figures, for computers hosting large amount of processes the amount of space required could be larger. Additionally, the value is estimated for one year of utilization data.

Universal Discovery Agent Installation Resources

The Discovery resources are files that support the deployment and installation of Universal Discovery Agents and Scanners. When using manual methods of deployment you can retrieve these resources by exporting them from **Administration > Package Manager > UDAgentManagement**. For details, see *How to Export a Package in the Universal CMDB Administration Guide*.

To export individual resource files, go to **Data Flow Management > Adapter Management > Resources Pane > UDAgentManagement > ExternalResources > UD_Agents**.

Tip: You do not have to export or include XML files in the discovery packages.

Universal Discovery resources are available for the following platforms:

- **Windows.** For details, see "[Universal Discovery Resources for Windows](#)" on the next page.
- **Mac.** For details, see "[Universal Discovery Resources for Mac](#)" on page 191.
- **UNIX.** For details, see "[Universal Discovery Resources for UNIX](#)" on page 191.

Universal Discovery Resources for Windows

Resources

Discovery resources for Windows are as follows:

Platform	Resource Name	Description
Windows (x86)	hp-ud-agent-win32-x86- <VersionNumber> .msi	This installer package is required for all installations.
	agentupgrade.cmd	Used when upgrading or migrating DDML agents to Universal Discovery Agents.

Parameters

You can use parameters in a command line interface to customize the Universal Discovery Agent installation, uninstallation, or upgrade as follows.

```
c:\AgentTest>msiexec <InstallOption> <Product.msi> /log <UPGRADELOGFILEPATH>
[CLEAN=ON] SETUPTYPE=Enterprise PORT=7738 TIMEOUT=900 CERTPATH=c:\ PERIOD=90
SOFTWAREUTILIZATION=ON URL0=15.178.179.124 URL1=15.178.179.125
URL2=15.178.179.126
```

Parameter Name	Description
InstallOption	Indicates the type of operation. The following options are supported: <ul style="list-style-type: none"> • /i: Installs the Universal Discovery Agent. • /x: Uninstalls the Universal Discovery Agent.
Product.msi	Indicates the product file name. For example, hp-ud-agent-win32-x86-10.20.000.xxx.msi
UPGRADELOGFILEPATH	Specify a path to save a log file. Note: <ul style="list-style-type: none"> • Only use with the agentupgrade.cmd script. • Use together with the /log switch.
CLEAN	Indicates the type of uninstall procedure. Most Universal Discovery

Parameter Name	Description
	<p>Agent files and scanner files are deleted.</p> <p>Note:</p> <ul style="list-style-type: none"> • This parameter must be used together with the uninstall option. • If you do not want to use this option, omit the parameter from the string.
SETUPTYPE	<p>Indicates the operational mode.</p> <p>Type Enterprise or Manual.</p> <p>Note: The manual parameter value is called "Software Utilization Plug In Only" in the Agent Installation Wizard User Interface.</p>
PORT	<p>Port number for Universal Discovery Agent to use for communication with Data Flow Probe.</p> <p>Type 2738 or 7738.</p> <p>Note: The default value is 2738. If you change this port number manually after installation, the new port number takes effect only after the Universal Discovery Agent is restarted.</p>
TIMEOUT	<p>Frequency that the Universal Discovery Agent contacts the Data Flow Probe when the Universal Agent sends Call Home messages.</p> <p>Measured in seconds.</p> <p>Default is 86400 seconds.</p> <p>Note: This parameter is called Call Home Frequency in the Infrastructure Discovery activity.</p>
CERTPATH	<p>Path to install certificate files.</p> <p>Default is the working directory.</p>
PERIOD	<p>Number of days to retain software utilization data.</p> <p>Default is 365 days.</p>
SOFTWAREUTILIZATION	<p>Enable or disable Software Utilization plug in.</p> <p>Use "ON" to enable and "OFF" to disable.</p> <p>Default is "OFF".</p>
URL0 URL1 URL2	<p>IP address for Data Flow Probe that is used for Call Home messages.</p>

Universal Discovery Agent Error Codes

For error codes that may be returned when using installation or upgrade packages, see [http://msdn.microsoft.com/en-us/library/windows/desktop/aa376931\(v=vs.85\).aspx](http://msdn.microsoft.com/en-us/library/windows/desktop/aa376931(v=vs.85).aspx).

Universal Discovery Resources for Mac

Discovery resources for Mac are as follows:

Platform	Resource Name
Mac OS X (x86)	hp-ud-agent-macosx-x86.dmg

Universal Discovery Resources for UNIX

Resources

The following script files are available for manual agent installations and upgrades:

Platform	Resource Name	Description
UNIX	agentinstall.sh	<ul style="list-style-type: none">• Installs the Universal Discovery Agent.• Replaces the non-native version of the UD Agent with a version that is packaged in the native operating system version of the discovery node.
	agentupgrade.sh	Upgrades the DDMI agent to a Universal Discovery agent. However, this version of the Universal Discovery agent is not packaged in the native operating system version of the discovery node.

These files are available in the **Package Manager**. For more information on exporting resources, see How to Export a Package in the *Universal CMDB Administration Guide*.

Additionally, discovery resources for UNIX and the UNIX variants that are also available in the **Package Manager** are as follows:

Operating System	Platform	File Name
HP-UX	ia64	hp-ud-agent-hpux-ia64.depot
	HPPA	hp-ud-agent-hpux-hppa.depot
Linux (Red Hat, SUSE, CentOS, Oracle)	x86,x64	hp-ud-agent-linux-x86.rpm
Linux (Ubuntu)	x86,x64	hp-ud-agent-linux-x86.deb
AIX	POWER	hp-ud-agent-aix-ppc.bff
Solaris	x86	hp-ud-agent-solaris-x86.i86pc
	SPARC	hp-ud-agent-solaris-sparc.sparc
Mac OS X	x86	hp-ud-agent-macosx-x86.dmg

Parameters

You can use parameters in a command line interface to customize the discovery installation as follows:

```
filename [--help] [--url0 ipaddress] [--url1 ipaddress] [--url2 ipaddress] [--port number] [--timeout seconds] [--cert path] [--usage] [--softwareutilization] [--softwareutilizationonly] [--period days] [--home path] [--upgrade] [--uninstall] [--clean] [--temp] [--user] [--group] packagename
--isnative
```

where:

Parameter Name	Description
cert	Path to install certificate files. Default: Working directory
clean	Specifies a type of uninstall procedure. Most Universal Discovery Agent files and scanner files are deleted. Note: This parameter can only be used together with the uninstall and home parameters.
filename	The name of the installation file. Note: <ul style="list-style-type: none"> This is a mandatory parameter. The filename is usually agentinstall.sh.

Parameter Name	Description
group	<p>Specifies the group name for the user account that you want to run the Universal Discovery Agent under.</p> <p>Note: Use this parameter together with the user parameter.</p>
help	Displays help messages.
home	<p>Directory that contains the Universal Discovery Agent log and the software utilization data files.</p> <p>Default: HOME directory</p>
packagename	<p>Full path for the package installation file.</p> <p>Default: Working directory</p> <p>Note: This parameter is required when installing or upgrading the Universal Discovery Agent.</p>
period	<p>Number of days to retain software utilization data.</p> <p>Default: 365 days</p>
port	<p>Port number for the Universal Discovery Agent to use for communication with the Data Flow Probe.</p> <p>Type 2738 or 7738</p> <p>Default: 2738</p> <p>Note: If you change this port number manually after installation, the new port number takes effect only after the Universal Discovery Agent is restarted.</p>
softwareutilization	Enables software utilization.
softwareutilizationonly	<p>Enables the Software Utilization plug-in only.</p> <p>Note:</p> <ul style="list-style-type: none"> The Universal Discovery Agent is disabled. This parameter is supported only when installing the Universal Discovery Agent manually.
temp	<p>Directory that contains Universal Discovery Agent and scanner temporary files.</p> <p>Default: \$TEMP directory.</p>
timeout	Frequency (in seconds) that the Universal Discovery Agent contacts the

Parameter Name	Description
	Data Flow Probe for Call Home. Default: 86400 seconds
uninstall	Uninstalls the Universal Discovery Agent. Note: When you use this parameter: <ul style="list-style-type: none"> • All parameters except the clean parameter are ignored. • The filename parameter is required.
upgrade	Upgrades the Universal Discovery Agent.
url0 url1 url2	IP address for Data Flow Probe that is used for Call Home messages.
usage	Displays help messages. Note: This parameter provides the same information as the help parameter.
user	The user account that is used to start up the Universal Discovery Agent.
isnative	Returns whether a native or non-native Universal Discovery Agent is installed.

Universal Discovery Agent Error Codes

The following error codes may be returned when using installation or upgrade scripts as follows:

Error Code	Description
1	General error
2	Wrong parameter
3	Not root user
4	File creation error
5	Wrong platform
6	Install package error
7	Directory missing
8	File missing
9	File not executable

Error Code	Description
10	Link startup script error
11	Startup script error
12	Universal Discovery Agent is already installed Note: Applicable only when performing an installation operation.
13	System package installer error
14	Run agent with non-root user error
15	The DDMI agent is installed.

Universal Discovery Agent File Locations

Universal Discovery Agents and supporting files are installed on the discovery node as follows:

Windows

Platform	Installation Files	Data/Utilization Data Files	Unique ID
x86	program files\hewlett-packard\discovery agent	<AgentServiceData>\Hewlett-Packard\Universal Discovery\Data\Perf where <AgentServiceData> is the location of the application data directory for the profile that is used by the UD Agent service. By default, <AgentServiceData> refers to the following if Windows is installed on C drive: <ul style="list-style-type: none"> • XP/Server 2003: C:\Documents and Settings\LocalService\Application Data • Vista and above: C:\Windows\system32\config\systemprofile\AppData\Roaming 	HKEY_LOCAL_MACHINE\SOFTWARE\Hewlett-Packard\Universal Discovery\V1\Options\UD_UNIQUE_ID
x64	program files (x86)\hewl	C:\Windows\SysWOW64\config\system profile\AppData\Roaming\Hewlett-	HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Hewlett-

Platform	Installation Files	Data/Utilization Data Files	Unique ID
	ett-packard\discovery agent	Packard\Universal Discovery\Data\Perf	Packard\Universal Discovery\V1\Options\UD_UNIQUE_ID.

Note:

- Certificate files are contained in the same location as program files. For more information, see ["Universal Discovery Agent Certificates" on page 166.](#)
- The Perf subdirectory contains most of the utilization data. This applies to all platforms listed.

UNIX

Platform	Installation Files	Data Files	
		Utilization Data Files	Unique ID
Linux /Solaris/HP-UX/Unix	/opt/HP/Discovery	\$HOME/.discagnt/Perf	UD_UNIQUE_ID entry in \$HOME/.discagnt/aioptionrc
Mac OS X (x86)	/Library/StartupItems/HPDiscoveryAgent	\$HOME/.discagnt/Perf	
AIX	/usr/lpp/HP/Discovery	\$HOME/.discagnt/Perf	

Note:

- Certificate files are contained in the same location as program files. For more information, see ["Universal Discovery Agent Certificates" on page 166.](#)
- The Perf subdirectory contains most of the utilization data. This applies to all platforms listed.
- "\$HOME" refers to the home directory of the account that runs the Universal Discovery Agent.
- You can modify the Universal Discovery Agent log and software utilization data files location when you use the **installagent.sh** script. For more information, see ["Universal Discovery Resources for UNIX" on page 191.](#)

Software Identification Tags

Tag File Name

When you install the Universal Discovery Agent, a Software Identification Tag file is created and named as follows:

Agent Deployment Mode	File Name
Complete Install	regid.1986-04.com.hp_UD-AgentComplete-<VersionNumber>.swidtag
Software Utilization	regid.1986-04.com.hp_UD-AgentSoftwareUtilizationOnly-<VersionNumber>.swidtag

For more information on the deployment modes for the Universal Discovery Agent, see ["Universal Discovery Agent Overview" on page 163](#).

Tag File Location

Operating system vendors can specify where software identification tags are located. If the vendor does not specify a location, software identification tags may be stored as follows:

Platform	Version	Local File Location	Global File Location
Apple Macintosh OS X	Leopard	/Library/StartupItems /HPDiscoveryAgent	/Library/Application Support/regid.1986-04.com.hp
	Prior to Leopard		/Applications /HPDiscoveryAgent.app /Contents
UNIX and Linux (Excluding AIX)		/opt/HP/Discovery	/usr/share/regid.1986-04.com.hp/
Windows	XP,2000,2003	<ul style="list-style-type: none"> (x32): C:\Program Files\Hewlett-Packard\Discovery Agent (x64): C:\Program Files 	%AllUsersProfile%\Application Data\regid.1986-04.com.hp

Platform	Version	Local File Location	Global File Location
Windows	Vista, Server 2008 and 2012	(x86)\Hewlett-Packard\Discovery Agent	%Program Data%\regid.1986-04.com.hp
AIX		/usr/lpp/HP/Discovery	/usr/share/regid.1986-04.com.hp/

Software Identification Tag Attributes

The following attributes are contained in scan files if Software Identification Tags are enabled during discovery:

Field Name	Attribute Name	Description
Entitlement_required_indicator	hwOSSoftwareIdTagEntitlementRequiredIndicator	Indicates if an entitlement must match up against this software in order for a successful software reconciliation to occur.
product_title	hwOSSoftwareIdTagProductTitle	Name of software as assigned by the software creator.
product_version	hwOSSoftwareIdTagProductVersionName, hwOSSoftwareIdTagProductVersionNumber	Textual and numeric version of the software.
software_creator	hwOSSoftwareIdTagSoftwareCreatorName, hwOSSoftwareIdTagSoftwareCreatorRegid	Software creator that produced the software package, and the creator's domain.
software_licensor	hwOSSoftwareIdTagSoftwareLicensorName, hwOSSoftwareIdTagSoftwareLicensorDomain	Software licensor that owns the copyright for the software package, and the licensor's domain.
software_id	hwOSSoftwareIdTagSoftwareUniqueid, hwOSSoftwareIdTagSoftwareIdCreatorDomain	Unique ID of the product and the domain name of the tag provider.
tag_creator	hwOSSoftwareIdTagTagCreatorName, hwOSSoftwareIdTagTagCreatorDomain	Name of the tag creator, and the tag creator's domain name.

Field Name	Attribute Name	Description
tag file path	hwOSSoftwareIdTagTagFilePath	<p>Location of the tag file. If the file is located at the root of the application's installation directory, this field will indicate the installation directory of the application.</p> <p>Tip: This information may be useful for application teaching. For more information, see "Application Teaching" on page 527.</p>
license linkage	hwOSSoftwareIdTagLicenseLinkageActivationStatus	<p>Licensing level that a software licensor uses to track software status. Every software licensor may have a different set of values.</p> <p>Information may include the following:</p> <ul style="list-style-type: none"> • Trial. Indicates that the software is in a trial mode and this value may include the number of days the trial mode is valid, or that the trial has expired. • Serialized. Indicates that the software user has entered a valid serial number during the installation process, however, the software is not activated. • Fully Licensed. Indicates that the product is activated. • Unlicensed. Indicates that the software is running in a limited mode. Software can enter into this state by one or more of the following:

Field Name	Attribute Name	Description
		<ul style="list-style-type: none"> a. A trial period has expired. b. A time-based license has expired. c. Software package contained a serial number, however, the software package was not activated in the given timeframe.
	hwOSSoftwareIdTagLicenseLinkageChannelType	<p>Indicates the channel the software was targeted for. Every software licensor may have a different set of values.</p> <p>Information may include the following:</p> <ul style="list-style-type: none"> • Volume. Targeted for volume consumption. • Retail. Target for the retail channel. • OEM. Targeted for the OEM channel. • Academic. Targeted for the education or academic channel.
	hwOSSoftwareIdTagLicenseLinkageCustomerType	<p>Identifies the target customer of the software. Every software licensor may have a different set of values.</p> <p>Information may include the following:</p> <ul style="list-style-type: none"> • Government. Targeted for government customers. • Corporate. Targeted for corporate customers. • Educational. Targeted

Field Name	Attribute Name	Description
		for education or academic customers. <ul style="list-style-type: none">• Retail. Targeted for retail customers.
serial number	hwOSSoftwareIdTagSerialNumber	Unique identifier that may be represented as a combination of numbers, letters, or symbols. The serial number for the software product is a commonly used unique number assigned for identification of a particular title and purchase. Note: The value might be the serial number that is run through a one-way hash encryption scheme.

For more information about enabling discovery of Software Identification Tags, see "[Hardware Data Page](#)" on page 609.

Chapter 5: Scanner Scheduler

This chapter includes:

Scanner Scheduler Overview	202
How to Deploy the Scanner Scheduler	202
Scanner Scheduler Resources	205

Scanner Scheduler Overview

Scanner Scheduler is often used together with Store and Forward servers when manually deploying scanners. The Scanner Scheduler enables you to download and update scanners from the Data Flow Probe to discovery nodes, and you can also specify when a scanner runs on discovery nodes. Using this feature ensures scanners are automatically updated, and it also ensures uninterrupted scanning when connectivity or firewall issues prevent the Data Flow Probe from initiating scan jobs on discovery nodes.

Additionally, you can centrally configure and manage schedules by using a configuration (.ini) file that is stored on a remote server. The scanner, using a third party data transfer program called Curl, periodically downloads this remote configuration file according to a download schedule that you configure. Updates that are contained in the remote configuration file overwrite the local configuration file.

Deploy the Scanner Scheduler manually using any remote access technology or third party distribution tool. The Scanner Scheduler runs as a service on Windows or as a detached process on UNIX.

To install the Scanner Scheduler, see ["How to Deploy the Scanner Scheduler" below](#).

To see resources for the Scanner Scheduler, see ["Scanner Scheduler Resources" on page 205](#).

To see support information, see the Supported Content section of the *Universal CMDB Discovery and Integrations Content Guide*.

How to Deploy the Scanner Scheduler

This task describes recommended workflows for deploying the Scanner Scheduler.

Installing the Scanner Scheduler

This task includes the following steps:

- ["Prerequisites" below](#)
- ["Copy the installation package for the Scanner Scheduler to the discovery node" below](#)
- ["Install the Scanner Scheduler" below](#)
- ["Generate scanner- Optional" on the next page](#)
- ["Customize download and running schedules" on the next page](#)
- ["Results" on the next page](#)

1. Prerequisites

Ensure that UCMDB is installed.

2. Copy the installation package for the Scanner Scheduler to the discovery node

Note: Ensure that you distribute or copy the installation files that are appropriate to the platform of the discovery node.

Windows:

- a. On the UCMDB server, copy the MSI installation package from the following location to your local computer:

UCMDB\UCMDBServer\tools\InventoryDiscovery\ScannerScheduler

- b. Copy the MSI installation package to the discovery node using any manual method or remote access technology.

UNIX:

From the UCMDB installation media, copy the file that is appropriate to your discovery node platform to your local computer. Additionally, copy the **scannerschedulerinstall** installation script file.

Tip: The file name of the resources file indicates the platform.

3. Install the Scanner Scheduler

Windows:

For attended installations, double-click or execute the MSI file. For unattended, or silent installations, run the following command: **msiexec /quiet /I <MSIFilename>**

Note: To debug the installation, use the following command: `/L*v <FullPathToLogFile>`.

Log files are stored in the same location as scan files. For more information on scan file locations, see "[Scanner Options Page](#)" on page 635.

UNIX:

Run the following command with root privileges: `scannerschedulerinstall hp-ud-scanner-scheduler-<platform>-10.20.000<buildnumber>.<packageformat>`

4. Generate scanner- Optional

Note: If you do not want to update the scanners that are deployed to discovery nodes, skip this step.

If you want to use Scanner Scheduler to download and update scanners to discovery nodes, use the Scanner Generator wizard to generate a scanner. For more information, see "[Scanner Generator Wizard](#)" on page 605.

5. Customize download and running schedules

Customize the `config.ini` file to specify schedules for running scanners, to download centrally-managed configuration files using Curl, and to download scanners to discovery nodes. For more information, see "[Scanner Scheduler Resources](#)" on the next page.

6. Results

The Scanner Scheduler starts automatically when the discovery node is started.

- The scanner downloads and runs according to the parameter values that are specified in the `config.ini` file.

Upgrade the Scanner Scheduler

Windows:

From the Control Panel, uninstall the Scanner Scheduler. Then, install the Scanner Scheduler normally.

UNIX:

From a command line, use the `upgrade` parameter. For example, `scannerschedulerinstall --upgrade hp-ud-scanner-scheduler-<platform>-10.20.000<buildnumber>.<packageformat>`

Uninstall the Scanner Scheduler

Windows:

From the Control Panel, uninstall the Scanner Scheduler.

UNIX:

From a command line, use the **uninstall** parameter. For example, **scannerschedulereinstall --uninstall**

For more information on Scanner Scheduler, see "[Scanner Scheduler Overview](#)" on page 202.

For more information on Scanner Scheduler operations and resources, see "[Scanner Scheduler Resources](#)" below.

Scanner Scheduler Resources

File Locations

The following table describes information about the Scanner Scheduler installation and log file locations.

The Curl program and the **config.tmp** file are located in the same directories as listed under the Installation Location column.

Platform	Installation Location	Log File Location
Windows 32-Bit	<p><ProgramFiles>\Hewlett-Packard\Universal Discovery\10.20\Scanner Scheduler</p> <p>Note:</p> <ul style="list-style-type: none"> This location can be configured by using the following command: INSTALLDIR=C:\ScannerScheduler The <ProgramFiles> environment variable is normally located at C:\Program Files 	<ALLUSERSPROFILE>\Hewlett-Packard\Universal Discovery
Windows 64-Bit	<p><ProgramFiles(x86)>\Hewlett-Packard\Universal Discovery\10.20\Scanner Scheduler</p> <p>Note:</p>	

Platform	Installation Location	Log File Location
	<ul style="list-style-type: none"> This location can be configured by using the following command: INSTALLDIR=C:\ScannerScheduler The <ProgramFiles(x86)> environment variable is normally located at C:\Program Files(x86) 	
UNIX	/opt/HP/ScannerScheduler	\$HOME/.discagnt directory
Mac	/Library/StartupItems/HPScannerScheduler	
AIX	/usr/lpp/HP/ScannerScheduler	

Configuration File Parameters

The **config.ini** file contains parameters for managing the running schedule of the scanner, the downloading schedule for the scanner, and for downloading a configuration file on a remote server. The parameters are as follows:

Configuration File Parameter	Description
Monday Tuesday Wednesday Thursday Friday Saturday Sunday	<p>For each day of the week, enter the range of hours you want your scheduled event to run. If you specify multiple time intervals, use commas to separate each interval. For example: 10:00-12:00,14:00-18:00</p> <p>Note: The 24-hour clock is used.</p>
FrequencyHours	<p>Indicates how frequently the scheduled event occurs. Assume you want to use a weekly interval for your scheduled event. In this scenario, set the value to 168.</p> <p>If this parameter is set to 0, scheduling is disabled.</p> <p>Note: This field is mandatory.</p>
RandomDelayMinutes	<p>Specifies a random delay to the start time for load balancing purposes. Assume that the scanner is scheduled to run at 9:00 and the random delay is 60 minutes. In this scenario, the scanner runs at a random point in time between 9:00 and 10:00.</p> <p>If this parameter is set to 0, no random delay is used.</p>

Configuration File Parameter	Description
CommandLine	<p>Enter a command to run the scanner, to run a program that will download the config.ini file from a remote server, or to download the scanner.</p> <ul style="list-style-type: none"> • The Scan section. Enter a command to run the scanner. If no path is specified, the Scanner Scheduler attempts to start the scanner from the same directory as the Scanner Scheduler executable is located. • The DownloadConfig section. Enter a command to run Curl, or any other data transfer tool, to download a remote config.ini file. Additionally, in the <RemoteConfigPath> parameter, enter a URL that specifies the location of the config.ini file that you want to download. <p>Note:</p> <ul style="list-style-type: none"> ◦ After the config.ini file is downloaded, the file is stored as config.tmp and then automatically converted to config.ini. ◦ The RemoteConfigPath parameter is mandatory. <ul style="list-style-type: none"> • The DownloadScanner section. In the <RemoteScannerPath> parameter, enter the path to the location where the scanner that you want to download is located. <p>Note: The scanner file name is scan.tmp after it is downloaded. However, you can change the file name in the ScannerFileName parameter.</p>
ScannerFileName	<p>In the <LocalScannerPath> parameter, enter the full file path to the local computer where you want to store the scanner file. The scanner file name is changed from scan.tmp to the file name specified in this parameter.</p> <p>Note: This parameter is mandatory.</p>

Windows Specific Resources

File name	Description
ScannerScheduler.exe	Executable file of the Scanner Scheduler service.

File name	Description
config.ini	Configuration file that contains parameters that manages the scanning schedule of the scanner. It also manages, together with a third party program, the download schedule of another config.ini file that is located on a remote server.
curl.exe	Executable file of Curl. This third party program can be used to download a new configuration file from a remote server.
libeay32.dll	OpenSSL DLL to enable Curl to work over HTTPS.
libssl32.dll	OpenSSL DLL to enable Curl to work over HTTPS.
curl-ca-bundle.crt	Root CA certificates to enable Curl to work over HTTPS.

UNIX Specific Resources

File Name	Description
bin/scansched	Executable file of the Scanner Scheduler service.
bin/config.ini	Configuration file that contains parameters that manage the scanning schedule of the scanner. The configuration file also manages, together with a third party program, the download schedule of another config.ini file that is located on a remote server.
bin/curl	Executable file of Curl. This third party program can be used to download a new configuration file from a remote server.
bin/curl-ca-bundle.crt	Root CA certificates to enable Curl to work over HTTPS.
discscannerscheduler	Script to manage the scanner scheduler. For more information about available parameters that you can use in this script, see " Scanner Scheduler Parameters (UNIX only) " below.

Scanner Scheduler Parameters (UNIX only)

To manage the Scanner Scheduler for nodes that are running UNIX, enter the following command:

discscannerscheduler <ParameterName>

where **<ParameterName>** is a placeholder for the parameter name specified as follows.

Note: Ensure that you run the command from the installation location.

Parameter Name	Description
start	Starts the Scanner Scheduler service.
stop	Stops the Scanner Scheduler service.
restart	Restarts the Scanner Scheduler service.
status	<p>Indicates running status information of the Scanner Scheduler service.</p> <ul style="list-style-type: none">• If the Scanner Scheduler is running, the following message is returned: "Universal Discovery Scanner scheduler (pid xxxx) is running."• If the Scanner Scheduler is not running, the following message is returned: "Universal Discovery Scanner scheduler stopped."

Chapter 6: Store and Forward

This chapter includes:

Store and Forward Overview	210
How to Install the Store and Forward Server	210
Store and Forward Installation Wizard	214
Store and Forward Resources	216
Store and Forward Commands	221

Store and Forward Overview

Store and Forward is a system that enables you to design flexible, secure, and resilient communication paths to move scan files through firewalls or other networking obstacles. Store and Forward works together with Scanner Scheduler to maintain clear, uninterrupted paths between scanners and the Data Flow Probe. For more information on Scanner Scheduler, see ["Scanner Scheduler Overview" on page 202](#).

Each Store and Forward server uses a configuration file to determine its behavior. Depending on the parameter values contained in the configuration file, a Store and Forward server may forward or route scan files through logical "channels" that map to directories on one or more "upstream provider" Store and Forward servers. The last Store and Forward server in the system is the Data Flow Probe. A web server that is installed together with the Store and Forward server continuously listens on a TCP port for incoming scan files. Store and Forward servers support resumed file transfer. Monitoring statistics for each Store and Forward server are available by accessing a web page that is hosted on each server.

To install the Store and Forward server, see ["How to Install the Store and Forward Server" below](#).

To see support information, refer to the *Universal CMDB Support Matrix* document.

How to Install the Store and Forward Server

This task describes how to install the Store and Forward server. Perform this task for each computer that you want to use as a Store and Forward server.

This task includes the following steps:

- ["Prerequisites" below](#)
- ["Copy the installation package" below](#)
- ["Install the Store and Forward server" below](#)
- ["Copy certificate files from upstream servers" on the next page](#)
- ["Configure the system behavior" on page 213](#)
- ["Results" on page 213](#)
- ["Additional operations" on page 213](#)

1. Prerequisites

- Scanners are deployed in Manual Deployment mode.
- Scanners are configured to save scan files offsite. For more information, see ["Scanner Options Page" on page 635](#).

2. Copy the installation package

Note: Ensure that you copy installation files that are appropriate to the platform of the computer that you want to install the Store and Forward server.

Windows:

From the UCMDB server, copy the MSI installation file from the following location to the computer that you want to install the Store and Forward server:

UCMDB\UCMDBServer\tools\InventoryDiscovery\StoreAndForward

Linux:

From the UCMDB installation DVD, copy the **hp-ud-store-and-forward-linux-x86-10.20.000.xxx.tar** installation file to the computer where you want to install the Store and Forward server.

3. Install the Store and Forward server

Windows:

- a. Double-click the MSI file. The main page of the installation wizard displays.
- b. Navigate through the wizard. For more information about the wizard, see ["Store and Forward Installation Wizard" on page 214](#).

Linux:

- a. Run the following command to decompress the archive file: **tar -xzf <FileName>.tar.gz**
- b. Run the following command to switch to root user if not logged in as root already: **su root**
- c. Run the following commands with root privileges to configure parameter values: **./configure**

Note: The installation directory must be the current directory when you run this command.

- d. Enter the following information when prompted:
 - i. The TCP port that you want to use for the Store and Forward server service. The default is **5005**.
 - ii. The username that you want to use to authenticate to the web server that is hosting the Store and Forward status page. The default is **hpud**.
 - iii. The password that you want to use together with the username to authenticate to the web server that is hosting the Store and Forward status page. This field is mandatory.
 - iv. The communication protocol that you want to use between Store and Forward servers. Enter **1** for HTTP (plain) or **2** for HTTPS (secure).
- e. Start the service by running the following command with root privileges: **/etc/init.d/hpudsaf start**

4. Copy certificate files from upstream servers

Note: This step is only applicable if the HTTPS (secure) communication protocol is used.

- a. Copy the **server.crt** files of each upstream server to the computer that you are installing the Store and Forward server. An upstream server is a server that you are forwarding scan files to. This file is stored in the **<DataDir>\Cert** directory. For Windows, **<DataDir>** is configured in "[Install the Store and Forward server](#)" on the previous page. For Linux, **<DataDir>** is the **data** folder in the directory where you installed the Store and Forward server in "[Install the Store and Forward server](#)" on the previous page.
- b. Rename each upstream server certificate file so that all files have unique names. For example, **server1.crt**, **server2.crt**.
- c. Concatenate all the certificate files from upstream servers into one file. Separate each upstream server file with plus (+) signs. To do this, run the following command with root privileges: **copy /b <server1.crt> + <server2.crt> + <server3.crt> trustedcerts.crt**. A file named **trustedcerts.crt** is created.

- d. Copy the **trustedcerts.crt** file to the **<DataDir>\Cert** directory of the computer that you are installing the Store and Forward server.

Note: If the host name of any upstream server changes, perform this step again.

5. Configure the system behavior

Update the **config.ini** file to control the behavior of the Store and Forward server.

- The **config.ini** file is contained in the following location:
 - **Windows:** The **conf** folder that is contained in the directory where you installed the Store and Forward server.
 - **Linux:** The **conf** folder that is contained in the directory where you installed the Store and Forward server.

To see parameters that are available to update, see ["Store and Forward Resources" on page 216](#).

Note: If you make changes to the configuration file, restart the Store and Forward server. For more information, see "Results" below.

6. Results

- The Store and Forward server service and the Apache web server service start automatically when the computer is started. For more information on names of services, see ["Store and Forward Resources" on page 216](#).
- To verify the system is operating as expected, go to the following web page on each Store and Forward server to view operating statistics:

http://<StoreAndForwardServer>:<port>/server_status.xml

Note: If the HTTPS communication protocol is used, type **HTTPS** instead of **HTTP**.

7. Additional operations

To throttle the upload bandwidth, perform the following:

- a. Locate the **http.conf** file in the installation folder where you installed the program files.
- b. Locate the following line: **safbwInputLimit 0**
- c. Change **0** to any non-zero integer to specify the maximum bandwidth (in kilobytes).

For more information on Store and Forward concepts, see ["Store and Forward Overview" on page 210](#).

For more information on Store and Forward operations and resources, see ["Store and Forward Resources"](#) on page 216.

For more information on Store and Forward commands, see ["Store and Forward Commands"](#) on page 221.

Store and Forward Installation Wizard

Enables you to install and configure the Store and Forward server on a computer that is running Windows.

To access	From the UCMDB installation media, copy the following file to your local computer and then double click to launch the wizard: Universal Discovery Store and Forward server (x86) 10.33.000.xxx.msi .
Important information	<ul style="list-style-type: none"> This MSI installer is used for Windows computers only. The Windows computer must be running Microsoft Installer version 2.0 or above.
Related Tasks	"How to Deploy the Scanner Scheduler" on page 202
See also	"Store and Forward Overview" on page 210
Wizard Map	"Destination Folder Page" below > "Data Files Page" on the next page > "Store and Forward Configuration Page" on the next page > "SSL Certificate Generation Page" on page 216

Destination Folder Page

Enables you to select a folder for the Store and Forward server program files.

Important Information	The Windows computer must be running Microsoft Installer version 2.0 or later.
Wizard Map	The "Store and Forward Installation Wizard" contains: Destination Folder Page > "Data Files Page" > "Store and Forward Configuration Page" > "SSL Certificate Generation Page"

UI Element (A–Z)	Description
Change	Click to browse to a folder that you want to contain the program files.

Data Files Page

Enables you to select a folder for the Store and Forward data files.

Important Information	The Windows computer must be running Microsoft Installer version 2.0 or later.
Wizard Map	The "Store and Forward Installation Wizard" contains: "Destination Folder Page" > Data Files Page > "Store and Forward Configuration Page" > "SSL Certificate Generation Page"

UI Element (A–Z)	Description
Change	Click to browse to a folder that you want to contain the data files.

Store and Forward Configuration Page

Enables you to make configurations for the Store and Forward server.

Important Information	The Windows computer must be running Microsoft Installer version 2.0 or later.
Wizard Map	The "Store and Forward Installation Wizard" contains: "Destination Folder Page" > "Data Files Page" > Store and Forward Configuration Page > "SSL Certificate Generation Page"

UI Element	Description
TCP Port	Type a port number that listens for incoming scan files from downstream servers. Default: 5005
User name	Type a user name to use to for the service. Default: hpud
Password	Type a password to use for the service.

UI Element	Description
	<p>Note: This is a mandatory field.</p>
Communication Protocol	<p>Select a communication protocol that you want to use as the transport mechanism when uploading scan files.</p> <ul style="list-style-type: none"> • HTTPS (secure) • HTTP (plain)

SSL Certificate Generation Page

Enables you to make configurations to the certificate file if HTTPS is selected as the communication protocol.

Important Information	The Windows computer must be running Microsoft Installer version 2.0 or later.
Wizard Map	<p>The "Store and Forward Installation Wizard" contains:</p> <p>"Destination Folder Page" > "Data Files Page" > "Store and Forward Configuration Page" > SSL Certificate Generation Page</p>

UI Element (A-Z)	Description
DNS Name	<p>Enter the full computer name of the computer that is running the Store and Forward server.</p> <p>For example, somehost.example.com</p>

Store and Forward Resources

Windows

By default, program files are installed in the following location:

<Program Files>\Hewlett-Packard\Universal Discovery\<VersionNumber>\Store and Forward

By default, data files, log files, and scan files that are in transit are stored in the following location:

<ALLUSERSPROFILE>\Application Data\Hewlett-Packard\Universal Discovery S&F

In addition, the following directories are created after installation.

Subdirectory	Description
bin	Contains the Apache web server executable files, DLL files, and the Store and Forward server executable files
conf	Contains the configuration files, including httpd.conf (the configuration file for the Apache web server) Note: The httpd.conf file contains parameters that control bandwidth throttling
modules	Contains the Apache web server modules
Logs	Contains the logs for the Apache web server and the Store and Forward server
Incoming	Contains incoming scan files
InProgress	Contains the files that the server is processing
Status	Contains status files
Resume	Contains scan files that are partially uploaded

The Windows service is registered with the following parameters:

Service attribute	Value
Apache Service Name	ovedApacheSF
Apache Display Name	Universal Discovery Store and Forward Web Server
Apache Startup Type	Automatic
Store and Forward Service Name	ovedStoreAndForward
Store and Forward Display Name	Universal Discovery Store and Forward Server
Store and Forward Startup Type	Automatic

Linux

The following directories are created in the installation folder after installation.

File name	Comment
bin	Contains the Apache web server executable files, DLL files, and the Store and Forward server executable files.
conf	Contains the configuration files, including httpd.conf (the configuration file for the Apache web server). Note: The httpd.conf file contains parameters that control bandwidth throttling.
data	Parent data directory.
data/Logs	Contains Apache web server and Store and Forward server log files.
data/Incoming	Contains incoming scan files.
data/InProgress	Contains the files that the server is processing.
data/Status	Contains status files.
data/Resume	Contains scan files that are partially uploaded.
modules	Contains the Apache web server modules.

The Linux service is registered with the following parameters:

Service attribute	Value
Linux Service Name	StoreNForward
Apache Service Name	httpd

Status Information XML File Printout

In addition to using web-based methods to access status file information, data that is contained in this file can also be accessed by external programs or scripts. The file resembles the following:

```
<?xml version="1.0" encoding="UTF-8"?>
<?xml-stylesheet type="text/xsl" href="server_status.xsl"?>
<StoreAndForwardStatus version="1.0">
<statusDirBytes>0</statusDirBytes>
<incomingDirBytes>0</incomingDirBytes>
<inProgressDirBytes>0</inProgressDirBytes>
<resumeDirBytes>0</resumeDirBytes>
```

```

<freeDiskSpaceBytes>50882215936</freeDiskSpaceBytes>
<numIncomingFiles>0</numIncomingFiles>
<numInProgressFiles>0</numInProgressFiles>
<numResumeFiles>0</numResumeFiles>
<modifiedTime>12/22/10 08:23:30</modifiedTime>
</StoreAndForwardStatus>

```

Configuration File

The structure of the **config.ini** file is as follows.

Section Name	Parameter Name	Description
Log	filterLevel	Type default or debug . When debug is specified, detailed logging is enabled.
	rotateSizeMB	Specifies the size of each log file. The Store and Forward server can store the log information in several log files.
	rotationFileCount	Specifies the number of log files to keep. When the parameter value is reached, the oldest log file is discarded.
[BaseDirectories]	dataDir	Specifies the location of the data directory. Normally, it is not necessary to modify this setting because it is configured automatically by the installer.
	incomingDir	Specifies the location of the Incoming directory. Normally, it is not necessary to modify this setting, as it is configured automatically by the installer.
[Channels]	channelX	Specifies the name for each channel. Channel names are used to name the top level directory of the Store and Forward server. The corresponding physical directory is created under the Incoming directory of the Store and Forward server.
[UpstreamProviders]	providerX	Specifies the URLs for upstream Store and Forward servers. The URL should include the HTTP username and password required to access the URL. When the HTTPS protocol is used, the host name of the Store and Forward server

Section Name	Parameter Name	Description
		<p>supplied in this URL must match the host name given during the installation of that Store and Forward server, as this host name is encoded in the HTTPS certificate.</p> <p>When configuring a Store and Forward server that is installed together with the Data Flow Probe, use the following configuration:</p> <p>This key specifies the full path to a local directory. In this case, the received file is copied to that directory, or moved if the channel is mapped to only one upstream provider. The only provider that is listed should be the incoming directory of the XML Enricher, as all files received by this Store and Forward server will be moved automatically to the Incoming directory of the XML Enricher.</p>
[ChannelMapping]	channelX	Specifies how the files arriving to this channel will be forwarded. One or more upstream Store and Forward servers from the [UpstreamProviders] section should be specified. Multiple servers are separated with commas.
[StatusPage]	updateFrequencyMins	<p>Specifies how frequently (in minutes) the status page is updated.</p> <p>The default is 20. If the setting is set to 0, the status page is not updated.</p>

Sample Configuration File

The following is a sample **config.ini** file that has two upstream Store and Forward servers configured, two channels, and three providers:

```
[Log]
filterLevel=default
rotateSizeMB=10
rotationFileCount=5

[BaseDirectories]
dataDir=C:\ProgramData\Hewlett-Packard\DDMI S&F\
incomingDir=C:\ProgramData\Hewlett-Packard\DDMI S&F\Incoming\
```

```

[Channels]
channel0=ddmi
channel1=hpca
[UpstreamProviders]
provider0=http://ddmi:ddm1passwd@ForwardS&Fserver1:5005/ddmi/
provider1=http://ddmi:ddm1passwd@ForwardS&Fserver2:5005/hpca/
provider2=http://ddmi:ddm1passwd@ForwardS&Fserver3>:5005/ddmi/
[ChannelMappings]
channel0=provider0,provider2
channel1=provider1
[StatusPage]
updateFrequencyMins=20

```

Store and Forward Commands

Commands that are available for the Store and Forward server service are as follows:

Windows

Description	Command
Restart	net start ovedStoreAndForward
Stop	net stop ovedStoreAndForward
Uninstall	Control Panel > Add/Remove Programs

Linux

Description	Command
Restart	/etc/init.d/hpudsaf restart
Stop	/etc/init.d/hpudsaf stop
Uninstall	1. /sbin/chkconfig --del

Description	Command
	hpudsaf 2. rm -rf /etc/init.d/hpudsaf

Part III: Adapter Management

Chapter 7: Adapter Configuration

This chapter includes:

Identifying Running Software by Processes	224
Automatically Deleted CIs and Relationships and Candidates for Deletion CIs	226
How to Configure Adapter Settings	227
How to Define the Owner Tenant Adapter Parameter	228
How to Configure Full Population Run	228
How to Configure Global Probe Result Filtering	229
How to Configure CI Aging Settings	234
How to Define CITs to be Deleted by Java-based Population Adapters	235
How to Attach Discovery Documentation to a Discovery Package	235
How to Attach a Readme to a Discovery Package	236
How to View Discovery Resource History	237
How to Create and Configure Mapping Files Using the Visual Mapping Tool	239
Pre/Post-Scan Script Editor	251
Pre-Scan and Post-Scan Scripts	251
Adapter Management User Interface	252
Internal Configuration Files	295

Identifying Running Software by Processes

An application is identified by the existence of one or more running processes which are defined by their names and by command line (optional).

A process can be optionally marked as a key process or as a main process.

An application is identified if the following holds true:

- At least one process was found.
- All processes that are marked as key processes exist.

If an application is identified, a result RunningSoftware CI is created for the application obeying the following rules:

- If none of the processes is marked as a main process, a single RunningSoftware CI will be created, linked to all discovered processes by dependency relationships.
- If there are processes that are marked as main processes, a RunningSoftware CI will be created for each instance of these main processes.

For example, assume that rules are defined for the identification of two applications, **application_a** and **application_b**:

- **application_a** is identified by **proc.exe** and **unique_proc_a.exe**.
- **application_b** is identified by **proc.exe** and **unique_proc_b.exe**.

Say that **proc.exe** is found but none of its processes are marked as key or main processes. In this case, **RunningSoftware** CIs are created for both **application_a** and **application_b**. These CIs are linked by a dependency relationship to the same process (that is, **proc.exe**).

Assume too that **unique_proc_a.exe** and **unique_proc_b.exe** are marked as key processes:

- If the **proc.exe** process only is discovered, a **RunningSoftware** CI is not created.
- If **unique_proc_a.exe** is discovered, **RunningSoftware** CIs are created for **application_a** linked by a dependency link to **unique_proc_a.exe**. If in addition, **proc.exe** is discovered, it is linked to the same CI. The same holds for **application_b**.

Assume that two instances of **unique_proc_a.exe** are discovered:

- If the process is not marked as a main process, a single **RunningSoftware** CI is created for **application_a** linked to both processes.
- If the process is marked as a main process, two separate **RunningSoftware** CIs are created for **application_a**.

For details on the key field in the Software Identification Rule Editor dialog box, see "[Identifying Processes](#)" on page 291.

Automatically Deleted CIs and Relationships and Candidates for Deletion CIs

During discovery, the Data Flow Probe compares CIs found during the previous, successful job invocation with those found during the current job invocation. A missing component, such as a disk or software, is assumed to have been removed from the system, and its CI is **automatically deleted** from the Probe's database.

By default, the Data Flow Probe deletes CI instances of certain CITs, for example, the current configuration for the Host Resources and Host Applications jobs (snmp: file system, installed software, osuser, service).

DFM enables you to customize which CI instances the Probe should automatically delete for specific jobs.

You can also mark a CIT as a **candidate for deletion**. In this case, if no CI instances of that CIT are discovered, the CIT is isolated rather than automatically deleted. Carefully choose the CITs that are to be candidates for deletion. For example, process CITs are not good candidates because they often shut down and start up again and, as a result, may be deleted at every invocation.

Example of Automatic Deletion

During the previous job invocation, the Data Flow Probe ran the **Host Resources by WMI** job and discovered a host with **disks a, b, c, and d**. During the current job invocation, the Probe discovers **disks a, b, and c**, compares this result with the previous result. Since it finds that **disk d** is missing, it deletes the CI for **disk d**.

Note:

- The Data Flow Probe does not wait for the aging mechanism to perform the calculation, but immediately sends a deletion request to the server. For details about aging, see "The Aging Mechanism Overview" in the *Universal CMDB Administration Guide*.
- The change is defined on the job's adapter.
- If discovery fails and errors occur, objects are sent for deletion according to how the results are managed. For details, see "[Adapter Configuration Tab](#)" on page 259.
- You can use this procedure to delete relationships, too. For example, the **containment** relationship is used between a node and an IP address. A laptop machine is allocated a

different IP address very often. By deleting the relationship, you prevent the accumulation of old IP addresses attached to this node.

- You can view deleted CIs in the Probe log and in the **Deleted** column in the Discovery Results pane. For details, see ["Data Flow Probe Log Files" on page 99](#) and ["Discovery Results Tab/Pane" on page 678](#).

For details on configuring automatic deletion, see ["How to Configure the Data Flow Probe to Automatically Delete CIs" on page 72](#).

How to Configure Adapter Settings

You should edit adapter and XML files in one of the following ways:

Change the adapter's definitions in the Adapter Management module

Note: This method is recommended.

1. Navigate to **Data Flow Management > Adapter Management**.
2. In the Resources pane, select the adapter file in the **Packages > <package name> > Adapters** folder.
3. Do one of the following:
 - To edit general adapter settings, use the **Adapter Definition** and **Adapter Configuration** tabs. For details, see ["Adapter Definition Tab" on page 253](#) and ["Adapter Configuration Tab" on page 259](#).
 - To define specific settings for the selected adapter, right-click the adapter and select **Edit Adapter Source** from the shortcut menu.

Edit the adapter package and redeploy it using the Package Manager

Export the package to your local drive, edit the package and redeploy it. For information see, "How to Export a Package" and "How to Deploy a Package" in the *Universal CMDB Administration Guide*.

How to Define the Owner Tenant Adapter Parameter

In multi-tenancy environments, all discovered CIs/relationships are assigned an owner tenant. If an owner tenant parameter is defined in the discovery adapter, the discovered CIs/relationships are assigned this owner tenant.

If a job using the adapter has an override defined for this parameter, then the overriding value is assigned to the discovered CI/relationship. For details, see ["How to Define the Owner Tenant For a Discovery Job" on page 476](#).

This task describes how to define an owner tenant parameter in an adapter.


Note: This section is relevant for multi-tenancy environments only.

1. Prerequisite

The owner tenant that you want to define in adapter's parameter must already be defined in UCMDB. For details on creating owner tenants in UCMDB, see "New Tenant/Edit Tenant Dialog Box" in the *Universal CMDB Administration Guide*.

2. In the Adapter Management module, select the adapter whose parameter you want to define.

3. Click the **Adapter Definition** tab.

4. In the Adapter Parameters pane, click the **Add**  button:

- a. In the **Name** box, type **defaultOwner**.
- b. In the **Value** box, enter the name of the owner tenant in UCMDB that you want to define in the adapter.
- c. (Optional) Enter a description for the owner tenant parameter.

How to Configure Full Population Run

Because the UCMDB integration adapter only synchronizes changes, over time CIs are not touched and are aged out. Therefore, by default, the UCMDB integration adapter runs a full population job every seven days.

Note: For other adapters, if the **Allow Integration job to delete removed data** check box is

selected, touch is performed automatically. If the check box is cleared, touch is not performed.

To change the full population value of the UCMDB integration adapter:

1. Open the CmdbAdapter adapter source.
 - a. Select **Data Flow Management > Adapter Management > Resources pane > CmdbAdapter**.
 - b. Under **Adapters**, right-click **CmdbAdapter**, and select **Edit Adapter Source**.
2. In the source file, locate the following tag:

```
<full-population-days-interval>  
    7  
</full-population-days-interval>
```

3. Edit the value as follows:

Value	Description
7	Run full population job every 7 days
1	Run full population job each day
0	Always run a full population job
-1	The option is disabled

How to Configure Global Probe Result Filtering

Global filtering enables you to filter Probe results for all adapters, so that only results of interest to you are sent to the UCMDB Server.

You can also filter specific adapters. For details, see ["Adapter Configuration Tab" on page 259](#).

This section includes:

Configure Filtering in UCMDB	230
Configure Filtering Using the globalFiltering.xml File	231


Configure Filtering in UCMDB

This task describes how to use the UCMDB interface to filter the UCMDB CIs that are discovered.

1. Prerequisites

Before creating a filter, perform an analysis on what information you want to map and what data element in the scan file contains the information you want to filter.


2. Select a CI to filter

- a. Select **Adapter Management**.
- b. In the Resources tree, expand the **DDMiInfra** node and then expand the **Configuration Files** node.
- c. Right-click **GlobalFiltering.xml** and select **Open in Frame**.
- d. In the Global Filtering dialog box, click **Include** or **Exclude**.
 - **Include**. All CIs that do not match the filter are removed. If this marker is left empty, all results are sent to the server.
 - **Exclude**. All CIs that match the filter are removed. If this marker is left empty, all results are sent to the server.
- e. Click **Select CI Type** . The Select CI Type dialog box opens.

Note: This option is only available when **Include** or **Exclude** is selected in the left pane.

- f. Select a CI for which you want to create a filter, and click **OK**.

3. Select attributes to filter

- a. Click **Select Attribute** . The Select an Attribute dialog box opens.
- b. Select properties for the attribute, and click **OK**.

Note: You can use the "between" operator when filtering results, but only when the Object class is "ip_address" and the attribute name is "name".

For details on CI attribute types, see "Attributes Page" in the *Universal CMDB Modeling Guide*.

4. Activate and configure settings

In the Global Filtering Configuration Settings pane, select your options.

Available when: **Global Filtering Configuration** or **Include** or **Exclude** is selected in the left pane.

5. Results

Use the CI Type Manager to verify that data is filtered as expected in UCMDB. For more information, see "CI Type Manager" in the *Universal CMDB Modeling Guide*.

Configure Filtering Using the globalFiltering.xml File

This document explains how to perform filtering using a manual method. If you want a UI-driven solution to performing this task, see ["Configure Filtering in UCMDB" on page 579](#).

Note:

- You can use regular expressions in filters.
- Attributes in the filter should be of type **string** only. For details on CI attribute types, see *Attributes Page* in the *Universal CMDB Modeling Guide*.
- You can use the "between" operator when filtering results, but only when the Object class is "ip_address" and the attribute name is "name".
- A result is considered to be a match only if all filter attributes have the same values as those in the CI. (If one of a CI's attributes is not specified in the filter, all the results for this attribute match the filter.)
- A CI can match more than one filter. The CI is removed or remains according to the filter in which it is included.
- **Recursive Filtering.** Using global filtering, you can filter out a CI so that it is not included in the filter results. This CI may be a root CI, containing other CIs or relationships. By default, during the filter process, the contained CIs and relationships, as well as any CIs related to them, are added to the filter results—including the root CI. This causes undesired filter results. **Recursive filtering** corrects this by ensuring that if a root CI is filtered out, then any contained CIs or relationships are filtered out too, such that the root CI cannot be found again.

To enable recursive filtering:

In the **globalFiltering.xml** file, under the **resultFilters** element, locate the **recursiveFilter** attribute. (If the **recursiveFilter** attribute does not appear, then you must add it.) Set the attribute value to **true**.

Note: By default, recursive filtering is disabled, that is **recursiveFilter = false**.

- DFM filters first according to the **<includeFilter>** and then applies the **<excludeFilter>** on the results of **<includeFilter>**.

Configure a Filter

Open the **globalFiltering.xml** file. (**Adapter Management module > Resources pane > Packages > DDM Infra > Configuration Files**)

The code in displayed in the View pane:

```
<resultFilters>
  <excludeFilter>
    <vector />
  </excludeFilter>
  <includeFilter>
    <vector />
  </includeFilter>
</resultFilters>
```

- **<excludeFilter>**. When a vector marker is added to this filter, all CIs that match the filter are removed. If this marker is left empty, all results are sent to the server.
- **<includeFilter>**. When a vector marker is added to this filter, all CIs that do not match the filter are removed. If this marker is left empty, all results are sent to the server.

The following example shows an IpAddress CI that has address and domain attributes:

```
<vector>
  <object class="ip_address">
    <attribute name="name" type="String">192\.168\.82\.17.*</attribute>
    <attribute name="routing_domain" type="String">DefaultProbe</attribute>
  </object>
</vector>
```

If this vector is defined in **<includeFilter>**, all results **not** matching the filter are removed. The results sent to the server are those where the ip_address matches the regular expression **192.168.82.17.*** and the ip_domain is **DefaultProbe**.

If this vector is defined in **<excludeFilter>**, all results matching the filter are removed. The results sent to the server are those where the ip_address does **not** match the regular expression **192.168.82.17.*** and the ip_domain is **notDefaultProbe**.

The following example shows how logical OR and logical AND statements can be created.

Example of 'OR' condition:

```
<vector>
  <object class="ip_address">
    <attribute name="name" type="String">192\.168\.82\.17.*</attribute>
  </object>
  <object class="ip_address">
    <attribute name="name" type="String">192\.168\.82\.18.*</attribute>
  </object>
  <object class="ip_address">
    <attribute name="routing_domain" type="String">DefaultProbe</attribute>
  </object>
</vector>
```

If this vector is defined, all results where the IP address matches "192.168.82.17.*" OR matches "192.168.82.18.*" OR routing_domain is "DefaultProbe" is filtered.

Example of 'AND' condition:

```
<vector>
  <object class="ip_address">
    <attribute name="name" type="String">192\.168\.82\.17.*</attribute>
    <attribute name="routing_domain" type="String">DefaultProbe</attribute>
  </object>
</vector>
```

If this vector is defined, all results where the IP address matches "192.168.82.17.*" AND routing_domain is "DefaultProbe" is filtered.

The following example shows an ip_subnet CI that has no attributes.

```
<vector>
  <object class="ip_subnet">
  </object>
</vector>
```

Configure a Filter to Ignore Case

You can configure a filter to ignore case by prefixing a regular expression with **(?i)**. For example, **(?i)DefaultProbe** finds **defaultprobe** as well as **DefaultProbe**.

The following example removes all occurrences of the **DefaultdoMain** attribute because the vector code is located in the **<excludeFilter>** section:

```
<resultFilters>
```

```
<excludeFilter>
  <vector>
    <object class="ip_address">
      <attribute name="routing_domain" type="String">(?i)
        DefaultdoMAin</attribute>
    </object>
  </vector>
</excludeFilter>
<includeFilter>
  <vector />
</includeFilter>
</resultFilters>
```

How to Configure CI Aging Settings

This task explains how to configure the aging mechanism for adapters.

To learn more about aging, see "The Aging Mechanism Overview" in the *Universal CMDB Administration Guide*.

To enable aging of CIs:

1. Select the adapter: **Adapter Management > Resources pane > Packages > <adapter>**
2. In the **Adapter Configuration** tab, under **Results Management**, select an **Enable Aging** option as follows:

System Default	Enables aging of CIs using the default aging setting defined in each CI type's attribute settings. For details, see "Configuration Item Properties Dialog Box" in the <i>Universal CMDB Modeling Guide</i> .
Always Enabled	Always enables aging of CIs discovered by jobs that use this adapter. Note: When this option is selected, the default aging setting defined in each CI type's attribute settings is ignored.
Always disabled	Disables aging of CIs discovered by jobs that use this adapter. Note: This option overrides the default aging setting defined in each CI type's attribute settings.

3. Save your changes.

How to Define CITs to be Deleted by Java-based Population Adapters

This task describes how to define CITs to be deleted by population jobs that use Java-based population adapters.

1. Open the population adapter's configuration file.
2. Under the **<taskInfo>** tag, locate the **<remove-cis>** tag.

If this tag does not exist, create it.

3. Under the **<remove-cis>** tag, add the CITs to be removed using the format in the following example:

```
<remove-cis isEnabled="false">  
  <ci-type>link</ci-type>  
  <ci-type>object</ci-type>  
</remove-cis>
```

4. Save the configuration file.

Note: When defining integration jobs that use the population adapter, to configure the job to delete CITs as defined in the adapter, ensure that the **Allow Integration Job to delete removed data** option is selected. For details, see ["New Integration Job/Edit Integration Job Dialog Box" on page 349](#).


How to Attach Discovery Documentation to a Discovery Package

This task describes how to attach updated or new documentation to a discovery package.


1. Prerequisites

- a. Create the help document in PDF format.
- b. Create a folder called **docs**, and copy your PDF into that folder.
- c. Zip the **docs** folder, and copy it to your local file system.

2. Deploy the document on the UCMDb server

Navigate to **Administration > Package Manager**, and click the **Deploy packages to server**  button to deploy the .zip file containing the PDF you want to deploy. For details, see "How to Deploy a Package" in the *Universal CMDB Administration Guide*.

3. Attach the document to the relevant discovery package

- a. Navigate to **Data Flow Management > Adapter Management**.
- b. In the **Resources** pane, expand the adapter file: **Packages > <package name> > Adapters** and select the adapter to which to attach the document.
- c. Do one of the following:
 - In the **Adapter Definition** tab, under **Details**, click the **Edit**  button adjacent to the **Content Help** box, and select the help document that you deployed.
 - Right-click the adapter and select **Edit Adapter Source** from the shortcut menu. Look for **RelatedDocument** in the code, and replace the line with:

```
<RelatedDocument>name_of_pdf.pdf</RelatedDocument>
```

where **name_of_pdf** is the name of the help document you deployed.

How to Attach a Readme to a Discovery Package


This task describes how to attach an updated or new Readme file to a discovery package.

1. Prerequisite

To attach a Readme file to a discovery package, the package's .zip file must be located somewhere on your local file system.

If you are updating the Readme file of a discovery package that is already deployed on your UCMDB server, you must export the package's .zip file to your local file system before attaching the updated file. For details on exporting packages, see "How to Export a Package" in the *Universal CMDB Administration Guide*.

2. Add the Readme file to the discovery package's .zip file
 - Create or update the Readme file, and save it with the name, **Readme.txt**.
 - Copy the **Readme.txt** file into the root of the package's .zip file.
3. Deploy the package on the UCMDB server

Navigate to **Administration > Package Manager**, and click the **Deploy packages to server**  button to deploy the .zip file containing the Readme. For details, see "How to Deploy a Package" in the *Universal CMDB Administration Guide*.

How to View Discovery Resource History

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

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

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

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

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

To view a discovery resource and its history:

1. Log in to the UCMDB JMX console. For details, see How to Access the JMX Console in the *Universal CMDB Administration Guide*.
2. In the UCMDB JMX Quick Search box, enter **listResourceTypes**.

3. Enter your Customer ID. (**Default: 1**)
4. Click **Invoke**. The **URM Services** mbean is displayed.
5. Among the UCMDB resource types displayed on this page, the following discovery resource types are displayed:

Resource Type	Description	Displays Diff Metadata	Displays Diff Content
Discovery_ADAPTER_METADATA	Adapter resources	✓	✓
Discovery_CONFIGURATION_FILE_METADATA	Configuration Files	✓	✓
Discovery_JOB_METADATA	Discovery job definitions	✓	✓
Discovery_MODULE_METADATA	Discovery modules	✓	✓
Discovery_WIZARD_METADATA	Activity types	✓	✓
Discovery_SCRIPT_METADATA	Script resources	✓	✓
Discovery_BIN_RESOURCE_METADATA	External resources	✓	✗
Discovery_DOC_METADATA	PDF documents that come with the adapters	✓	✗
Discovery_MULTI_SCANNER_METADATA	Multiple scanner packages	✓	✗
Discovery_SCANNER_CONFIG_METADATA	Scanner configuration files	✓	✗
Discovery_SAI_RES_METADATA	SAI resources	✓	✗

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

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

Mbean: UCMDB:service=URM Services. Method: listResources[[java.lang.Integer](#)[java.lang.String](#)]

[Add new resource](#)

Resources of type: Discovery_ADAPTER_METADATA

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

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

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

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

How to Create and Configure Mapping Files Using the Visual Mapping Tool

The new mapping tool enables you to create, update, or delete mapping files in a visual way. You can configure both link root-based TQL queries and CI root-based TQL queries.

Prerequisites


- You have deployed any Generic Adapter package, or the package for any of the latest out-of-the-box adapters (Asset Manager Generic Adapter or the SM 9.40 Adapter)
- You have established an integration point with Asset Manager or Service Manager, or your custom adapter/integration that uses the Generic Adapter Framework
- The integration is activated

How to Open and View a Supported Mapping File Using the Visual Mapping Tool

The current version of the Visual Mapping tool supports the following mapping files:

- Enhanced Generic Push Adapter mapping files
- Generic Adapter mapping files for Population, Federation and Push scenarios

To open and view a supported mapping file using the visual mapping tool

1. Navigate to **Data Flow Management > Adapter Management**.
2. In the Resources pane, expand the **Packages > <package name> > Configuration Files** folder.
3. Do one of the following:
 - Click a mapping file and click **Yes** in the popup window that asks if you want to open the configuration file with the new mapping tool editor.
 - Right-click a mapping file and select **Open Mapping Tool** from the context menu
 - Click a mapping file and click the **Open Mapping Tool**  icon at the top of the script pane, or
 - In the Configuration Files pane, double click a mapping file and click **Yes** in the popup window that asks if you want to open the configuration file with the new mapping tool editor.


The new mapping tool editor window opens, with tree representation of local and external class models loaded and displayed.


Note:

- In case the integration point provides a null external class model, you can still open the Visual Mapping tool. An empty default class model will be displayed in the External Class Model pane instead.
 - If you open an old Enhanced Generic Push Adapter mapping file using the Visual Mapping tool, you will be asked if you want to convert the file to the new schema and that if you want to use the visual mapping tool as the default editor.
4. To view the entities and attributes of the UCMDb TQL or the external class model, expand the relationship type hierarchical tree in the Local Query pane or the External Class Model pane.

How to Create a Mapping File Using the Visual Mapping Tool

To create a mapping file using the visual mapping tool

1. Navigate to **Data Flow Management > Adapter Management**.
2. In the Resources pane, expand the **Packages > <package name> > Configuration Files** folder.
<package name> indicates the adapter package in where you want to create the new mapping file.
3. Click the **Create new resource**  icon at the top of the Resource pane, and select **New Configuration File**.
4. In the **Enter a Name** dialog that pops up, provide values as described in the table below.



Field	Description
Name	Enter a name for the new mapping file. Naming convention for new mapping files: <adapter_name>/mappings/push/<filename>.xml For example, <adapter_name>/mappings/population/customDataPopulation.xml. Note: You must specify the adapter name and include push or population in the name.
Package	Click  for the Package field, then in the Select Package dialog that pops up, select a package and click OK .

The new mapping file is created.

5. Open the new empty mapping file in the mapping tool editor, and edit the attribute mappings as necessary.

For details, see ["How to Edit and Update a Mapping File Using the Visual Mapping Tool"](#) on the [next page](#).

Note:



- For push scenario, you can add multiple roots, and you can select which one to use.
 - You can have duplicated **source_instance** nodes as long as the root-element is different.
6. Click **Validate Mapping File**  to validate the mapping file you just created.
 7. Click **Save** .

How to Edit and Update a Mapping File Using the Visual Mapping Tool

You can do the following to edit or update a mapping file using the visual mapping tool:

To edit or modify the mapped target attribute value for a specific attribute mapping

You can use one of the following methods:

- **Quick action.** Locate a corresponding entity in the External Class Model pane, and then select a desired attribute value in the External Class Model Attributes pane, and then click the green arrow button ( or ) to add the value to the mapping in the Visual Mapping pane.
- **Drag and drop.** After selecting a desired attribute value in the External Class Model Attributes pane, simply drag and drop the value to the Visual Mapping pane to update the selected mapping.
- **Auto-complete.** Directly type in the target attribute value field and select a desired value to update the mapping. The auto-complete suggestions are generated based on valid existing relationships between entities from the external class model or from the local TQL query.

When you type a character, the first level suggestions will appear. Usually these are all first level CITs from the external class model that match the string or items from the local TQL query.

After you type or select a valid CIT entity:

- If you enter the "." character, you obtain suggestions for linked CITs based on existing relationships from the external class model or from the local TQL query.

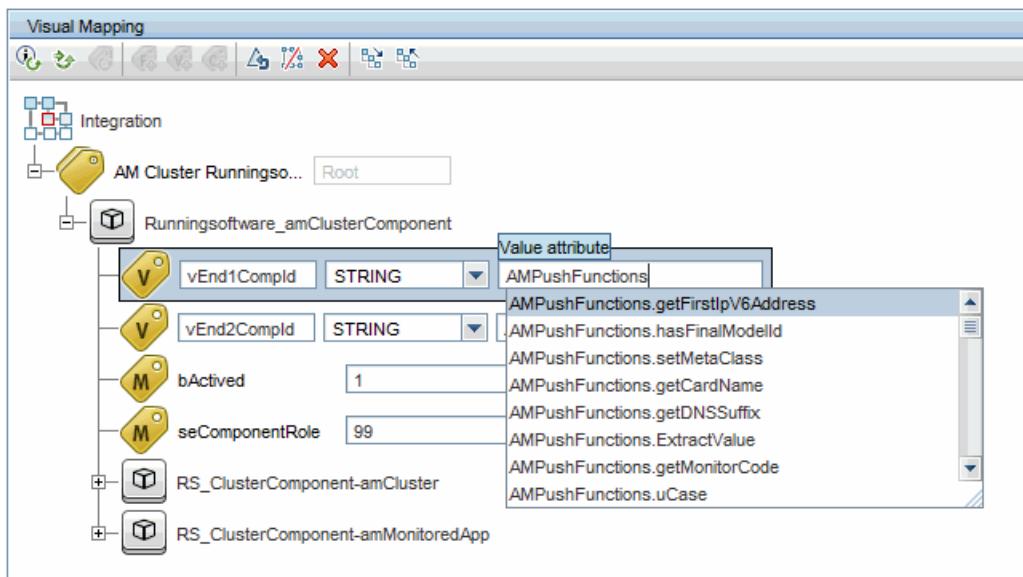
For example, you have a Computer to Node relationship,

- if you type **Computer**, **Node** will appear in the suggestions list.
- if you type **Node**, Computer will not appear unless you have another relationship from Node

to Computer.

- If you enter the "[" character, you obtain attribute suggestions for the current CIT:
 - For local TQL query, attributes are filtered with the Element Layout feature.
 - For external class model, all attributes are displayed.

The Visual Mapping tool can also provide auto-complete suggestions on possible methods from imported Groovy scripts. For example, you have a mapping file that imports the **mappings.scripts.AMPushFunctions** Groovy script, if you write an attribute value like **AMPushFunctions**, you should receive a list of possible method names; If you write an attribute value like **AMPushFunctions.get**, you should receive a list of possible method names that start with **get**.




- **Edit the mapping value in the XML Editor directly.** You can directly edit the XML mapping value in the XML Editor pane below the Visual Mapping pane to update the mapping.



To add a new attribute mapping for the selected target_entity tag

1. In the Local Query pane, select a UCMDB entity.
2. To add a UCMDB attribute to the Visual Mapping pane, in the Local Query Attribute pane, select a desired attribute and click the green arrow button (← or →, depending on the push, population, or federation scenario).



To add a source attribute from a different UCMDB TQL query,

- a. From the **Query** drop-down list, select a different UCMDB TQL query.

If the desired TQL is not in the drop-down list, click **Add TQL Queries** . In the Add Queries dialog box, select and add an available integration TQL query from the **Available items** pane to the **Selected items** pane, then click **OK**.


- b. Expand the TQL query representation.
 - c. Select a UCMDB entity that corresponds to the parent **target_entity** tag in the Visual Mapping pane where you want to add the new UCMDB attribute.
 - d. In the Local Query Attributes pane, select an attribute and click the green arrow button ( or , depending on the push, population, or federation scenario) to move the attribute to the Visual Mapping pane.
3. Add a mapping attribute value from the External Class Model entity to the Visual Mapping pane.



To do so, follow one of the following methods:

- **Quick action.** Locate a corresponding entity in the External Class Model pane, and then select a desired attribute value in the External Class Model Attributes pane, and then click the green arrow button ( or ) to add the value to the mapping in the Visual Mapping pane.
- **Drag and drop.** After selecting a desired attribute value in the External Class Model Attributes pane, simply drag and drop the value to the Visual Mapping pane to update the selected mapping.
- **Auto-complete.** Directly type in the target attribute value field and select a desired value to update the mapping. The auto-complete suggestions are generated based on valid existing relationships between entities from the external class model or from the local TQL query.
- **Edit the mapping value in the XML Editor directly.** You can directly edit the XML mapping value in the XML Editor pane below the Visual Mapping pane to update the mapping.

To update the mapping file for the selected `source_instance` or `target_entity` tag

Do one of the following:


-  **Update Info Tag.** Clicking this button opens the Update Info Tag dialog box, enabling you to modify and update the information about the data repositories being integrated, including Name, Version, and Vendor for both source and target data repositories.

-  **Update Import Tag.** Clicking this button opens the Update Import Tag dialog box, enabling you to select and add available items and import new groovy scripts. You can also move up or down the sequence of a script to decide the order of scripts to be imported.
-  **Update Optional Tags.** Clicking this button opens the Update Optional Tags dialog box, enabling you to update optional tags by defining values for the Type, Is Valid, and Is Deleted fields. You can also select the Show Warning check box to display warning messages.


Note: This button is not available for the source_entity tag.

To add a new mapping element to the existing mapping file


Select the parent **source_instance** or **target_entity** element of your interest, and do the following to add the source element:



-  **Add For Each Tag.** Clicking this button opens the Add For Each Tag dialog box, enabling you to define the source and the index for the tag that you want to add for each child mappings under the current parent entity:
 - **Source Entities.** Defines the source entities for the tag.
 - **Count Index.** Defines the iteration loop index ("i") that can be used to reference the currently iterated element. For example, **pc.ip[i]**.
 - **Var Name.** (Optional) Specifies the variable name for the tag.

Each time you edit a field you will see a notification of what attribute will be edited.

-  **Add Variable Tag.** Clicking this button opens the Add Variable Tag dialog box, enabling you to define and add variable tags to the selected variable element:
 - **Name.** Specifies name for the variable.
 - **Type.** Select a value from the drop-down list as type of the variable in database.
 - **Value.** Specifies a value for the variable.

Note: This button is not available for the source_instance tag.

-  **Add Custom Section.** Enables you to add an empty section in the Visual Mapping pane, allowing you to manually define a new mapping element that may not fall into any of the existing mapping categories, including customized XML tags.

After adding an empty section in the Visual Mapping pane by clicking the **Add Custom Section**  button, you can edit the empty section in the XML Editor pane. Clicking **Save**  in the XML Editor saves the code.

Note: To save the entire mapping file, click **Save**  for the entire Visual Mapping tool window.

To use the "is-valid" XML attribute inside attribute mappings to indicate valid attributes

When creating attribute mappings such as the one below, you may have a use case to ignore certain attribute mappings within a target entity based on some custom logic:

```
<target_entities>
  <!--The query name must match the one selected in the UI-->
  <source_instance query-name="Node with ID" root-element-name="Computer">
    <!-- need to match case in UCMDB TQL -->
    <target_entity name="Root">
      <!--This is how the RTN External ID is set-->
      <variable name="external_id_obj" datatype="STRING" value="Computer['external_id_obj']"/>
      <!--RTN Attributes-->
      <target_mapping name="name" datatype="STRING" value="Computer.Asset[0]['name']"/>
      <target_mapping name="description" datatype="STRING" value="Computer['name']"/>
    </target_entity>
  </source_instance>
</target_entities>
```

This can be done via the newly added **is-valid** XML attribute on the **target_mapping** XML tag.

If you change the mapping line for the **description** attribute to use the new XML attribute, you get something like this:

```
<target_mapping name="description" is-valid="CustomFunctions.isSupportedType
(Computer['name'])" datatype="STRING" value="Computer['name']"/>
```

where **CustomFunctions.isSupportedType(Computer['name'])** represents a Groovy expression that will result in a boolean value (**true** means the attribute is valid, **false** means the attribute will be ignored).

For a quick check you can use any simple expression like "1 == 1" or "true".

Relevant log lines are also available. For example, if the expression is invalid, you will see the following log statements in the **fcmdb.push.all.log** or **fcmdb.push.mapping.log**:


```
2014-08-14 14:07:56,974 [JobExecuterWorker-0:DS_ga_test] TRACE - >> Execution of
is-valid expression [1 == 2] = [false]
```

```
2014-08-14 14:07:56,974 [JobExecuterWorker-0:DS_ga_test] DEBUG - >> Ignoring
invalid property [description] from target entity [Root]
```

And, if the expression is valid you will simply see:

```
2014-08-14 14:06:39,660 [JobExecuterWorker-0:DS_ga_test] TRACE - >> Execution of
is-valid expression [1 == 1] = [true]
```

To configure the icons for the external entities

1. Open the icon-related mapping file for the adapter.
For example, for AM Generic Adapter, open the **am-entity-config.xml** file.
For Service Manager adapter, open the **icon.properties** file.
2. Locate the icon type tag for the CIT of your interest in the mapping file.
For example, for AM Generic Adapter, it is **icon-type**.
3. Modify the value for icon type tag with a UCMDB icon value as needed.
For available UCMDB icons, check **Modeling > CI Type Manager > Icon** tab.
4. Click **Save**.
5. Open a desired mapping file, click the **Refresh External Class Model**  button, the icons should be updated.

To configure the positions of Local Query and External Class Model panes on left or right

To do so,

1. Go to **Administration > Infrastructure Settings Manager**.
2. In the Categories pane, select **GUI Settings**.
3. In the Name column, locate the **Switch between external and local tree panels in the integration mapping tool** setting.
4. In the Value column, click the value for the setting you selected, and then choose a value from the drop-down list.

The default value for this setting is **False**.

5. Click **Save** .


The change takes effect immediately.

To search for CI types or attributes in the Local Query or External Class Model panes


You can search for a CI type or an attribute in both of the Local Query, External Class Model, and their Attributes panes the same way as you do in the Script pane.

You can use * as a wildcard character to search inside the text.

To remove a mapping element from the mapping file

To remove a `target_entity` or `target_mapping` tag from the mapping file, select the desired mapping element, and click **Remove Node** .


To remove the entire mapping

To remove the entire mapping, select any tag in the Visual Mapping pane and click **Clear Entire Mapping** .

To revert to the last saved change

To revert to the last saved change, click **Revert Changes** .

To validate the changes you made to the entire mapping

Click **Validate Mapping File**  to validate the changes you just made to the mapping file.

Note: Although the Visual Mapping tool supports all mapping files, the following configurations are not supported:

- Non-instance based adapters: The UCMDB enhanced push adapter works with instance based adapters. (For more information, see the *Universal CMDB Developer Reference Guide*).
- Mappings containing both CI root and link root TQL queries in the same file.
- Mappings having wildcard tags that select multiple TQL queries for a target mapping.

In case you wish to edit an existing mapping file that references one of the above mentioned cases, you may see that the Open Mapping Tool option is not available, or an error message stating that the mapping file is unsupported and that only manual XML editing is possible.

How to Synchronize Class Model Changes to External System through Push Adapter

With the new mapping tool, you can create new CI types and attributes for external class model in Universal CMDB and synchronize the changes in real time to the external system. This enables you to manage class model changes on both systems centrally from Universal CMDB.

To synchronize class model changes to external system through push adapter

1. Open an existing mapping file using the Visual Mapping tool.

The external tree is populated with a class model.


2. In the External Class Model pane, select a node.

3. **Create and synchronize a CI type.**

- a. Click **Add New CI Type to External Class Model**  in the toolbar for the External Class Model pane.

The Add New CI Type to External Class Model dialog box opens, comprising of general section and metadata section.

The fields in the metadata section are populated dynamically as specified in the external system (passed through the adapter).

Note: If you already selected a CIT before you click **Add New CI Type to External Class Model** , the new CIT is created as a child CIT of the selected node; If no CIT is selected, the new CIT is created as a root CIT.

- b. Define the following standard properties for the new CI type:
 - **Name.** Specify the name for the new CI type.
 - **Description.** (Optional) Detailed description of the CI type.
- c. Click **OK**.

The new CIT synchronization is triggered and the save operation runs as a background task.


Until the status of the save operation is confirmed, the newly created CIT appears as greyed out in the external tree.

After the save is successful, the CIT turns into a selectable tree node, and the node can be further used in mappings and drag and drop scenarios.

In case the save operation failed, the CIT will not appear in the external tree anymore, and an error notification appears at the top of the Visual Mapping pane.

4. Create and synchronize an attribute.

You can similarly create new attributes for a selected CIT and synchronize the change to the external system. To do so,

- a. In the External Class Model Attributes pane, click **Add New Attribute to Selected External Node**  on the toolbar.

The Add New Attribute dialog box that opens.

There is no metadata section in this dialog box.

- b. Define the following properties for the new attribute:
 - **Name.** Specify the name for an attribute property.
 - **Display Name.** Specify the display name for an attribute property.
 - **Description.** (Optional) Detailed description of the attribute property.
 - **Type.** Select a value from the drop-down list as type of the attribute property in database.
- c. Click **OK**.

The new attribute synchronization is triggered and the save operation runs as a background task.


Until the status of the save operation is confirmed, the newly created attribute appears as grayed out in the external attributes table.

After the save is successful, the attribute turns into a selectable attribute entry, and the attribute can be further used in mappings and drag and drop scenarios.





In case the save operation failed, the attribute will not appear in the external attributes table anymore, and an error notification appears at the top of the Visual Mapping pane.

Pre/Post-Scan Script Editor

Enables you to edit pre and post scan scripts in your Management Zones.

To access	<ul style="list-style-type: none"> • Adapter Management > Inventory Discovery > expand Adaptors > Inventory Discovery by Scanner > expand the Global Configuration Files pane, select the PrePostScanScriptingConfiguration file and click Edit . • Data Flow Management > Universal Discovery > Zone-based Discovery > Inventory Discovery Activity > Preferences tab > select Scanner based Inventory Discovery and click Edit Script.
Important information	UI elements are available only when a script file is selected in the left pane.
Relevant tasks	"How to Edit Pre-/Post-Scan Scripts" on page 544
See also	"Inventory Discovery Scanners" on page 509

User interface elements are described below:

UI Element	Description
	Find Text. Opens the Find Text dialog box, enabling you to find text in the selected script file. For more information, see "Find Text Dialog Box" on page 273 .
	Go to Line. Opens the Go To Line dialog box, enabling you to jump to a specific line in the script file. Enter the line number and press Enter .
	Import a File. Opens the Import File dialog box, enabling you to import a script file or a resource file.
	Export to a File. Opens the Export File dialog box, enabling you to export the selected script or resource file.

Pre-Scan and Post-Scan Scripts

Scripts can be run by the Scanner on discovery nodes. Scripts are typically created to capture custom data on specific hardware, settings, or applications. Scripts together with related files are packaged with the Scanner and deployed to a remote machine. You can create a script using any external text editor and import into UCMDB, or you can create it using an embedded text editor.

The pre-scan scripts run at scanner start-up before the hardware and software scanning. The post-scan scripts run after the hardware and software scanning is complete.

To see more information on how to edit pre and post scan scripts, see ["How to Edit Pre-/Post-Scan Scripts" on page 544](#).

Note: If you create a post-scan script, you may want to map your captured data to a UCMDB attribute using the Hardware Mapping Configuration tool. To do this, see ["How to Map Scan File Attributes to UCMDB" on page 572](#).

Adapter Management User Interface

This section describes:



Adapter Definition Tab	253
Adapter Configuration Tab	259
Adapter Management Window	265
Adapter Source Editor Window	265
Attributes Assignment Editor Dialog Box	267
Choose Discovered Class Dialog Box	268
Configuration File Pane	269
Edit Process Dialog Box	271
Find Resource/Jobs Dialog Box	272
Find Text Dialog Box	273
Input Query Editor Window	274
Mapping Tool Editor Window	277
Permission Editor Dialog Box	284
Resources Pane	285
Script Pane	288
Software Identification Rule Editor Dialog Box	290
Software Library Dialog Box	292
Global Filtering Dialog Box	293

Adapter Definition Tab

Enables you to define an adapter by specifying which CITs the adapter should discover and which protocols are needed to perform discovery.









To access	Select Adapter Management > Resources pane > Packages > <adapter> .
Relevant tasks	"Implement a Discovery Adapter" in the <i>Universal CMDB Developer Reference Guide</i>

User interface elements are described below:

UI Element (A–Z)	Description
Adapter Category	Used to arrange adapters by category.
Content Help	<p>The Help document associated with the adapter, in PDF format.</p> <p>To change the Help document associated with the adapter, do one of the following:</p> <ul style="list-style-type: none"> Click  and select the relevant PDF file. Right-click the adapter in the Packages tree and click Edit adapter source. Find the following line in the code: <code><RelatedDocument>name_of_pdf.pdf</RelatedDocument></code> and change the name of the PDF file. <p>To detach the selected Help document, click .</p>
Description	A detailed description of the adapter's purpose, including relevant comments.
Display Name	A display name to identify the adapter.
Type	<ul style="list-style-type: none"> For Discovery adapters: jython For Integration adapters: can be of various types
Used as Integration Adapter	<p>Select to define that this adapter is an integration adapter.</p> <p>Note: These adapters cannot be used for defining discovery jobs, and are accessible only through the Integration Studio.</p>

Input Pane

User interface elements are described below:

UI Element (A–Z)	Description
Input CI Type 	<p>The input CIT is used as the adapter input. For details, see "Define Adapter Input (Trigger CIT and Input Query)" in the <i>Universal CMDB Developer Reference Guide</i>.</p> <p>Click the button to choose a CIT to use as the input.</p>
	Edit Input Query. Enables you to edit the input query.
	Remove Input Query. Enables you to delete the input query.
Input Query	<p>Defines a query for validation of the triggered CIs for jobs that run this adapter. (CIs matching the job's triggered query must match the Input query as well.)</p> <ul style="list-style-type: none"> Click the Edit Input Query  button to open the Input Query Editor window. Click the Remove Input query  button to remove the Input query from the adapter. <p>To define which CIs can be Trigger CIs for jobs that run a specific adapter, see "Input Query Editor Window" on page 274. For more information, see "Trigger CIs and Trigger Queries" on page 27.</p> <p>For an example of an input query definition, see "Example of Input Query Definition" in the <i>Universal CMDB Developer Reference Guide</i>.</p> <p>Note:</p> <ul style="list-style-type: none"> Because this field is optional, not all adapters include an Input query. None signifies this adapter does not have an Input query definition. To ensure that the Data Flow Probe is always kept up to date with possible changes to the Trigger CI data, you can configure UCMDB to periodically recalculate the Trigger CI data and send any changes to the Data Flow Probe. For details, see "How to Configure Periodic Data Flow Task Updates" on page 68. This option is disabled by default because it can interfere with performance.
Triggered CI Data	<ul style="list-style-type: none"> . Add Trigger CI data to the adapter. . Remove Trigger CI data from the adapter. . Edit the Trigger CI data in the Parameter Editor dialog box.





UI Element (A–Z)	Description
	<ul style="list-style-type: none"> • Name. The information that is needed to perform a task on a specific CI. This information is passed to the CI queried in the task. Important: Do not use id for a Triggered CI Data entry, as it is a reserved name. • Value. The attribute value. Variables are written using the following syntax: <code>\${VARIABLE_NAME.attributeName}</code> where VARIABLE_NAME can be one of three predefined variables: <ul style="list-style-type: none"> ◦ SOURCE. The CI that functions as the task's trigger. ◦ HOST. The node in which the triggered CI is contained. ◦ PARAMETERS. The parameter defined in the Parameter section. You can create a variable. For example, <code>\${SOURCE.network_netaddr}</code> indicates that the trigger CI is a network.

Used Scripts Pane

Displays the scripts used by the selected adapter.

Important Information	Available for Jython adapters only
------------------------------	------------------------------------

User interface elements are described below (unlabeled elements are shown in angle brackets>):






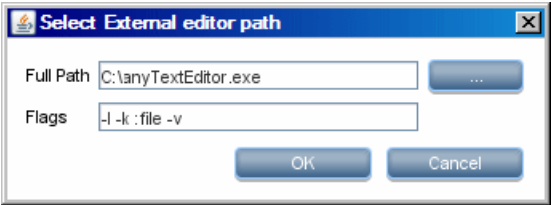



UI Element (A–Z)	Description
	Move up/Move down. Enables you to change the order of the scripts. DFM runs the scripts in the order in which they appear here.
	Add script. Enables you to add a script to the adapter.
	Remove script. Enables you to remove a script from the adapter.
	Edit. Enables you to edit the selected script in the Script Editor that opens.
<Scripts>	A list of Jython scripts used by the adapter.

Workflow Steps Pane

Displays only the **workflow** element of the selected adapter script.

Important Information	<p>Available: Only for the adapters that contain workflows</p> <p>Example: UDAgentManagement adapters</p>
------------------------------	---

User interface elements are described below:






UI Element (A–Z)	Description
	<p>Find text. Enables you to find specific text in the workflow steps. For details, see "Find Text Dialog Box" on page 273.</p>
	<p>Go to line. Enables you to jump to a specific line in the workflow steps. In the Go To Line dialog box, enter the line number, and press ENTER.</p>
	<p>Open External Editor. Opens the workflow steps in an external text editor.</p> <p>Prerequisite: Click the Edit the External Editor Preferences  button to define the path to an external editor. If no external editor path is defined, you will be prompted to provide one when you try to open the external editor.</p>
	<p>Edit the External Editor Preferences. Click to edit the external editor preferences. You can run the editor by adding flags to the path.</p> <p>Note: You cannot specify the file name. Instead, you can use flags relevant to your external editor to retrieve the file name, such as :file.</p> <p>In the following example, :file sets the place of the file in relation to the flags.</p> <div style="border: 1px solid gray; padding: 5px; margin: 10px 0;">  </div> <p>If no flags are defined, the file name is automatically added to the end of the path.</p>
	<p>Switch Editor Mode. Enables you to switch between the default advanced editor and a simple text editor.</p>
Validation Information	<p>Displays if the definition is valid or not:</p> <ul style="list-style-type: none"> • . Indicates that the definition is valid. • . Indicates that there is an error in the definition.

Required Permissions Pane

Enables you to view the permissions that you have configured for an adapter.



To access	Select Data Flow Management > Adapter Management > an adapter > Adapter Definition tab > Required Permissions pane.
Important Information	<ul style="list-style-type: none"> • Workflow: <ul style="list-style-type: none"> ◦ Configure the permissions in the Permission Editor dialog box. ◦ View the permissions in this pane. ◦ When working with jobs in the Universal Discovery window, view these permissions for a specific job. • For details on the fields in this pane, see "Permission Editor Dialog Box" on page 284.
See also	<ul style="list-style-type: none"> • "Permission Editor Dialog Box" on page 284 • "Discovery Permissions Window" on page 495 • "Viewing Permissions While Running Jobs" on page 467

User interface elements are described below:

UI Element (A–Z)	Description
	Add. Opens the Permission Editor dialog box, enabling you to add a permission object. The Permission Editor dialog box opens. For details, see "Permission Editor Dialog Box" on page 284 .
	Edit. Opens the Permission Editor dialog box, enabling you to edit a selected permission object. For details, see "Permission Editor Dialog Box" on page 284 .
	Remove. Enables you to delete a selected permission object.
	Move up/Move down. Enables you to change the order of the permissions. Select the permission object and click the up or down button. The order given here is the order in which the credentials are verified.
	Export Data to File. Enables you to export a permission object in Excel, PDF, RTF, CSV, or XML format. For details, see "Browse Views Mode" in the <i>Universal CMDB Modeling Guide</i> .




Required Discovery Protocols Pane

User interface elements are described below (unlabeled elements are shown in angle brackets):

UI Element (A–Z)	Description
	Add required protocol. Enables you to add a required protocol.
	Remove required protocol. Enables you to remove an existing protocol that is no longer required.
<Protocols>	<p>List of protocols required by the adapter for the task. For example, the NTCMD protocol, together with its user name, password, and other parameters, is needed for DFM to access a Windows system.</p> <p>For information, see "Supported Protocols" in the <i>HPE UCMDB Discovery and Integrations Content Guide - Supported Content</i>.</p>

Discovered CITs Pane

User interface elements are described below:

UI Element (A–Z)	Description
	Add Discovered CIT. Opens the Choose Discovered Class dialog box, enabling you to select a CIT to be discovered by the adapter. For details, see " Choose Discovered Class Dialog Box " on page 268.
	Remove Discovered CIT. Enables you to remove the CIT from the list of CITs that the adapter discovers.
	View Discovered CITs as Map. Opens the Discovered CITs Map window enabling view a graphical map of the CITs and relationships that are discovered by the adapter.
CITs	List of CITs that the adapter discovers.




Global Configuration Files Pane

Enables you to add default configuration files to the adapter, as well as the specific configuration files that the adapter needs.

Important	The applicationsSignature.xml file contains a list of all applications that DFM
------------------	--




Information	attempts to find in the environment. The configuration file applicationsSignature.xml opens the Software Library dialog box. For details, see " Software Library Dialog Box " on page 292.
Relevant tasks	"How to Discover Running Software – Scenario" on page 473

User interface elements are described below:

UI Element (A–Z)	Description
	Add. Opens the Global Configuration Files dialog box, enabling you to select configuration files that are needed by the adapter.
	Remove. Enables you to delete a selected configuration file.
	Edit. Opens the selected configuration file in an appropriate editor. For example, the file msServerTypes.xml opens the Script Editor.

Adapter Parameters Pane

User interface elements are described below:

UI Element (A–Z)	Description
	Add Parameter. Opens the Parameter Editor dialog box, enabling you to enter details about a new parameter. The value you enter here is assigned to the attribute.
	Remove Parameter. Enables you to remove a selected parameter.
	Edit Parameter. Opens the Parameter Editor dialog box, enabling you to make changes to the parameter definition.
Name	Each row represents the definitions for one parameter.
Value	Separate values with commas.

Adapter Configuration Tab

Enables you to define additional options relevant to adapter execution and result filtering.

To access	Select a specific adapter in the Resources pane and click the Adapter Configuration tab.
Important Information	Click the Save button to save any changes you make.
See also	"DataFlowProbe.properties File" on page 83

Trigger Dispatch Options Pane

Enables you to specify dispatch options for triggers.

UI Element (A–Z)	Description
Override default probe selection	Defines the Probe to use with the adapter. For more information, see "Override Probe Selection - Optional" in the <i>Universal CMDB Developer Reference Guide</i> .
Supports IPv6	When selected, indicates that the adapter can connect to a remote machine via IPv6 addresses, and can handle IPv6 results in the output. Note: If this option is not selected for an adapter, and no IPv4 addresses are found for the trigger, the trigger is not dispatched to the Probe.

Execution Options Pane


User interface elements are described below:

UI Element (A–Z)	Description
Create communication log	Choose to create a log file that logs the connection between the Probe and a remote machine. <ul style="list-style-type: none"> • Always. A communication log is created for this session. • Never. A communication log is not created for this session. • On Failure. A communication log is created for this session, only if the execution fails. <p>That is, DFM reports an error (report of a warning does not create a communication log). This is useful when you need to analyze which queries or operations take most of the time, send data for analysis from different locations, and so on. If the job completes successfully, no log is created.</p> <p>When requested (in the Discovery Progress pane), a log retrieved from the</p>

UI Element (A–Z)	Description
	<p>Probe is displayed (if a log has been created). For details, see "Discovery Progress Dialog Box" on page 670.</p> <p>Note: For debug purposes, you can always retrieve the communication logs for the last 10 executions, even if Create communication logs is set to On Failure.</p> <p>Communication log files are created on the Probe Manager under the C:\hp\UCMDB\DataFlowProbe\runtime\communicationLog folder. For details on how the communication logs work, see "Record DFM Code" in the <i>Universal CMDB Developer Reference Guide</i>.</p> <p>Note: CDATA mechanism is used to store information retrieved from user environment in the communication logs. When scan files get some characters or XML segments that cannot be parsed by the CDATA mechanism, the information will be saved in binary format for further troubleshooting purpose. Micro Focus Support will decode the binary data in the communication logs to perform troubleshooting.</p>
Include results in communication log	<p>Select to enable capturing the discovered results with the created communication log; these discovered results may help in investigating various discovery problems.</p>
Max. execution time	<p>The maximum time allowed for an adapter to run on one Trigger CI.</p>
Max. threads	<p>Each job is run using multiple threads. You can define a maximum number of threads that can be used concurrently when running a job. If you leave this box empty, the Probe's default threading value is used (8).</p> <p>The default value is defined in the DataFlowProbe.properties file, in the appilog.agent.local.services.defaultMaxJobThreads parameter.</p> <p>Note: The jobs in the Network – Host Resources and Applications module require a permanent connection to the Probe's internal database. Therefore, these jobs are limited to a maximum number of 20 concurrent threads (which is the maximum number of concurrent connections permitted to the internal database). For details, see "Host Resources and Applications Discovery" in the <i>Universal CMDB Discovery and Integrations Content Guide</i>.</p>

Results Management Pane

User interface elements are described below:

UI Element (A–Z)	Description
Enable aging	<p>The aging mechanism specifies how long a period must pass in which CIs are discovered, before DFM treats these CIs as no longer relevant and removes them. Choose from one of the following aging options:</p> <ul style="list-style-type: none"> • System Default: Use the system's default value for the Enable Aging attribute of each CI type. • Always Enabled: Select this option to always enable the aging mechanism. • Always Disabled: Select this option to always disable the aging mechanism. <p>The value you set here is for each CI result that is reported to the UCMDB by the jobs of this adapter.</p> <p>For details on aging, see "The Aging Mechanism Overview" in the <i>Universal CMDB Administration Guide</i>.</p>
Enable Automatic Deletion	<p>Choose between:</p> <ul style="list-style-type: none"> • Always. Automatic Deletion or Candidate for Deletion is always enabled, regardless of whether discovery succeeds or fails. • On Success or Warnings. Automatic Deletion or Candidate for Deletion is enabled only when discovery finishes with a success or warning status. In the case of a discovery error, nothing is removed and CIs are not marked as a candidate for deletion. • Only on Success. Automatic Deletion or Candidate for Deletion is enabled only when discovery finishes with a success status. In the case of a discovery error or warning, nothing is removed and CIs are not marked as a candidate for deletion (this is the default). <p>Selecting this option enables the Automatic Deletion box where you select specific CITs for deletion or as candidates for deletion, if the Data Flow Probe does not find them during its next invocation.</p> <p>To select CITs, click the Add  button. In the Choose Discovered Class dialog box, choose the CITs that should be automatically deleted.</p> <p>The changes you make here are added to the adapter configuration file, for example:</p> <pre data-bbox="412 1556 1370 1829"> <resultMechanism isEnabled="true"> <autoDeleteCITs isEnabled="true"> <CIT>shell</CIT> <candidateForDeletionCIT>node</candidateForDeletionCIT> </autoDeleteCITs> </pre>

UI Element (A–Z)	Description
	<div data-bbox="431 338 1369 394" style="background-color: #f0f0f0; padding: 5px; border: 1px solid #ccc;"> </resultMechanism> </div> <p>For information about how the Data Flow Probe handles CI deletion, see "Automatically Deleted CIs and Relationships and Candidates for Deletion CIs" on page 226.</p> <p>Note for Java-based population adapters: In order for CITs to be deleted by the population engine, you must configure the adapter configuration file manually as described in "How to Define CITs to be Deleted by Java-based Population Adapters" on page 235.</p>
<p>Enable collecting 'Discovered by' data</p>	<ul style="list-style-type: none"> • Selected. DFM collects data on the results of running the adapter. This data is then used to enable rediscovery of CIs. The data is necessary for the Discovery tab in IT Universe to function correctly. It is also used for the View Based Discovery Status functionality which leverages the data to aggregate the complete discovery status for certain views. • Cleared. DFM does not collect this data. The check box needs to be cleared for adapters where rediscovery is not helpful. For example, the Range IPs by ICMP job has this check box cleared by default because its Trigger CI is the Probe Gateway and so all CIs discovered by this job have the same Trigger CI. If the check box was not cleared, a rediscovery attempt on any view containing any single IP would result in a ping sweep throughout the entire customer network—certainly not desirable behavior. <p>The job results of this adapter are displayed in the Discovery for View dialog box only if this check box is selected. For details, see "How to Check the Status of Application Discovery (Rediscover a View)" and "Show Discovery Status and Changes Dialog Box" in the <i>Universal CMDB Modeling Guide</i>.</p>
<p>Enable reporting of empty values</p>	<p>When selected, the Data Flow Probe reports empty values for discovered properties to UCMDB.</p> <p>Default: Enabled</p>
<p>Enable update 'Last Access Time'</p>	<p>When selected, if a CI is touched when a discovery or integration job runs, the Last access time property of the CI is updated. This indicates that the CI represents an active component in the system, and prevents the CI from becoming a deletion candidate.</p> <p>For details about the aging mechanism and deletion candidates, see "The Aging Mechanism Overview" in the <i>Universal CMDB Administration Guide</i>.</p> <p>Note: If this option is not selected:</p>

UI Element (A–Z)	Description
	<ul style="list-style-type: none"> For new CIs, the Last access time property is given the same value as the Create Time property For existing CIs, subsequent activations of the job do still update the LastModifiedTime property, but the Last access time property is not updated. <p>Use-Case Example</p> <p>When importing data from an external data source, this data may include meta-data about CIs. If this option is enabled, the CIs are updated with the metadata and their Last Access Time value is updated. Disabling this option can be useful if you do not want to affect the aging status or the deletion candidacy of these CIs. In this case, the information is added to the CIs but their Last Access Time remains unchanged.</p>
Fail entire bulk if invalid CIs are found	<p>If a set of objects (for example, 1,000 objects) includes even one invalid CI (for example, a node cannot be identified because of missing topological information), the reconciliation engine drops the entire set and does not send it to the CMDB. This is the default behavior.</p> <p>If this option is not selected, the results are still sent to the CMDB but without the invalid CIs (and their topology). In the above example, 999 objects would be processed. UCMDB displays an error message when you view the results.</p> <p>Available for: Discovery adapters and Jython-based integration adapters only</p>
Initiate agent connection	<p>When this option is selected, the adapter finds a credential to work with an agent so that other discovery adapters can connect to the agent.</p>

Result Grouping Pane

User interface elements are described below:

UI Element (A–Z)	Description
Grouping Interval (Seconds)	<p>To group results in the Probe before they are sent to the server, type the value that indicates how long results are stored in the Probe before being transferred to the server.</p> <p>The default value is 30 seconds.</p> <p>Note: If you enter a value in both boxes, DFM applies the value of whichever occurs first.</p>

UI Element (A–Z)	Description
Max. CIs in group	Specify the number of CIs that should accumulate in the Probe before being transferred to the server. The default value is 5000.

Adapter Management Window

Enables you to view or edit default parameter values used for the discovery and integration processes.










To access	Select Data Flow Management > Adapter Management or right-click a job in the Universal Discovery window and click Go to Adapter .
Important Information	<ul style="list-style-type: none"> An asterisk (*) next to a resource (adapter, script, or configuration file) signifies that the resource has changed since the package (in which it is included) was deployed. If the original package is redeployed, the changes are deleted from the resource. To save the changes, move the resource to a new package and deploy the package (the asterisk disappears). Only administrators with an expert knowledge of the discovery and integration processes should delete packages.
See also	<ul style="list-style-type: none"> "Adapter Definition Tab" on page 253 "Global Configuration Files Pane" on page 258 "Adapter Configuration Tab" on page 259 "Script Pane" on page 288 "Resources Pane" on page 285 "Configuration File Pane" on page 269 <i>Universal CMDB Discovery and Integrations Content Guide</i>

Adapter Source Editor Window

Enables you to edit an adapter script.


To access	Right-click an adapter in the Resources pane and select Edit Adapter Source .
See also	"Resources Pane" on page 285

User interface elements are described below:



UI Element (A–Z)	Description
	Find text. Enables you to find specific text in the adapter definition. For details, see "Find Text Dialog Box" on page 273 .
	Go to line. Enables you to jump to a specific line in the adapter definition. In the Go To Line dialog box, enter the line number, and press ENTER .
	<p>Open External Editor. Opens the adapter definition in an external text editor.</p> <p>Prerequisite: Click the Edit the External Editor Preferences  button to define the path to an external editor. If no external editor path is defined, you will be prompted to provide one when you try to open the external editor.</p>
	<p>Edit the External Editor Preferences. Click to edit the external editor preferences. You can run the editor by adding flags to the path.</p> <p>Note: You cannot specify the file name. Instead, you can use flags relevant to your external editor to retrieve the file name, such as :file.</p> <p>In the following example, :file sets the place of the file in relation to the flags.</p> <div data-bbox="472 932 1341 1167" data-label="Image"> </div> <p>If no flags are defined, the file name is automatically added to the end of the path.</p>
	Switch Editor Mode. Enables you to switch between the default advanced editor and a simple text editor.
Validation Information	<p>Displays if the definition is valid or not:</p> <ul style="list-style-type: none"> • . Indicates that the definition is valid. • . Indicates that there is an error in the definition. • . Indicates that the definition could not be validated. <p>Note: This may occur due to an internal error while performing the validation. This does not, under any circumstances, harm the process of saving your definition to the server. See %temp%\UcmdbLog\error.log for details. For further assistance, contact Support.</p>

Attributes Assignment Editor Dialog Box

Enables you to define a regular expression that discovers specific running software according to a CIT's attribute value.

To access	In the Software Identification Rule Editor dialog box, click  .
Relevant tasks	"How to Discover Running Software – Scenario" on page 473
See also	"Software Identification Rule Editor Dialog Box" on page 290

User interface elements are described below:

UI Element (A–Z)	Description
Attribute assignments for Type	<p>Enables you to manage rules that discover a CIT according to an attribute. The attribute is defined according to a regular expression.</p> <ul style="list-style-type: none"> . Enable you to add/edit/remove an attribute assignment. Name. Choose from the list of attributes of the CIT selected in the editor. This attribute name is replaced by the value found by the regular expression. To find an attribute, start typing the name. Type. The type of operation defined for the attribute, for example, Boolean, string, date, and so on. Value. The value that replaces the name in the Rule ID field in the Parse Rule Editor dialog box (see "Parsing Rules" below). <p>Use the following syntax for the value:</p> <pre> <code>\${<rule ID name>(<group number>)}</code> </pre> <p>For example, <code>\${DB_SID(1)}</code> means that DFM should search for the Rule ID with the name DB_SID and retrieve its regular expression.</p> <p>DFM should then retrieve the code for the first group (1). For example, in the regular expression <code>.+ls+(lw+)\$</code>, the first group is <code>(lw+)\$</code>, that is, a word or words that appear at the end of the line.</p>
Parsing Rules	<p>Enables you to manage parsing rules that match attribute to process-related information.</p> <p>Note: Only users with a knowledge of regular expressions should make changes to a parse rule.</p> <ul style="list-style-type: none"> . Enable you to add/edit/remove a parsing rule.


UI Element (A–Z)	Description
	<ul style="list-style-type: none"> • Rule ID. The name of the rule. The Rule ID must be unique. It is needed to identify the rule in the Attributes Assignment Editor pane. • Process Attribute. The rule is invoked on the selected process-related attribute. • Regular Expression. Enables you to create a dynamic expression that finds at least one process that defines this running software. The regular expression is invoked on the value in the Process Attribute field. <p>For example, a command line process includes the following regular expression:</p> <pre>.+ls+(w+)\$</pre> <p>This expression searches for any character, followed by a space or spaces, followed by a word or words (a-z or A-Z or 0-9) that appear at the end of the line.</p> <p>The following command line matches this regular expression:</p> <pre>c:\ora10\bin\oracle.exe UCMDB</pre>

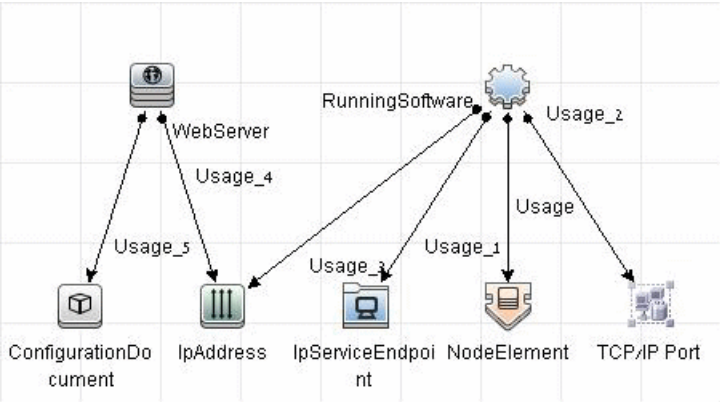
Choose Discovered Class Dialog Box

Enables you to choose CITs that are to be discovered by a selected adapter and to limit links so that they are mapped only when they connect specific CITs.

To access	<p>Select Data Flow Management > Adapter Management > Resources pane > an adapter.</p> <ul style="list-style-type: none"> • In the Adapter Definition tab > Discovered CITs pane, click the Add Discovered CIT button. • In the Adapter Configuration tab > Results Management pane, select the Enable Automatic deletion check box and click the Add button in the Automatic Deletion pane.
------------------	--

User interface elements are described below:

UI Element (A–Z)	Description
Link	<p>Enables DFM to discover CITs only when they are linked by link types you choose in this box.</p> <p>Select a link type from the list and click the  button in the End 1 and End 2 boxes to open the Choose Configuration Item Type dialog box. Choose the CITs that DFM should map when they are linked by the selected link type.</p>

UI Element (A–Z)	Description
	<p>DFM automatically recognizes the links between CIs and adds them to the map of discovered CITs. However, during adapter writing, you may need to exclude links between certain CITs.</p> <p>For example, both nodes and IPs and nodes and ports are linked by usage. You might need to receive results only for those nodes and IPs that are connected by the usage link, and not for nodes and ports. The End 1 and End 2 links determine the result received from the adapter, and this result is reflected in the map, as can be seen in the following example:</p>  <p>Note: This section is relevant only when adding a discovered CIT, not for defining CITs for automatic deletion.</p>
Object	Select a CIT to be added to the list of CITs that an adapter is to discover. Save the changes by clicking the Save button at the bottom of the Adapter Definition pane.






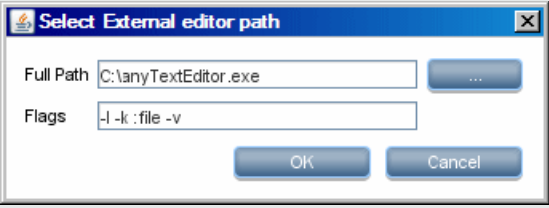



Configuration File Pane

Enables you to edit a specific configuration file that is part of a package. For example, you can edit the **portNumberToPortName.xml** file so that specific port numbers, names, or types are discovered.

To access	Click a specific configuration file in the Resources pane.
Important Information	<p>The Editor is sensitive to the type of file (.xml, .properties, or .groovy) and displays words with context specific meanings as highlighted text.</p> <p>The following files are for internal use only and should only be changed by users with an advanced knowledge of adapter-writing:</p> <ul style="list-style-type: none"> • discoveryPolicy.xml


	<ul style="list-style-type: none"> • jythonGlobalLibs.xml <p>For details, see "How to Define Discovery Rules" on page 306 and "Internal Configuration Files" on page 295.</p>
--	--

User interface elements are described below:


UI Element (A–Z)	Description
	Find specific text in the configuration file. For details, see "Find Text Dialog Box" on page 273 .
	Click to go to a specific line in the configuration file. In the Go To Line dialog box, enter the line number.
	Click to opens the configuration in an external text editor. Prerequisite: Click the Edit the External Editor Preferences  button to define the path to an external editor. If no external editor path is defined, you will be prompted to provide one when you try to open the external editor.
	<p>Edit the External Editor Preferences. Click to edit the external editor preferences. You can run the editor by adding flags to the path.</p> <p>Note: You cannot specify the file name. Instead, you can use flags relevant to your external editor to retrieve the file name, such as :file.</p> <p>In the following example, :file sets the place of the file in relation to the flags.</p> <div style="border: 1px solid gray; padding: 10px; margin: 10px 0;">  </div> <p>If no flags are defined, the file name is automatically added to the end of the path.</p>
	Click to toggle between the advanced editor and a simple text editor. You can use the simple editor when the advanced editor causes problems.
	For XML files, signifies that the code is valid.
	For XML files, signifies that the code is not valid.




Edit Process Dialog Box

Enables you to add a process that can identify specific running software.

To access	In the Software Identification Rule Editor dialog box, in the Identifying Processes pane, click Add  .
Relevant tasks	"How to Discover Running Software – Scenario" on page 473
See also	<ul style="list-style-type: none"> • "Attributes Assignment Editor Dialog Box" on page 267 • "Software Identification Rule Editor Dialog Box" on page 290

User interface elements are described below:



UI Element	Description
Name	<p>The name of the processes that can identify specific running software, for example, java.exe.</p> <ul style="list-style-type: none"> • Select Starts with to use a process that starts with the string entered in this field. • Select Ignore Case to ignore the case of the string entered in this field.
Port	<p>The port number or name.</p> <p>Enter the port number or click Add  to select the ports in the Global Ports List.</p> <ul style="list-style-type: none"> • If the process has to listen at a specific port, the port should be listed. You can enter more than one port, separated by commas, for example, 8888,8081,8080,81,8000,82,80. • If the process does not have to listen at a specific port (that is, the running software can use any port), select the All Ports option. <p>Note: To enable discovery of processes that are not listening at any of the ports entered in the Port field (that is, identification is by process name only), select Port match is optional.</p> <p>If Port match is optional is not selected, processes are discovered based on the process name and the port number entered in the Port field.</p>
Command Line	<p>The running software can also be mapped using the process name. In this case, you must add a process command line (or part of it) with which the process name uniquely identifies the software, for example, c:\ora10\bin\oracle.exe UCMDB.</p>
Owner	<p>The name of the user that must run the matching process.</p>

UI Element	Description
Service Endpoint Name	The name of port to be reported as an IpServiceEndpoint CI linked to discovered RunningSoftware and used to discover the port number.
Main process	Select this check box to mark this process as a unique and distinguishing process. For such processes there need to be several instances of the software CI.
Key Process	Select this check box if, during discovery, Universal Discovery must distinguish between applications that run similar processes (for example, IP, port, command line, or owner). For an explanation of this box, see " Identifying Running Software by Processes " on page 224.
Parsing Rules	<p>Enables you to manage parsing rules that match attribute to process-related information.</p> <p>Note: Only users with a knowledge of regular expressions should make changes to a parse rule.</p> <ul style="list-style-type: none">    Enable you to add/edit/remove a parsing rule. Rule ID. The name of the rule. The Rule ID must be unique. It is needed to identify the rule in the Attributes Assignment Editor pane. Process Attribute. The rule is invoked on the selected process-related attribute. Regular Expression. Enables you to create a dynamic expression that finds at least one process that defines this running software. The regular expression is invoked on the value in the Process Attribute field. <p>For example, a command line process includes the following regular expression:</p> <pre>.+ \s+(w+)\$</pre> <p>This expression searches for any character, followed by a space or spaces, followed by a word or words (a-z or A-Z or 0-9) that appear at the end of the line.</p> <p>The following command line matches this regular expression:</p> <pre>c:\ora10\bin\oracle.exe UCMDB</pre>


Find Resource/Jobs Dialog Box

Enables you to build a search query to find a particular resource or job.

To access	Do one of the following: <ul style="list-style-type: none"> Select Universal Discovery > Discovery Modules/Jobs > Discovery Modules
------------------	---

	<p>tree. Click the Find Job  button.</p> <ul style="list-style-type: none"> • Select Adapter Management > Resources pane. Click the Find resource  button.
See also	"Resources Pane" on page 285

User interface elements are described below:


UI Element (A–Z)	Description
	<p>Click to select a CIT from the dialog box that opens. Click OK to return to the Find Resource dialog box.</p> <p>Note: This button is not accessible when Name is selected.</p>
Direction	Searches forwards or backwards through the packages.
Find All	Click to highlight all instances of the text entered in Name .
Find Discovery Job by/ Find Discovery resource by	<p>Choose between:</p> <ul style="list-style-type: none"> • Name. Enter the name, or part of it, of the resource. • Input type/Adapter input type. CIs that trigger the job. Click the button to open the Choose Configuration Item Type dialog box. Locate the CI type that you are searching for. • Output type/Adapter output type. CIs that are discovered as a result of the job or the adapter.
Find Next	The next job/resource meeting the search criteria is highlighted in the Discovery Modules/Resources pane.

Find Text Dialog Box

Enables you to find text in a script or configuration file.

To access	Select a script or configuration file and click the Find text button in the file pane.
------------------	---

User interface elements are described below:

UI Element (A–Z)	Description
	<ul style="list-style-type: none"> Click Find to find one instance of the text you are searching for. Click Find All to find all instances of the text.
Direction	Search forwards or backwards through the script or configuration file.
Find what	<p>Type the text to be found or click the down arrow to choose from previous searches.</p> <p>Click the adjacent arrow to display a list of symbols you can use in wildcard or regular expression searches. This arrow is enabled when you select the Use option.</p>
Options	Select an option to narrow your search.
Origin	Enables a search of the entire scope or from the current cursor position.
Target	<ul style="list-style-type: none"> Global. Searches throughout the file. Selected Text. Searches through the selected text.

Input Query Editor Window

Enables you to define which CIs can be Trigger CIs for jobs that run a specific adapter.

To access	Select Data Flow Management > Adapter Management > select an adapter > Adapter Definition tab > Input pane, and click the Edit Input Query button next to the Input Query box.
Important information	To ensure that the Data Flow Probe is always kept up to date with possible changes to the Trigger CI data, you can configure UCMDB to periodically recalculate the Trigger CI data and send any changes to the Data Flow Probe. For details, see "How to Configure Periodic Data Flow Task Updates" on page 68 . This option is disabled by default because it can interfere with performance.
See also	<ul style="list-style-type: none"> "Trigger CIs and Trigger Queries" on page 27 "Trigger Query Editor Window" on page 501

User interface elements are described below:

UI Element (A–Z)	Description
<Panels>	<ul style="list-style-type: none"> "CI Type Selector Pane" on the next page "Editing Pane" on the next page

UI Element (A–Z)	Description
	<ul style="list-style-type: none"> • "Information Pane" on the next page
Query Name	The name of the adapter's Input query.

CI Type Selector Pane

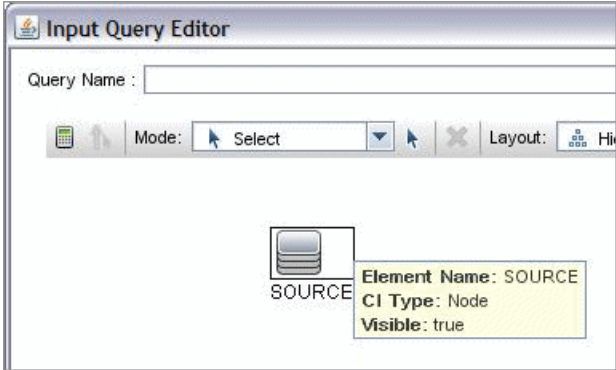
Displays a hierarchical tree structure of the CI Types found in the CMDB. For more details, see "CI Type Manager User Interface" in the *Universal CMDB Modeling Guide*.

Note: The number of instances of each CIT in the CMDB is displayed to the right of each CIT.

To access	To create or modify a query, click and drag nodes to the Editing pane and define the relationship between them. Your changes are saved to the CMDB. <p>Note: Each time you select the same object from the tree, you must rename the object node to have a unique name.</p>
Relevant tasks	<ul style="list-style-type: none"> • "How to Define a TQL Query" in the <i>Universal CMDB Modeling Guide</i> • "How to Create a Pattern View" in the <i>Universal CMDB Modeling Guide</i>
See also	"How to Add Query Nodes and Relationships to a TQL Query" in the <i>Universal CMDB Modeling Guide</i>

Editing Pane

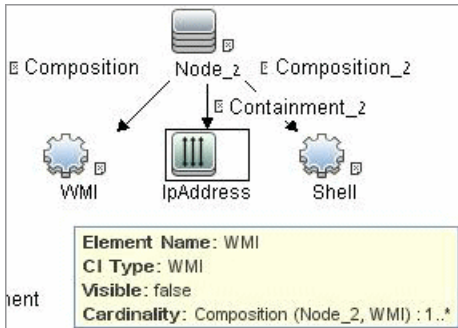
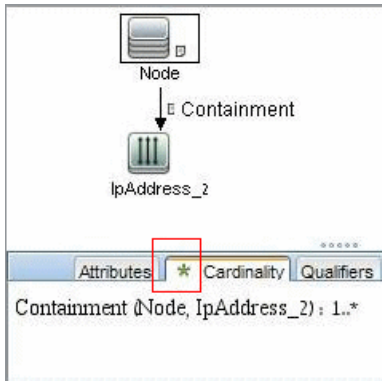
User interface elements are described below:

UI Element (A–Z)	Description
<node>	Hold the cursor over a node to view information about the node: 

UI Element (A-Z)	Description
<right-click menu>	For details, see "Shortcut Menu Options" in the <i>Universal CMDB Modeling Guide</i> .
<Toolbar>	For details, see "Toolbar Options" in the <i>Universal CMDB Modeling Guide</i> .


Information Pane

Displays the properties, conditions, and cardinality for the selected node and relationship.

Important Information	<p>Hold the pointer over a node to view information:</p>  <p>Element Name: WMI CI Type: WMI Visible: false Cardinality: Composition (Node_2, WMI) : 1..*</p> <p>A small green indicator is displayed next to the tabs that include information:</p> 
------------------------------	---


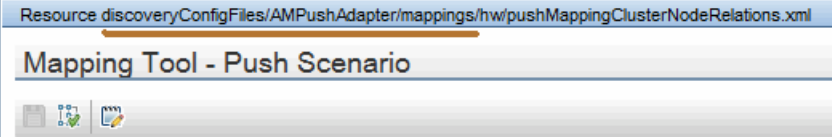
User interface elements are described below:

UI Element (A-Z)	Description
Attributes	Displays the attribute conditions defined for the node or the relationship. For details, see "Attribute Tab" in the <i>Universal CMDB Modeling Guide</i> .




UI Element (A-Z)	Description
Cardinality	Cardinality defines how many nodes you expect to have at the other end of a relationship. For example, in a relationship between node and IP, if the cardinality is 1:3, the query retrieves only those nodes that are connected to between one and three IPs. For details, see "Cardinality Tab" in the <i>Universal CMDB Modeling Guide</i> .
Details	<ul style="list-style-type: none"> • CI Type. The CIT of the selected node/relationship. • Visible. A tick signifies that the selected node/relationship is visible in the topology map. When the node/relationship is not visible, a box  is displayed to the right of the selected node/relationship in the Editing pane: <div data-bbox="441 701 808 999" data-label="Diagram"> </div> <ul style="list-style-type: none"> • Include subtypes. Display both the selected CI and its descendants in the topology map. <p>Note: To change the visible and subtype settings, select a node in the Editing pane and click the Edit button. In the Query Node Properties dialog box, select or clear the boxes.</p>
Edit button	Select a node or relationship in the Editing pane and click the Edit button to open the Query Node Properties dialog box. For details, see "Query Node/Relationship Properties Dialog Box" in the <i>Universal CMDB Modeling Guide</i> .
Qualifiers	Displays the qualifier conditions defined for the node or the relationship. For details, see "Qualifier Tab" in the <i>Universal CMDB Modeling Guide</i> .
Selected Identities	Displays the element instances that are used to define what should be included in the query results. For details, see "Identity Tab" in the <i>Universal CMDB Modeling Guide</i> .

Mapping Tool Editor Window

Enables you to configure value and field mappings in a visualized way for complex integration configurations for data push, population, or federation integration scenarios.

<p>To access</p>	<p>Select Data Flow Management > Adapter Management > Select a specific adapter in the Resources pane > Expand the Configuration Files folder:</p> <ul style="list-style-type: none"> • Click a mapping file and click Yes in the popup window that asks if you want to open the configuration file with the new mapping tool editor • Right-click a mapping file and select Open Mapping Tool from the context menu • If you chose to open the mapping file with the XML editor, you can switch to the Mapping Tool by clicking the Open Mapping Tool  icon at the top of the Script pane <p>Or, in the Configuration Files pane, double click a mapping file and click Yes in the pop-up window that asks if you want to open the configuration file with the new mapping tool editor.</p>
<p>Important information</p>	<p>The Mapping Tool window title bar includes the actual physical location of the script. For example, the following script is located in</p> <p>C:\hp\UCMDB\DataFlowProbe\runtime\probeManager\discoveryConfigFiles\AMPushAdapter/mappings (or probeGateway\AMPushAdapter/mappings)</p> 
<p>See also</p>	<ul style="list-style-type: none"> • "How to Create and Configure Mapping Files Using the Visual Mapping Tool" on page 239

User interface elements are described below:

UI Element (A–Z)	Description
	<p>Save. Saves the changes you made to the mapping file.</p>
	<p>Validate Mapping File. Validates the mapping file you created, edited, or modified.</p>
	<p>Open XML Editor. Enables you to switch back to the default script editor.</p>
<p><Panes></p>	<ul style="list-style-type: none"> • Local Query Pane • (Local Query) Attributes Pane • Visual Mapping Pane • External Class Model Pane








UI Element (A–Z)	Description
	<ul style="list-style-type: none"> • (External Class Model) Attributes Pane • XML Editor Pane

Local Query Pane

Displays a hierarchical tree structure of the local TQL query in the CMDB.

Relevant tasks	<ul style="list-style-type: none"> • "How to Define a TQL Query" in the <i>Universal CMDB Modeling Guide</i> • "How to Create a Pattern View" in the <i>Universal CMDB Modeling Guide</i>
See also	"How to Add Query Nodes and Relationships to a TQL Query" in the <i>Universal CMDB Modeling Guide</i>



User interface elements are described below:

UI Element	Description
	Query: <Query Name> . Displays the name of the currently selected integration TQL query found in CMDB.
	Add TQL Queries. Opens the Add Queries dialog box, enabling you to select and add available integration TQL queries from the Available items pane to the Selected items pane, so that you can map items from them.
	Refresh TQL Query Representation. Refreshes the query representation.
	Expand All. Expands the entire hierarchical tree structure to display all of the items available under the integration TQL queries.
	Collapse All. Collapses the hierarchical tree structure, leaving the top-level integration TQL query showing.
 (for Population or Federation scenario)	Add Node to Mapping for Population scenario. Enables you to add the selected node to the mapping.
 (for Push scenario)	Add Node to Mapping for Push and Federation scenarios. Enables you to add the selected node to the mapping.

(Local Query) Attributes Pane

The Attributes pane for the Local Query pane displays attributes of a local integration TQL query.





User interface elements are described below:










UI Element (A–Z)	Description
 (for Population or Federation scenario)	Add Attribute to Mapping. Enables you to add the selected attribute to the mapping.
 (for Push scenario)	Add Attribute to Mapping. Enables you to add the selected attribute to the mapping.
<Attributes table>	<p>The Attributes table contains the following columns:</p> <ul style="list-style-type: none"> • Status. Status of an attribute. • Display name. Display name of an attribute. • Name. Name of an attribute. • Type. Type of an attribute. • Description. Detailed description of an attribute.






Visual Mapping Pane

Allows you to establish mappings for items you selected from the Local Query pane and the External Class Model pane in a visual way.

User interface elements are described below:

UI Element (A-Z)	Description
	Update Info Tag. Opens the Update Info Tag dialog box, enabling you to modify and update the information about the data repositories being integrated, including Name, Version, and Vendor for both source and target data repositories.
	Update Import Tag. Opens the Update Import Tag dialog box, enabling you to select and add available items and import new groovy scripts. You can also move up or down the sequence of a script to decide the order of scripts to be imported.
	<p>Update Optional Tags. Opens the Update Optional Tags dialog box, enabling you to update optional tags by defining values for the Type, Is Valid, and Is Deleted fields. You can also select the Show Warning check box to display warning messages.</p> <p>Note: This button is not available for the source_instance element.</p>
	Add For Each Tag. Opens the Add For Each Tag dialog box, enabling you to define the source and the index for the tag that you want to add for each child mappings under the current parent entity:





UI Element (A-Z)	Description
	<ul style="list-style-type: none"> • Source Entities. Defines the source entities for the tag. • Count Index. Defines the start index when iterating over the source entities. • Var Name. (Optional) Specifies the variable name for the tag.
	<p>Add Variable Tag. Opens the Add Variable Tag dialog box, enabling you to define and add variable tags to the selected variable element:</p> <ul style="list-style-type: none"> • Name. Specifies name for the variable. • Type. Select a value from the drop-down list as type of the variable. • Value. Specifies a value for the variable. <p>Note: This button is not available for the source_instance element.</p>
	<p>Add Custom Section. Enables you to add an empty mapping element, where you can manually define a new mapping element that may not fall into any of the existing mapping categories.</p>
	<p>Revert Changes. Allows you to revert the changes you just made.</p>
	<p>Clear Entire Mapping. Enables you to clear the entire mapping.</p>
	<p>Remove Node. Enables you to remove a selected node or attribute mapping association from the mapping file.</p>
	<p>Expand All. Expands the entire hierarchical tree structure to display all of the mapping elements.</p>
	<p>Collapse All. Collapses the hierarchical tree structure, leaving the top-level integration mapping showing.</p>
<p><Groovy Function Viewer></p>	<p>Each time you select a target mapping that contains a groovy function, this component is displayed.</p> <p>Also, when you edit a target mapping and fill in some groovy function, you can preview the code of that function.</p> <p>Note: The current version supports only one function per line.</p>
<p><In the Visual Mapping pane></p>	<p>The visual representation of mapping relationship elements inside the Visual Mapping pane are described below:</p> <ul style="list-style-type: none"> •  - Represents the root integration tag in the Visual Mapping pane. •  - Represents a source_instance root element. The Root Element Name



UI Element (A-Z)	Description
	<p>attribute field is editable in the Visual Mapping pane.</p> <ul style="list-style-type: none"> •  - Represents a target_entity element. This is the default icon. The icon of any target_entity can be customized at the adapter level. For details, see Configure Icons for Mapping Entities. •  - Represents a variable mapping element. The Name attribute, Datatype, and Value attribute fields are all editable. When you edit the value in the Value attribute field, the groovy function viewer shows up, allowing you to view the XML script for the groovy function. •  - Represents an attribute mapping of the target_mapping element. <ul style="list-style-type: none"> ◦ For population and federation scenarios, the name value is read-only, and the Value attribute field is editable. ◦ For push scenario, both the Name attribute and Value attribute fields are editable. •  - Represents a for-each-source-entity tag. You can define values for the Source Entities attribute, Count Index attribute, and Var Name attribute fields. •  - Represents a custom tag that you define.

External Class Model Pane

Displays a hierarchical tree structure of the external class model.

User interface elements are described below:




UI Element	Description
	Refresh External Class Model. Refreshes the external class model.
	Expand All. Expands the entire hierarchical tree structure to display all of the items available under the external class model.
	Collapse All. Collapses the hierarchical tree structure, leaving the top-level external class model showing.
	Add New CI Type to External Class Model. Opens the Add New CI Type to External Class Model dialog box, enabling you to define the following properties for a new CI type so as to add the new CI type to the external class model:


UI Element	Description
	<ul style="list-style-type: none"> • Name. Specify the name for the new CI type. • Description. (Optional) Detailed description of the CI type. <p>Note: This button is enabled only if the adapter setting enable.classmodel.changes is set to true inside the Adapter Source Editor.</p>
 (for Push scenario)	Add Node to Mapping. Enables you to add the selected node to the mapping.
 (for Population or Federation scenario)	Set Node as Root Element. Enables you to set the selected node as root element in the mapping.

(External Class Model) Attributes Pane

The Attributes pane for the External Class Model displays attributes of an external class model.




User interface elements are described below:

UI Element (A–Z)	Description
 (for Push scenario)	Add Attribute to Mapping. Enables you to add the selected attribute to the mapping.
 (for Population or Federation scenario)	Add Attribute to Mapping. Enables you to add the selected attribute to the mapping.
	<p>Add New Attribute to Selected External Node. Opens the Add New Attribute dialog box, enabling you to define the following properties for a new attribute so as to add it to the selected external node:</p> <ul style="list-style-type: none"> • Name. Specify the name for an attribute property. • Display Label. Specify the display label for an attribute property. • Description. (Optional) Detailed description of the attribute property. • Type. Select a value from the drop-down list as type of the attribute property. <p>Note: This button is enabled only if the adapter setting enable.classmodel.changes is set to true inside the Adapter Source Editor.</p>

UI Element (A–Z)	Description
	Editor.
<Attributes table>	<p>The Attributes table contains the following columns:</p> <ul style="list-style-type: none"> • Status. Status of an attribute.  indicates that the concerning attribute is marked as Mandatory inside the adapter configuration. • Display name. Display name of an attribute. • Name. Name of an attribute. • Type. Type of an attribute. • Description. Detailed description of an attribute.

XML Editor Pane

User interface elements are described below:

UI Element	Description
	Find Text. Opens the Find Text dialog box, enabling you to find text in the selected script file. For more information, see "Find Text Dialog Box" on page 273 .
	Go to Line. Opens the Go To Line dialog box, enabling you to jump to a specific line in the script file. Enter the line number and press Enter .
	Save. Saves the changes you made to the mapping configuration file.
<Script Editing Pane>	Displays the XML script and allows you to edit the script manually. The script displayed in the XML Editor pane corresponds to the hierarchical tree element you selected in the Mapping UI pane.

Permission Editor Dialog Box

Enables you to configure an adapter you have written, so that users can view permissions for the job.




To access	Select Data Flow Management > Adapter Management > an adapter > Adapter Definition tab > Required Permissions pane, and click the Add button.
Important Information	The information you define here is not dynamic, that is, if an adapter is changed, the information in this dialog box is not updated.
See also	<ul style="list-style-type: none"> • "Discovery Permissions Window" on page 495 • "Viewing Permissions While Running Jobs" on page 467

	<ul style="list-style-type: none"> • "Adapter Definition Tab" on page 253 • "Discovery Module/Jobs – Details Tab" on page 486
--	---

User interface elements are described below:

UI Element (A–Z)	Description
Operation	The action that is being run.
Permission	Enter a name for the permission, to appear in the Required Permissions pane.
Usage Description	Free text that you enter to describe the permission object and its parameters. This text is usually a general comment on the type of permission object, whereas the description is a more specific comment. For example, you could enter Permissions for host machines here, and Permissions for host machines running on Windows for a particular row.

Permission Objects and Parameters Pane

UI Element (A–Z)	Description
	Click to open the Permission Object and Parameter pane. You can enter more than one object or parameter for each permission. The information you enter in this dialog box appears in the Required Permissions pane, in the Objects and Parameters column.
	Click to delete a permission object.
	Click to edit an existing permission object.
Context	Specific information about the permission object's environment, for example, Windows or UNIX.
Parameter	The parameters that are needed during the job run. For example, the UNIX permission object <code>cat</code> needs the <code>/etc/passwd</code> parameter.
Permission Object	The name of the command, table, or other content of the Jython script.



Resources Pane









Enables you to locate a specific package, adapter, script, configuration file, or external resource. You can also create an adapter, Jython script, configuration file, or Discovery activity, and you can import

an external resource.

To access	Select Data Flow Management > Adapter Management .
Important Information	<ul style="list-style-type: none"> Depending on the node you select in the Resources tree, different information is displayed in the right pane. If you select: <ul style="list-style-type: none"> One of the following folder nodes: Packages root, a specific package, an adapter, script, configuration file, or external resource: a list of the resources in that folder is displayed. To access a resource directly, double-click the resource in the View pane. An adapter: The Adapter Definition and Adapter Management tabs are displayed. For details, see "Adapter Definition Tab" on page 253 and "Adapter Configuration Tab" on page 259. A script or configuration file: The script editor is displayed. For details, see "Script Pane" on page 288. An external resource: Information about the file is displayed. You can view the history of discovery resources from the JMX console of the UCMDB Server. For details, see "How to View Discovery Resource History" on page 237.
See also	"Package Manager User Interface" in the <i>Universal CMDB Administration Guide</i> .

User interface elements are described below (unlabeled elements are shown in angle brackets>):

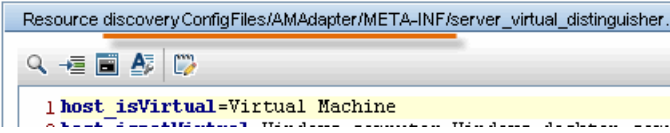
UI Element (A–Z)	Description
	<p>Create New Resource. Enables you to create a resource in a selected package. Select a resource, enter its details, click the ellipsis  button, and select a package to which to add the resource. If you do not select a package, the new resource is created in the <No Package> folder:</p> <ul style="list-style-type: none"> New Adapter. Enter the adapter name. Choose whether it should be used as a discovery adapter or for integration. For integration adapters, choose the integration type from the list of available types. Click OK. Edit the adapter. For details, see "Adapter Definition Tab" on page 253 and "Adapter Configuration Tab" on page 259. For details on moving an adapter to a package, see "How to Create a Custom Package" in the <i>Universal CMDB Administration Guide</i>. For details on creating integration adapters, see "Discovery and Integration Adapters" on page 25. New Jython script. Enter the script name. For details, see "Script Pane" on page 288. New Configuration File. Enter the configuration file name. By default, the file takes an .xml extension. To give the file another extension, for example, *.properties, name the file and include the extension. Add the appropriate XML code or other content. For XML files, you can save the file only if it is valid. For details, see

UI Element (A–Z)	Description
	<p>"Configuration File Pane" on page 269.</p> <ul style="list-style-type: none"> • Import External Resource. Opens the Select Resources to Import dialog box. <ul style="list-style-type: none"> ◦ Resources. Click the ellipsis  to locate the resources that you want to import. You can import more than one file by selecting multiple files at the same time. ◦ Package. Click the ellipsis  to locate the package that you want to contain the resources. ◦ Path. Enter a directory path for the resources. • New Discovery Wizard. Name the new wizard. By default, the file takes an .xml extension. The file is in template format. • New Scanner Configuration Configure the new scanner using the Scanner Configuration Generator wizard. For more information see section about the "Scanner Generator Wizard" on page 605. • Import Normalization Rules from Content Pack. Opens the Import Content Pack dialog box, enabling you to import the normalization rules files only that are contained in a Content Pack archive file. For more information about discovery rules that normalize data, see "Discovery Rules Engine Overview" on page 296.
	<p>Delete the Selected Item. Deletes the resource.</p>
	<p>Find Resource. Opens the Find Resource dialog box. For details on filtering, see "Filtering Discovery Results" on page 660.</p>
	<p>Refresh. Refreshes the list of packages.</p>
	<p>Packages tree. Displays a list of all packages.</p>
	<p>Package root. Displays a list of all resources included in the package. Expand the folders to see available resources:</p> <p>Right-click a resource to do one of the following:</p> <ul style="list-style-type: none"> • Save As. Enables you to clone an existing resource. The new resource includes all attributes of the existing resource. Give the resource a name, and click the ellipsis  button to select a package to which to add the resource. • Delete. Enables you to delete the resource. The resource is removed completely from the system. • Open in Frame. Enables you to view or edit the resource script in the Script Editor. Available for: Configuration files and scripts • Go to Discovery Job. Enables you to open the discovery job associated with the selected adapter in the Universal Discovery window



UI Element (A–Z)	Description
	<p>Available for: Adapters only. This option is enabled if the adapter is included in a discovery job.</p> <ul style="list-style-type: none"> • Go to Integration Point. Enables you to view and edit the integration point that uses this adapter in the Integration Studio. <p>Available for: Adapters only. This option is enabled if the adapter is used by an integration point.</p> <ul style="list-style-type: none"> • Edit Adapter Source. Enables you to view or edit the adapter's XML file in the Adapter Source Editor. For details, see "Adapter Source Editor Window" on page 265. <p>Available for: Adapters only</p>









Script Pane



Enables you to edit a specific script that is part of a package.

To access	Click a specific script in the Resources pane.
Important Information	<p>The script pane title bar includes the actual physical location of the script. For example, the following script is located in</p> <p>C:\hp\UCMDB\DataFlowProbe\runtime\probeManager\discoveryConfigFiles/AMAdapter/META-INF</p> <p>(or probeGateway\discoveryConfigFiles/AMAdapter/META-INF)</p> 
See also	Adapter Development and Writing in the <i>Universal CMDB Developer Reference Guide</i>

User interface elements are described below (unlabeled elements are shown in angle brackets>):




UI Element (A–Z)	Description
	Find text. Enables you to find specific text in the script definition. For details, see "Find Text Dialog Box" on page 273 .
	Go to line. Enables you to jump to a specific line in the script definition. In the Go To Line dialog box, enter the line number, and press Enter .

UI Element (A–Z)	Description
	<p>Open External Editor. Opens the script definition in an external text editor.</p> <p>Prerequisite: Click the Edit the External Editor Preferences  button to define the path to an external editor. If no external editor path is defined, you will be prompted to provide one when you try to open the external editor.</p>
	<p>Edit the External Editor Preferences. Click to edit the external editor preferences. You can run the editor by adding flags to the path.</p> <p>Note: You cannot specify the file name. Instead, you can use flags relevant to your external editor to retrieve the file name, such as :file.</p> <p>In the following example, :file sets the place of the file in relation to the flags.</p> <div data-bbox="516 751 1341 989" data-label="Image"> </div> <p>If no flags are defined, the file name is automatically added to the end of the path.</p>
	<p>Switch Editor Mode. Enables you to switch between the default advanced editor and a simple text editor.</p>
	<p>Open Mapping Tool. Enables you to open the new mapping tool window. See "Mapping Tool Editor Window" on page 277.</p> <p>Note: This icon is available for adapter mapping configuration files only.</p>
	<p>See "Validation Information" below.</p> <p>Note: This button is displayed when a script contains Framework API errors.</p>
<p><script definition></p>	<p>The Jython script used by the package. For details on working with Jython, see Create Jython Code in the <i>Universal CMDB Developer Reference Guide</i>.</p>
<p>Validation Information</p>	<p>Displays if the script definition is valid or not:</p> <ul style="list-style-type: none">  For Jython files, indicates that the script definition is valid.  For Jython files, indicates that the script definition is not valid, and displays the errors in the script.





UI Element (A–Z)	Description
	<p>For example:</p> <p>Script has failed validation.</p> <p>At line 48: <code>Factory.getProtocolProperty(found. This is a problem - Usage of Factory is deprecated. Use Framework.getProtocolProperty instead.</code></p> <p>Click , then OK to update the script.</p> <p>The error may occur due to changes in the Framework object's API. For details, see the <i>Universal CMDB Developer Reference Guide</i>.</p> <ul style="list-style-type: none">  For Jython files, indicates that the script definition could not be validated. <p>Note: This may occur due to an internal error while performing the validation. This does not, under any circumstances, harm the process of saving your definition to the server. See <code>%temp%\UcmdbLog\error.log</code> for details. For further assistance, contact Support.</p>




Software Identification Rule Editor Dialog Box

Enables you to define rules for managing discovered running software.

To access	<ol style="list-style-type: none"> Go to Data Flow Management > Universal Discovery > Discovery Modules/Jobs. In the Discovery Modules tree, select Hosts and Resources. Select a job under Basic Applications, or under Inventory Discovery > Basic Inventory. In the Properties tab, select Global Configuration Files > applicationsSignature.xml. Click Edit  to open the Software Library dialog box. In the Software Library dialog box, click Add  or select an existing element and click Edit .
Important Information	Each rule must be matched by at least one process.
Relevant tasks	"How to Discover Running Software – Scenario" on page 473
See also	"Global Configuration Files Pane" on page 258



User interface elements are described below:

UI Element	Description
Software Signature ID	<p>The name of the software signature.</p> <p>Note: This is not the running software's name but a name you give to differentiate this discovery from similar discoveries.</p>
Category	<p>You can:</p> <ul style="list-style-type: none"> • Choose the category under which the new running software should appear. • Change the category for an existing element. • Add a new category by typing its name in this field. <p>The changes you make here are immediately displayed in the Software Library dialog box.</p>
Supported versions	<p>Versions supported for this running software.</p>
Created CI Properties	<p>The properties of the created CIs:</p> <ul style="list-style-type: none"> • CI Type. The CIT that is to be discovered • Discovered Product Name. The name of the running software to be created by this signature. • Vendor. The vendor of this running software. • Installed Software. The regular expression used to match the application in the list of installed software on the target machine's operating system. • Additional Attributes. Attributes of the created CI. To manage the attributes, click . For details, see "Attributes Assignment Editor Dialog Box" on page 267.
Identifying Processes	<p>Lists the processes that can identify specific running software. The Edit Process dialog box opens. For details, see "Edit Process Dialog Box" on page 271.</p> <p> Add. Opens the Edit Process dialog box opens where you can define a new identifying process.</p> <p> Edit. Opens the Edit Process dialog box opens where you can modify the selected identifying process.</p> <p> Remove. Removes the selected identifying process.</p>
Linked Configuration Files	<p>Enables you to manage configuration files linked to the identification rule.</p>

UI Element	Description
	<p>Note: You can create parsing rules to define the paths to the configuration files. For details, "Attributes Assignment Editor Dialog Box" on page 267.</p> <p> Add. Creates a new row where you can add the path to a linked configuration file. Enter the full path to the running software's configuration file and the file name.</p> <p> Edit. Enables you to edit the path to the selected configuration file.</p> <p> Remove. Removes the selected configuration file.</p>







Software Library Dialog Box

Enables you to view the logical groups of running software.

To access	<p>Use one of the following:</p> <ul style="list-style-type: none"> • From Data Flow Management > Universal Discovery > Discovery Modules/Jobs: <ol style="list-style-type: none"> a. In the Discovery Modules tree, select Hosts and Resources. b. Select a job under Basic Applications, or under Inventory Discovery > Basic Inventory. c. In the Properties tab, select Global Configuration Files > applicationsSignature.xml. d. Click Edit . • From Data Flow Management > Adapter Management window: <ol style="list-style-type: none"> a. Select one of the Host_Resources_By_SNMP/TTY/WMI adapters. b. In the Adapter Definition tab > Global Configuration Files pane, select applicationsSignature.xml and click Edit .
Important Information	<p>The software elements are organized in logical categories. You can change the names of these elements, you can move an element to another category, and you can define new elements and categories. For details, see the Category entry in "Software Identification Rule Editor Dialog Box" on page 290.</p> <p>The code you define in this dialog box and the Software Element Editor dialog box overwrites the code in applicationsSignature.xml.</p>
Relevant tasks	<p>"How to Discover Running Software – Scenario" on page 473</p>

See also	"Global Configuration Files Pane" on page 258
-----------------	---

User interface elements are described below (unlabeled elements are shown in angle brackets):

UI Element (A–Z)	Description
	Select a check box to include a category or software element in the discovery. Clear a check box to remove the category or element from the discovery.
	Add. Opens the Software Identification Rule dialog box, enabling you to define a new software element. For details, see "Software Identification Rule Editor Dialog Box" on page 290 .
	Export Application Signature to XML. Enables you to export the application signature of the selected software element to an xml file.
	Import Application Signature from XML. Enables you to import an application signature from an xml file to the selected software element.
	Edit. Opens the Software Identification Rule dialog box, enabling you to modify the selected software element. For details, see "Software Identification Rule Editor Dialog Box" on page 290 .
	Remove. Removes the selected software element from the library.
<List of software elements>	List of objects that are software elements.




Global Filtering Dialog Box

Global filtering enables you to filter Probe results for all adapters, so that only results of interest to you are sent to the UCMDB Server.

To access	In Adapter Management , do the following: <ol style="list-style-type: none"> 1. In the Resources tree, expand the DDMiInfra node and then expand the Configuration Files node. 2. Right-click GlobalFiltering.xml and select Open in Frame.
Important Information	Before creating a filter, perform an analysis on what information you want to filter and what data elements contains the information you want to filter.
Relevant tasks	"Configure Filtering in UCMDB" on page 579

See also	Configuration Items (CIs) in the <i>Universal CMDB Administration Guide</i> . "Configure Filtering Using the globalFiltering.xml File" on page 231
-----------------	---

User interface elements are described below:

UI Element	Description
	Select CI. Opens the Select CI dialog box, enabling you to select a UCMDDB CI. Available when: Include or Exclude is selected in the left pane.
	Select an Attribute. Opens the Select an Attribute dialog box, enabling you to add a filter to an attribute for the selected UCMDDB CI. <ul style="list-style-type: none"> • Attribute. Select an attribute from the drop down list. • Display Label. Name of the attribute. • Type. Data type of the attribute as it appears in the CI Type Manager. For more information, see CI Type Manager in the <i>Universal CMDB Modeling Guide</i>.
	Enables you to delete the selected UCMDDB CI or the attribute.

Global Filtering Configuration Settings

Enables you to activate filtering. It also enables you to define the behavior of filtering.

Important information	These settings apply to all included and excluded filters.
------------------------------	--

User interface elements are described below:

UI Element	Description
Activate	Enables you to activate filters. <ul style="list-style-type: none"> • Yes. Filters are activated. • No. Filters are not activated. Default: Yes
Recursive Filtering	Defines a filtering behavior in which filters are applied to CIs that are linked to CIs that have been filtered. Using global filtering, you can filter out a CI so that it is not included in the filter results. This CI may be a root CI, containing other CIs or relationships. By default, during the filter process, the contained CIs and relationships, as well as any CIs related to them,

UI Element	Description
	<p>are added to the filter results—including the root CI. This causes undesired filter results. Recursive filtering corrects this by ensuring that if a root CI is filtered out, then any contained CIs or relationships are filtered out too, such that the root CI cannot be found again.</p> <p>Default: No</p>

Attribute Editor

Enables you to define properties of attributes that you want filtered.

Important information	This page is displayed when an attribute is selected in the left pane.
------------------------------	--

User interface elements are described below:

UI Element	Description
Operator	Click the drop-down list to display a list of operator types.
Value	<p>Type a function that is appropriate for the operator type.</p> <p>The function must return a value.</p>

Internal Configuration Files

The following files are for internal use only and should be changed only by users with an advanced knowledge of content writing.

Configuration File	Description	Location
discoveryPolicy.xml	Includes the schedule when the Probe does not execute tasks. For details, see "New/Edit Policy Dialog Box" on page 103 .	Data Flow Management > Adapter Management > Packages > AutoDiscoveryInfra > Configuration Files
jythonGlobalLibs.xml	A list of default Jython global libraries that DFM loads before running scripts.	Data Flow Management > Adapter Management > Packages > AutoDiscoveryContent > Configuration Files

Chapter 8: Discovery Rules Engine

This chapter includes:

Discovery Rules Engine Overview	296
Discovery Rules Syntax	297
How to Define Discovery Rules	306
How to View Discovery Rules in JMX	307
How to Disable the Discovery Rules Engine	308

Discovery Rules Engine Overview

When Universal Discovery discovers data, the Discovery Rules Engine processes the given set of input CI and relationship data, and returns a set of output attribute values. The Discovery Rules engine enriches the discovered CI and relationship data with new data deduced from the discovered attributes.

For example:

- **Input:** A Node contains the string **Cisco** and the string **Version 12.3a**,
- **Output :** The operating system for the Node is recognized as **Cisco IOS Version 12.3(3a)**.

The Data Flow Probe then activates the Rules Engine to fill in additional information on the discovered data.

All discovery jobs use the discovery rules engine. Out-of-the-box rules are applied to data that can be completed by the discovery jobs (sys_object_id, mac_address, and so on). Moreover, you can add user-defined rules to the Discovery Rules Engine.

Limitations

- The Discovery Rules Engine completes only empty fields, it does not overwrite existing values.
- Rules are run according to a random order. User-defined discovery rules have no priority over out-of-the-box discovery rules. If the input suits more than one rule, the output is returned from the rule that ran first. It is important to ensure that rules are accurate (existing and new rules). If rules are accurate there is no need for prioritization. However, if a CI's property values match two rules that have a single input attribute of the same type (equals, oid-starts-with, regex), then the rule that has

more information (for example, a longer OID) will be preferred.

- There are no dependencies between rules. A field that was completed using the Discovery Rules Engine cannot be used as input for another rule.

Related Topics

- For details on the syntax of Discovery Rules, see ["Discovery Rules Syntax" below](#).
- For details on defining new rules, see ["How to Define Discovery Rules" on page 306](#).
- For details on viewing out-of-the-box rules, see ["How to View Discovery Rules in JMX" on page 307](#).
- To disable the Rules Engine on a particular population adapter, see ["How to Disable the Discovery Rules Engine" on page 308](#).
- For details on log files, see ["Data Flow Probe Log Files" on page 99](#).

Discovery Rules Syntax

This section describes the syntax of discovery rules. Discovery rules are supplied in an XML file. Some examples are presented here, and detailed descriptions explaining the syntax in these examples follow.

Example 1

The following rule sets attribute **vendor** to **hewlett_packard_co** for CIs with the **discovered_model** attribute equal to **HP2140**.

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<rules:normalization-rules name="My rules"
xmlns:rules="http://www.hp.com/ucmdb/1-0-0/NormalizationRules">
<rules:normalization-rule ci-type="node" id="1">
  <rule-input>
    <attribute name="discovered_model" value="HP 2140" compare-
type="equals"/>
  </rule-input>
```

```
<rule-output>
  <attribute name="vendor">
    <value>hewlett_packard_co</value>
  </attribute>
</rule-output>
</rules:normalization-rule>
</rules:normalization-rules>
```

Example 2

The following rule appends **desktop** to the **node_role** attribute list when a discovered node CI is connected to interface whose **mac_address** starts with **0020C0**.

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<rules:normalization-rules name="My rules"
xmlns:rules="http://www.hp.com/ucmdb/1-0-0/NormalizationRules">
<rules:normalization-rule ci-type="node" id="3481">
  <rule-input>
    <connected-ci link-type="composition" direction="forward" end-
type="interface">
      <connected-ci-attribute name="mac_address" value="0020C0" compare-
type="starts-with"/>
    </connected-ci>
  </rule-input>
  <rule-output>
    <attribute name="node_role">
      <values>
        <add>desktop</add>
      </values>
    </attribute>
  </rule-output>
</rules:normalization-rule>
```

```
</rules:normalization-rules>
```

Example 3

The following example sets the values of **os_description**, **os_vendor**, **os_family** attributes and appends **desktop** and **nt** to the **node_rule** attribute when a discovered node CI has the **discovered_os_name** starting with **Windows 2000 Professional**.

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<rules:normalization-rules name="My rules"
xmlns:rules="http://www.hp.com/ucmdb/1-0-0/NormalizationRules">
<rules:normalization-rule ci-type="node" id="2">
  <rule-input>
    <attribute name="discovered_os_name" value="Windows 2000 Professional"
      compare-type="starts-with"/>
  </rule-input>
  <rule-output>
    <attribute name="os_description">
      <value>windows_2000_professional</value>
    </attribute>
    <attribute name="os_vendor">
      <value>microsoft_corp</value>
    </attribute>
    <attribute name="os_family">
      <value>windows</value>
    </attribute>
    <attribute name="node_role">
      <values>
        <add>desktop</add>
      </values>
    </attribute>
    <class-type>nt</class-type>
```

```
    </rule-output>  
</rules:normalization-rule>  
</rules:normalization-rules>
```

Example 4 (link rules)

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>  
<rules:normalization-rules name="My rules"  
  xmlns:rules="http://www.hp.com/ucmdb/1-0-0/NormalizationRules">  
  <rules:normalization-rule id="2909" ci-type="containment">  
    <link-rule-input>  
      <attribute name="name" value="MyName" compare-type="starts-with"/>  
      <end1 ci-type="node">  
        <attribute name="description" value="MyDescription" compare-  
type="starts-with"/>  
      </end1>  
      <end2 ci-type="ip_address">  
        <attribute name="name" value="1.1.1.1" compare-type="starts-  
with"/>  
      </end2>  
    </link-rule-input>  
    <rule-output>  
      <attribute name="description">  
        <value>HP StoreOnce B6000</value>  
      </attribute>  
    </rule-output>  
  </rules:normalization-rule>  
</rules:normalization-rules>
```

Explanation of Examples

Element: <normalization-rules>

Description: Represents a set of discovery rules. It is the top element in the XML file.

Attributes:

- Description (optional)
- Name (required): a unique name of the rule set in the XML file.

Inner elements:

- <normalization-rule>

Element: <normalization-rule>

Description: This element represents a single discovery rule.

Attributes:

- id (required): This ID must be unique within the scope of the XML file. In the first example above, id=1. In the second example, id=3481.
- ci-type (required): the type of CI that the rule is applied to. In both examples above, ci-type=node.

Inner elements:

- <rule-input>
- <link-rule-input>
- <rule-output> (required)

Note: One or the other of the <rule-input> or <link-rule-input> elements must appear in the file, but not both.

Element: <rule-input>

Description: Defines conditions on CI attributes and on attributes of connected CI(s), used for matching between a discovered CI and the rule. For example, if you have the following rule input:

```
<rule-input>  
  <attribute name="discovered_model" value="HP 2140" compare-type="equals"/>  
</rule-input>
```

this rule would match a CI with an attribute **discovered_model = HP 2140**.

Inner elements:

- <attribute> (optional)
- <connected-ci> (optional)

Note: <rule-input> must have one of the inner elements above.

Element: <attribute>

Description: Defines a condition on a CI attribute.

Attributes:

- name (required): The name of the discovered CI attribute examined by the discovery rules engine.
- value (required): The value that the discovered CI attribute has to match.
- compare-type (required): Defines the kind of match comparison applied by the rule. It must be one of the following options:
 - a. **equals:** The value of the discovered attribute is equal to the value in the rule.
 - b. **starts-with:** The value of the discovered attribute starts-with the value in the rule.
 - c. **ends-with:** The value of the discovered attribute ends with the value in the rule.
 - d. **contains:** The value of the discovered attribute contains the value in the rule.
 - e. **regex:** The value of the discovered attribute matches a given regular expression in the rule.
 - f. **oid-starts-with:** Either the value of the discovered attribute is equal to the value provided in the rule or it starts with the concatenation of the rule value and the dot (.) character.

For example, if you have the following rule:

```
<attribute name="sys_object_id" value=".1.3.6.1.4.1.42" compare-type="oid-starts-with"/>
```

It is interpreted as either:

- value of "sys_object_id" is equal to ".1.3.6.1.4.1.42"
- or
- value of "sys_object_id" starts with ".1.3.6.1.4.1.42."

This means that the following values would match this rule:

- ".1.3.6.1.4.1.42"
- ".1.3.6.1.4.1.42.1"

but this value would not match the rule:

- ".1.3.6.1.4.1.421"

Element: <connected-ci>

Description: Defines conditions on a connected CI.

Attributes:

- link-type (required): The type of relationship between the discovered CI and the connected CI.
- direction (required): The relationship direction; which is either "forward" or "backward".
- end-type (required): The type of the connected CI.

Inner elements:

- <connected-ci-attribute>

Element: <connected-ci-attribute>

Description: Defines a condition on a connected CI attribute. Similar to the <attribute> element (described above) that defines conditions on the attribute of a CI, the <connected-ci-attribute> refers to an attribute of a connected CI. This element has the same structure as the <attribute> element.

Element: <link-rule-input>

Description: Defines conditions on link attributes and on attributes of its ends, used for matching between a discovered link and the rule.

Inner elements:

- `<attribute>` - Zero or more attribute conditions on the link. The same as the previous `<attribute>` element.
- `<end1>` (required)
- `<end2>` (required)

Element: `<end1>`

Description: Defines a condition on the first end of the link.

Attributes:

- `ci-type` (required): the type of the end CI

Element: `<end2>`

Description: Defines a condition on the second end of the link.

Attributes:

- `ci-type` (required): the type of the end CI

Inner elements (for both end1 and end2):

- `<attribute>` (optional): Zero or more attribute conditions on the end. The same structure as other `<attribute>` elements.

Element: `<rule-output>`

Description: Defines the output values set by the rule in the case of a match. It also can set the type of the discovered CI. The rule output contains a list of attributes. Each attribute contains one or more values, and the rule engine sets these values. The following is an example of rule output:

```
<rule-output>  
  <attribute name="vendor">  
    <value>hewlett_packard_co</value>  
  </attribute>  
</rule-output>
```

In the output above, the attribute “vendor” has one value, and the rule engine sets this value to “hewlett_packard_co”.

Sometimes, an attribute has a string_list type. In this case, the rule output can add a new value to the list, as shown in the following example:

```
<rule-output>
  <attribute name="node_role">
    <values>
      <add>desktop</add>
    </values>
  </attribute>
</rule-output>
```

In the example above, the value **desktop** is added to the list of **node_role** values.

Rule output can also set a CI type, as shown in the following example:

```
<rule-output>
  <class-type>nt</class-type>
</rule-output>
```

Inner elements:

- <class-type> (optional)
- <attribute> (optional)

Note: <rule-output> must have one of the inner elements above.

Element: <class-type>

Description: When used, defines the new type of the discovered CI.

Element: <attribute>

Description: Defines the attribute to be set in the case of a match.

Attributes:

- name (required): The name of the CI attribute that is set by this rule.

Inner Elements:

- <value>
- <values>

Element: <value>

Description: Defines the value of the output attribute.

Element: <values>

Description: Defines the values of the output attribute in the case of an attribute list. The given values are appended to the result list.

Inner Elements:

- <add>

Element: <add>

Description: Defines the value to be appended to the list of CI attribute values.


How to Define Discovery Rules

This task describes how to define a new discovery rule in the Discovery Rules Engine.

If you are working on an upgraded version of UCMDB, you can also edit user-defined rules from your previous version.

To learn more about the Discovery Rules Engine, see "[Discovery Rules Engine Overview](#)" on [page 296](#).

To add new user-defined discovery rules:

1. Go to **Adapter Management**.
2. In the Resources pane, click **New** , and select **New Configuration File**.

Enter a name for the new discovery rule. The name must begin with **ruleEngine/** and end with **.xml**.

For example: **ruleEngine/myRule.xml**.

3. In the Package field, select **NormalizationRules**.
4. In the Editor pane that opens on the right, enter the new rule.

An example of valid rules can be found under **NormalizationRules > Configuration Files**, in **ruleEngine/samples.xml**.

5. Click **OK**.

To edit an existing discovery rule from a upgraded version of UCMDB:

1. Go to **Adapter Management**.
2. In the Resources pane, select the **UserDefinedRules** package.
3. Under **Configuration Files**, select the .xml file for the rule that you want to edit.

Note:

- Rules that were defined in previous versions of UCMDB (for example in **oidToHostClass.xml**), can be found under the **UserDefinedRules** package, in the configuration file **UserDefinedOidToHostClass.xml**.
- Out-of-the-box **OidToHostClass** rules can be found under **NormalizationRules > External resources** in the **ruleEngine/snmp.gz** file.

How to View Discovery Rules in JMX

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

To search for a rule:

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

Command	Description
scanForSNMPRules	Retrieves SNMP discovery rules that apply to the specified input attributes. Note:

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

How to Disable the Discovery Rules Engine

All population adapters are set up, by default, to use the Discovery Rules Engine adapters.

To disable the Discovery Rules Engine for a particular population adapter:

- In **Adapter Management**, open the population adapter's configuration file (<adapter>.xml).
- Search for the following parameter: **normalizationRules isEnabled**
 - If you find it, ensure that the value is set to **false**.
 - If you do not find it, add the following line under the **taskinfo** tag: **<normalizationRules isEnabled="false"/>**

Part IV: Integrations

Chapter 9: Integration Studio

This chapter includes:

Integration Studio Overview	310
Integration in a Multi-Tenancy Environment	316
How to Work with Federated Data	317
How to Work with Population Jobs	318
How to Work with Data Push Jobs	320
How to Set Up an Integration Point	324
How to Save an Integration Point Configuration as an Adapter Default	326
How to Remove Adapter Defaults	329
How to Deploy a Package to a Remote Data Repository	330
How to Configure Probe IP Ranges with Active Directory	333
How to Increase the Number of Threads for Data Push Jobs	334
Integration Studio User Interface	335
Limitations – Integration Studio	362

Integration Studio Overview

The Integration Studio is where you manage your UCMDB integration points and connect and share information with external repositories, such as other CMDBs, IT Performance Suite products, or third-party products.

Integration with other products is performed over secure communication channels through Data Flow Probes.

Alternatively, if your remote managed data repositories are accessible from the UCMDB server machine, non-Jython-based integrations can be performed using the UCMDB Integration Service, enabling the Data Flow Probe resources to be used for other discovery tasks.

Note: The UCMDB Integration Service is supported in a standalone UCMDB environment only.

Integration points in the CMDB are based on adapters, which are entities that are capable of communicating with external data repositories. A basic set of adapters is provided with the CMDB;

however, you can create additional adapters using the Federation Framework SDK. For details, see "Add an Adapter for a New External Data Source" in the *Universal CMDB Developer Reference Guide*.

You can also create adapters in the Adapter Management module. For details, see "[Resources Pane](#)" on [page 285](#).

For details about how to set up integration points for data integrations, see "[Integration Studio Page](#)" on [page 348](#).

Note: The following OOTB adapters deployed **should not be deleted**:

- **HistoryDataSource** - A federation adapter of UCMDB with its history data. You can build TQL queries to check the history changes of CIs. For example, attribute changes.
- **UCMDBDiscovery** - Not a real adapter. It is based on the API adapter and its only usage is to allow you to configure reconciliation priority of all discovery jobs with other integrations jobs from other data sources.

Integration points can be of one of the following types:

- "[Population](#)" [below](#)
- "[Federation](#)" [on the next page](#)
- "[Data Push](#)" [on page 314](#)

Population

An integration of Population type copies data from an external data repository into the CMDB, so that the CMDB now controls the data.

You use population in one of the following scenarios:

- When you need to track changes made by the CMDB at the CI level.
- When a remote repository is not reliable in terms of response time; for example, a network delay prohibits you from setting up run-time federation with the repository.
- When a remote repository does not support federation capabilities (no appropriate adapter exists).

Federation

An integration of Federation type includes data in the CMDB from other sources in such a way that the source of the data still retains control of the data.

You use the CMDB's federation capabilities to extend the scope of the existing Topology Query Language (TQL) capabilities to encompass data that is stored and maintained in an external repository. The ability to include such information is important as it prevents you from having to copy large amounts of data and, instead, bring it into your CMDB only when it is really needed.

Federation also has the benefit that the federated data does not burden the CMDB in terms of capacity; theoretically, you can set up an integration that federates trillions of CIs and relationships. Federated data is fetched at runtime, as requested, which lessens the impact on system performance.

Note: The CMDB does not offer change tracking on federated data because the data does not reside within the CMDB and the CMDB is not notified when external data is modified.

Federated integration creates a federated integration point, which can then be used when defining TQL queries. For details on TQL, see "Topology Query Language" in the *Universal CMDB Modeling Guide*.

Note: Federation can be configured in Actual state only, but can be performed in either Actual or Authorized state.

Retrieving Data from Multiple Federated Data Sources

During TQL query calculation, you can retrieve data for the same CIT from several federated data sources. The data is retrieved from the local CMDB, as well as from other federated data sources, according to how you have configured integration points. As data arrives at the CMDB, it is identified and reconciled, with the end result determined according to the configured reconciliation priority given to the various integrations.

Each CI that is retrieved from an external data repository includes an attribute (**Created By**) to show from which federated data source the CI has been retrieved.

For limitations, see ["Limitations – Integration Studio" on page 362](#).

Retrieving Attributes from an External Data Repository

- You can retrieve the attributes of a CI from an external data repository, when the core CI data is

stored in the CMDB.

- The core data repository must be the CMDB.
- The CIT must be located in a data repository for its attributes to be defined.
- The same attributes can be retrieved from multiple data repositories.
- For details on retrieval options, see the CI Type Retrieval Mode field on the ["Federation Tab" on page 337](#).
- When you configure an integration point to include federated CIs, you must select full federation of a CI or the federation of an attribute alone. You cannot set up two integrations for the same CIT where one is mapped to an external CIT and the other is mapped to that same CIT with an external attribute.
- A CIT can support external attributes if the adapter (which is federating the CIT data) supports mapping information (reconciliation) for this CIT.

Reconciling Information

Federated queries should use the mapping file to reconcile the CI from the CMDB with the attributes from the external data repository.

For details on the Mapping Engine, see "Federation Framework Flow for Federated TQL Queries" in the *Universal CMDB Developer Reference Guide*.

For details on selecting attributes to be included in the federation, see ["Federation Tab" on page 337](#).

For details on how reconciliation is performed, see ["Data Reconciliation" on page 739](#).

Use Cases

- You need to discover the SMS or Altiris desktops in your system. The desktop CIT is a core CIT and is already synchronized with the CMDB. However, you do not want to store all the desktop data in the CMDB as this is inefficient and unnecessary. It is enough to store core attributes such as name and MAC address in the CMDB, and to define the other details of the desktops as external attributes in two data repositories: SMS and Altiris.
- VMware creates virtual machines that contain a virtual machine monitor (hypervisor) that allocates hardware resources dynamically and transparently. Multiple operating systems can run concurrently on a single physical computer. Since the allocation resources—for example, memory—are dynamic, DFM cannot discover these resources (DFM runs once every 24 hours and the resource data can change hourly). To enable UCMDB to always be updated with real-time data, the solution is to divide the data into two: the core data of the virtual hosts should be discovered and

placed in the CMDB; the resource attributes should be retrieved from the external source. In this use case, the data for these attributes is retrieved from two data repositories: CMDB and VMware.

Calculating Federated TQL Queries

When defining an adapter, you can specify whether calculation of TQL queries must be performed first on the CMDB (default) or whether it can start on the adapter.

As an example of a one-node adapter, if you have a TQL query of **Node > CPU** (with conditions on the federated CPU):

- If the calculation is performed first on the data in the CMDB:
 - The TQL query for Node is calculated in the CMDB, which retains all of the Node's data.
 - Then **Node > CPU** is calculated by the adapter, which uses the reconciliation data from the previous step.
- If the calculation is performed first by the adapter:
 - The adapter calculates the TQL query for CPU, and returns the connected nodes as the reconciliation data.
 - Then the calculated data is sent to the CMDB, where the TQL query for Node is calculated according to the reconciliation data from the previous step.

The option to set the adapter as the starting point of the TQL query calculation is specified in the Adapter Management module. For details, see ["Adapter Source Editor Window" on page 265](#).

Data Push

An integration of Data Push type copies data from the CMDB to an external data repository, so that the CMDB no longer retains control over this data.

You use data push integrations to feed important data from your CMDB into an external system to facilitate your necessary business processes. An example of this is pushing data discovered by DFM into Micro Focus Service Manager, where tickets may be opened that are connected to the actual CIs in your IT infrastructure.

If an authorized state has been defined, you can perform data push from the authorized or actual state.

Data push architecture enhancement

In version 10.30, data push architecture is enhanced to separate the internal resources used by different integrations, localizing at integration point level, resources otherwise shared between the integration points, which, when run in parallel with large amount of data may prove slow. By reducing such shared resources, big improvements can be observed in a concurrent running scenario. Now the engine parallelism can be better exploited through the number of threads allocated. A new JMX setting **com.hp.ucmdb.synchronizer.manager.SynchronizerManagerFactory** is introduced, which allows you to increase the number of threads for data push jobs from the out-of-the-box value **3** to any desired value. For more information, see ["How to Increase the Number of Threads for Data Push Jobs" on page 334](#).

In version 10.30, the number of CIs from a data push TQL query is increased from 5 million to 20 million on Oracle.

Note: Due to previous engine limitation, the number of CIs to push was limited at 5 million CIs to ensure a healthy delivery. With the new data push architecture, the fuse has been increased to 20 million CIs, so push integrations may handle larger number of CIs.

To achieve this, you need use the native Oracle drivers, instead of the Data Direct drivers, due to errors received when using Data Direct drivers.

How to switch between native Oracle drivers and data direct drivers

To do so,

1. Open the **C:\hp\UCMDB\UCMDBServer\bin\wrapper.conf** file using a text editor.
2. Locate the **-Doracle.native.driver** setting in following line, and change its value to meet your needs (default value **true**):

```
wrapper.java.additional.47=-Doracle.native.driver=true
```

3. Save the file.
4. Restart the UCMDB server.

The values of the following infrastructure settings were also increased on UCMDB server side to support 20 million CIs:

```
dal.object.condition.max.result.size=99999999
dal.link.condition.max.result.size=99999999
dal.use.memory.instead.temp.table.high.threshold.oracle=60000000
model.change.percent.statistics.threshold=30
replication.timeout=180000000
tql.dfs.max.temp.results=200000000
```

```
tql.max.objects.visit.model.calc.task=200000000
push.remote.action.timeout=12000000
```

To view these settings, you can invoke the **UCMDB:service=Settings Services > showSettingsByCategoryJMX** method.

For limitations on Data Push jobs, see "[Limitations – Integration Studio](#)" on page 362.

Integration in a Multi-Tenancy Environment

When executing integration queries or jobs in a multi-tenancy environment, all CIs and relationships that are federated or populated from the remote data source are assigned an owner tenant.

Note: When executing integration queries or jobs in a multi-tenancy aware environment, the tenants defined in this environment must be a subset of the tenants defined in the data source environment (not multi-tenancy aware environment).

If the data source environment is multi-tenancy aware, when you run a query or a job, only the CIs and relationships of those tenants that you have permissions to view are federated or populated. The owner tenant value is brought in with all of the other attributes.

If the data source environment is not multi-tenancy aware, when you run the query or a job, UCMDDB automatically assigns a specified owner tenant value to each of the federated/populated CIs and relationships. For details about selecting an owner tenant value to assign to federated/populated CIs and relationships, see "[New Integration Point/Edit Integration Point Dialog Box](#)" on page 353.

Tenant Assignment in a Multi-Tenant Scenario

Scenario	Tenant Assignment Behavior
Single Tenant → Multi Tenant UCMDDB	CIs are pushed to the tenant of the integration user (user default tenant) . The target UCMDDB tenant is assigned.
Multi Tenant → Single Tenant UCMDDB	<ol style="list-style-type: none"> 1. If tenant owner property is defined in integration TQL layout then the CI tenant will be pushed. In this case the source UCMDDB tenant is assigned. 2. If the tenant owner property is NOT defined in integration TQL layout and there is a Default Owner Name integration point property defined, then this tenant will be assigned in the target environment. In this case the source UCMDDB tenant is assigned. 3. No tenant property if cases 1 and 2 from above are not met.

Tenant Assignment in a Multi-Tenant Scenario, continued

Scenario	Tenant Assignment Behavior
	<p>Note: In a Single Tenant UCMDB the tenant properties can be made visible by setting Display Tenant Attributes in UI (<code>display.tenant.attributes</code>) to true from the Infrastructure Manager.</p>
Multi Tenant → Multi Tenant UCMDB	<ol style="list-style-type: none"> 1. If the tenant owner property is defined in the integration TQL then the CI tenant will be pushed. In this case the source UCMDB tenant is assigned. 2. If the tenant owner property is NOT defined in integration TQL layout and there is a Default Owner Name integration point property, then this tenant will be assigned in the target environment. In this case the source UCMDB tenant is assigned. 3. If both tenant owner property is NOT defined in the integration TQL layout and Default Owner Name integration point property is NOT defined then the tenant of the integration user(user default tenant) will be assigned to the pushed CIs. The target UCMDB tenant is assigned. <p>Note: If a CI's tenant is pushed to target UCMDB and the tenant does not exist, then the following error will be logged:</p> <pre> ErrorCode [63507] Reconciliation DataIn Multi Tenant : trying to use tenant that does not exist.{<tenant name>} </pre>
Single Tenant > Single Tenant UCMDB	Not a tenant push scenario

How to Work with Federated Data

This task explains how to set up and work with data that is federated from different CMDB sources.

This task includes the following steps:

- ["Set up the federation type integration " on the next page](#)
- ["Set a reconciliation priority" on the next page](#)
- ["View Instances in IT Universe Manager" on the next page](#)
- ["View Reports" on the next page](#)

1. Set up the federation type integration

Set up the integration that will federate the data, including the CITs that should be federated. For details, see ["How to Set Up an Integration Point" on page 324](#).

2. Set a reconciliation priority

In the Integration Point pane, right-click the integration, and select **Reconciliation Priority Manager** from the shortcut menu. For more details, see ["Reconciliation Priority Window" on page 764](#).

3. View Instances in IT Universe Manager

For details about viewing the federated CI instances, see "Working with Views in IT Universe Manager" in the *Universal CMDB Modeling Guide*.

4. View Reports

You can view reports about the integration in the Modeling Studio. For details see Reports in the *Universal CMDB Modeling Guide*.

How to Work with Population Jobs

This task explains how to schedule population jobs and select the queries that are used to populate the CMDB with data.

This task includes the following steps:

- ["Create an integration point" on the next page](#)
- ["Set Reconciliation priority" on the next page](#)
- ["Run the population job" on the next page](#)
- ["Build a view of the population results" on page 320](#)
- ["View instances in IT Universe Manager" on page 320](#)
- ["View reports" on page 320](#)

1. Create an integration point

Set up the integration to populate the data. For details, see ["How to Set Up an Integration Point" on page 324](#).



2. Set Reconciliation priority

In the Integration Point pane, right-click the integration, and select **Reconciliation Priority Manager** from the shortcut menu. For more details, see ["Reconciliation Priority Window" on page 764](#).



3. Run the population job

Population jobs are set to run according to a default schedule setting. However, you can manually run the integration at any time from the Integration Jobs pane. For user interface details, see ["Integration Jobs Pane" on page 339](#).

Select the job.

- To synchronize all data for the first time, click the **Full Synchronization**  button.
- To synchronize only the data changes since the job last ran, click the **Delta Synchronization**  button.

Note:

- If CIs in a population job fail, the query is displayed in the Query Status tab as **Completed** with a warning symbol . You can drill down to see the errors that occurred and the CIs affected. This error data is saved in the system. When the job runs again to synchronize changes, UCMDB remembers the failed CIs and repopulates these as well.
- If, since the last synchronization, you have changed a TQL query (other than changes to conditions on existing nodes), click the **Clear Probe Results Cache**  button to ensure that the next run of the job is a full synchronization.
- **High Availability environment:** If a population job is running, and the UCMDB Server responsible for write requests becomes unavailable or is changed, the job fails. You can wait for the next invocation of the job schedule, or alternatively rerun the population job manually.
- For ResultTreeNodes (RTNs) coming from external sources, their **isDeleted** attribute setting will not be overridden by the mapping process. For example, if one RTN, which has

isDeleted attribute set **true**, comes from SM, using a population job, it will be deleted even if the mapping processing changes **isDeleted** to **false**.

4. Build a view of the population results

For details about viewing the populated data, see "Working with Views in IT Universe Manager" in the *Universal CMDB Modeling Guide*.

5. View instances in IT Universe Manager

For details about viewing the CI instances, see "Working with Views in IT Universe Manager" in the *Universal CMDB Modeling Guide*.

6. View reports

You can view reports about the integration in the Modeling Studio. For details see Reports in the *Universal CMDB Modeling Guide*.

How to Work with Data Push Jobs

This task explains how to schedule data push jobs and select the queries that are used to send data from the CMDB to another data repository.

This task includes the following steps:

- ["Create an integration point" below](#)
- ["Set Reconciliation priority" on the next page](#)
- ["Run the Data Push job" on the next page](#)
- ["Build a view of Data Push results" on page 322](#)
- ["View instances in IT Universe Manager" on page 322](#)

1. Create an integration point

Set up the integration to push the data from UCMDB. For details, see ["How to Set Up an Integration Point" on page 324](#).



2. Set Reconciliation priority

In the Integration Point pane, right-click the integration, and select **Reconciliation Priority Manager** from the shortcut menu. For more details, see "[Reconciliation Priority Window](#)" on [page 764](#).

3. Run the Data Push job


A scheduled data push job runs according to the scheduler setting; a live data push job runs when its TQL query result changes. For more information about live data push jobs, see "[Live Data Push Jobs](#)" on [page 323](#).

You can also run the integration manually at any time from the **Integration Jobs** pane. To do this, select the job, and then click one of the following buttons:

- **Full Synchronization** : to synchronize all data for the first time.
- **Delta Synchronization** : to synchronize only the data changes since the job last ran.

For user interface details, see "[Integration Jobs Pane](#)" on [page 339](#).

Note:

- If CIs in a data push job fail, the query is displayed in the Query Status tab as **Completed** with a warning symbol . You can drill down to see the errors that occurred and the CIs affected. This error data is saved in the system. When the job runs again to synchronize changes, UCMDb remembers the failed CIs and repushes these as well.
- You can define a limit on the number sequential CI failures allowed during a running data push job. When this limit is reached, the job automatically stops running, enabling you to troubleshoot the reason for so many failures before waiting for the entire job to end.

In the Administration module's Infrastructure Setting Manager, select **Integration Settings** and set the value of **Maximum number of data push job failures allowed in a sequence**. The default value for this setting is **20,000**.

- If, since the last synchronization, you have changed a TQL query (other than changes to conditions on existing nodes), all data is synchronized and the following message is written to the log: **TQL was changed between syncs - performing Full sync!**
- **High Availability environment:** If a data push job is running, and the UCMDb Server responsible for write requests becomes unavailable or is changed, the data push job fails. You can wait for the next invocation of the job schedule, or alternatively rerun the data push job manually.

- You can control the way the job handles null value attributes in the Adapter Configuration tab. For details, see "[Adapter Configuration Tab](#)" on page 259.
- You can increase the number of threads for data push jobs. For details, see "[How to Increase the Number of Threads for Data Push Jobs](#)" on page 334.


4. Build a view of Data Push results

For details about viewing the data push results, see "Working with Views in IT Universe Manager" in the *Universal CMDB Modeling Guide*.

5. View instances in IT Universe Manager

For details about viewing the CI instances, see "Working with Views in IT Universe Manager" in the *Universal CMDB Modeling Guide*.

Note: In case of UCMDB being configured with Multi-Tenancy, this is the context in which the job is run and which may affect push job TQL result:

1. When a user creates a push job, from now on the user will be the owner of it (the old push jobs will have no user). You can check the user from the JMX console (go to **JMX console > UCMDB:service=URM Services**, invoke the **listResources** JMX method by entering customer ID and **Integration_PUSH_CONFIG** as the **resourceType** value. On the returned result page, click the integration push job created, and then check the **<created-by>** tag). This user tenant may be used.
2. When this push job is triggered via the **Full Synchronization**  button from the UCMDB UI, it will be executed in the context of the logged in user. This means that, only the resources assigned to tenants of the logged in user will be pushed. (Similar for a **Delta Synchronization**)
3. When a job is triggered via the scheduler, it will be executed only in the context of the sync job owner user, which created the sync job.
4. If a job owner does not exist in case of scheduling, it will be executed in the context of the **sysadmin** user. (For example, for the old push jobs that have no user.)
5. In case of scheduling, if the user that is the owner of a sync job does not exist, the push job will fail.

In the **ucmdb.synchronizer.log** file, the following error will be logged:

Caused by: java.lang.IllegalArgumentException: User with id {<userName>} does not exist

The solution is to re-create the sync job or update the `created_by` tag of the sync job with an user that exists in UCMDB.

Live Data Push Jobs

A live data push job no longer relies on the schedule setting. Instead, a live data push job runs in following manner:

- When the result of its active TQL queries changes, it automatically runs a delta synchronization and sends the change to the consumer (external system).
- A live data push job can contain multiple TQL queries, and the job runs a delta synchronization when any of its TQL query result changes.
- If a TQL query result changes during the running of the job, the latest changes wait until the job finishes, and then trigger another run of the job.
- When a live data push job and a scheduled data push job use the same TQL query, the two jobs cannot run concurrently. If a job already runs, the other waits until the running job finishes.
- If you manually stop a live data push job, then the changes occurred during the running of the job do not trigger another run of the job.

Note:

- It is recommended to use only one TQL query in a live data push job.
- Live data push jobs only perform delta synchronizations. In order to perform full synchronizations, you need a scheduled data push job that contains the same TQL query.
- If the priority level of a TQL query is **Not Active**, it automatically changes to **Low** when you add the TQL query to a live data push job.
- When you remove a live job or deactivate the **Enable live job** option of the job, if the contained TQL query is not part of any other live jobs, the priority level of the TQL query is then set to **Not Active**.
- After you create a TQL query and use it in a live data push job, do not modify the layout attributes of any link in the TQL query. Otherwise, the live data push job fails.

How to Set Up an Integration Point

This task describes how to create and configure an integration point for a particular integration with UCMDB.

Note: The integration adapters provided with the Discovery and Integrations Content Pack come predefined with the basic setup recommended to perform integration with UCMDB, including adapter properties, integration jobs and, where relevant, federation settings. You can use these settings or configure them to suit your needs.

This task includes the following steps:

- ["Prerequisites" below](#)
- ["Create an integration point" below](#)
- ["Add the integration jobs and schedule the jobs to run" on the next page](#)
- ["For a federation-type integration, define the data to be federated" on page 326](#)
- ["How to Set Up an Integration Point" above](#)

1. Prerequisites


The integration adapter must be correctly configured before setting up the integration.

- **Pre-configured Integration Adapters:** These are provided out-of-the-box with the product. It is recommended to use the adapters as they come, without any further configuration.

However, if you do need to modify the adapter configuration, you are encouraged to do this from the Adapter Management module rather than manually. For details about adapter configuration, see ["How to Configure Adapter Settings" on page 227](#).

- **New External Data Source Adapters:** To configure an adapter for a new external data source, see ["Add an Adapter for a New External Data Source" in the *Universal CMDB Developer Reference Guide*](#).

2. Create an integration point

If you are creating a new integration point, select **Data Flow Management > Integration Studio**, and click the **New Integration Point**  button. For user interface details, see ["New Integration Point/Edit Integration Point Dialog Box" on page 353](#).

- a. Enter a name and description for the integration point.
- b. Select the appropriate integration adapter. For details on existing adapters, see ["Select Adapter Dialog Box" on page 357](#).
- c. Select whether or not to activate the integration upon creation.
- d. Upon selecting the adapter, the Adapter Properties section is populated with the relevant adapter properties. Provide the relevant information. For details, see the relevant section in *Universal CMDB Discovery and Integrations Content Guide*.
- e. Configure the adapter's protocol credentials, where required. For a list of supported protocols, see the *Universal CMDB Discovery and Integrations Content Guide*.
- f. Select the Probes to use for the integration.

Note:


- If your remote managed data repositories are accessible from the UCMDB server machine, you can use the UCMDB Integration Service instead of a Data Flow Probe to run non-Jython-based integrations. (This is relevant in a standalone UCMDB environment only.)

In this case, in the **Data Flow Probe** box, select **UCMDB Integration Service**.

If **UCMDB Integration Service** does not appear in the **Data Flow Probe** list, ensure that the UCMDB Integration Service is running on the UCMDB Server machine. For details, see ["How to Check the UCMDB Integration Service Status" on page 62](#).

- If your Probe is an integration probe, and it does not appear in this list, ensure that it is connected.

- g. **For Jython-based integration adapters only:** Create or select a trigger CI instance for the integration.
 - h. When you are finished, click **OK**. The integration point is automatically saved.
3. Add the integration jobs and schedule the jobs to run

Select the required integration point in the Integration Point pane. In the Integration Jobs pane, click the **New Integration Job**  button.

- Where relevant, define the job queries.
- Population and Data Push integration jobs are set to run according to a default schedule setting. You can change the schedule in the Schedule Definition pane.

For user interface details, see ["New Integration Job/Edit Integration Job Dialog Box" on page 349](#).

4. For a federation-type integration, define the data to be federated

In the Federation tab, select the CITs to be federated.

For user interface details, see ["Federation Tab" on page 337](#).

How to Save an Integration Point Configuration as an Adapter Default

You can save an integration point configuration as an adapter default. This is useful if you want to use an integration point's configuration to create other integration points with a similar configuration.

This task describes how to save an integration point configuration as an adapter default.

1. Prerequisites
 - a. Define an integration point based on a particular adapter. For example, MSSMS, based on the Microsoft SMS adapter.
 - b. Define population or push jobs and federation details.
 - c. Save the integration point.
2. Save the integration point configuration as an adapter default
 - a. In the Integration Point pane, right-click the integration point that you created, and select **Save as Adapter Default**.
 - b. In the Save as Adapter Default dialog box, enter details for the adapter default as follows:
 - **Name and Description.** A name for the adapter default and a description.

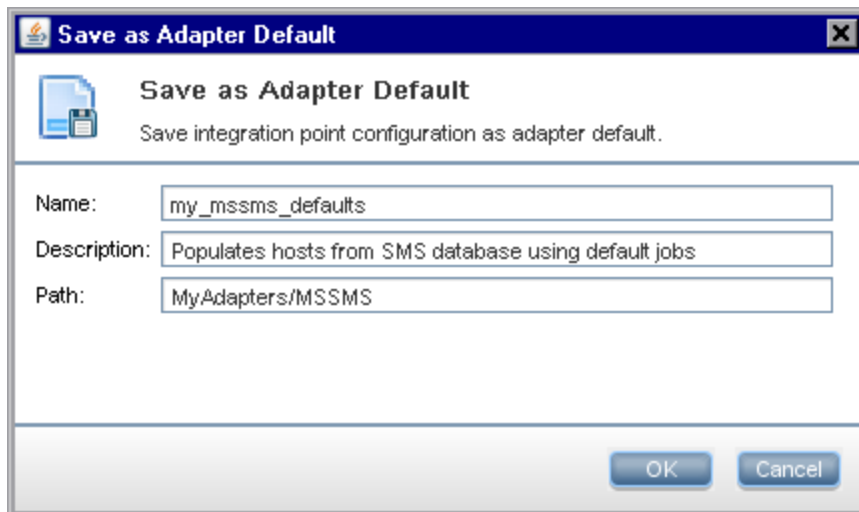
Caution: If you give the adapter default the same name as an existing adapter default, UCMDB treats this as though you are redefining the existing adapter default, and the new definition overwrites the existing definition. If you do not want to overwrite an existing adapter default, give the new adapter default a different name.
 - **Path.** (Optional) The path to the folder under which your adapter should be displayed in the

Select Adapter dialog box (when creating a new integration point). The adapter default is displayed under the same category as the adapter that was originally used to create the integration point, in the path that you define here.

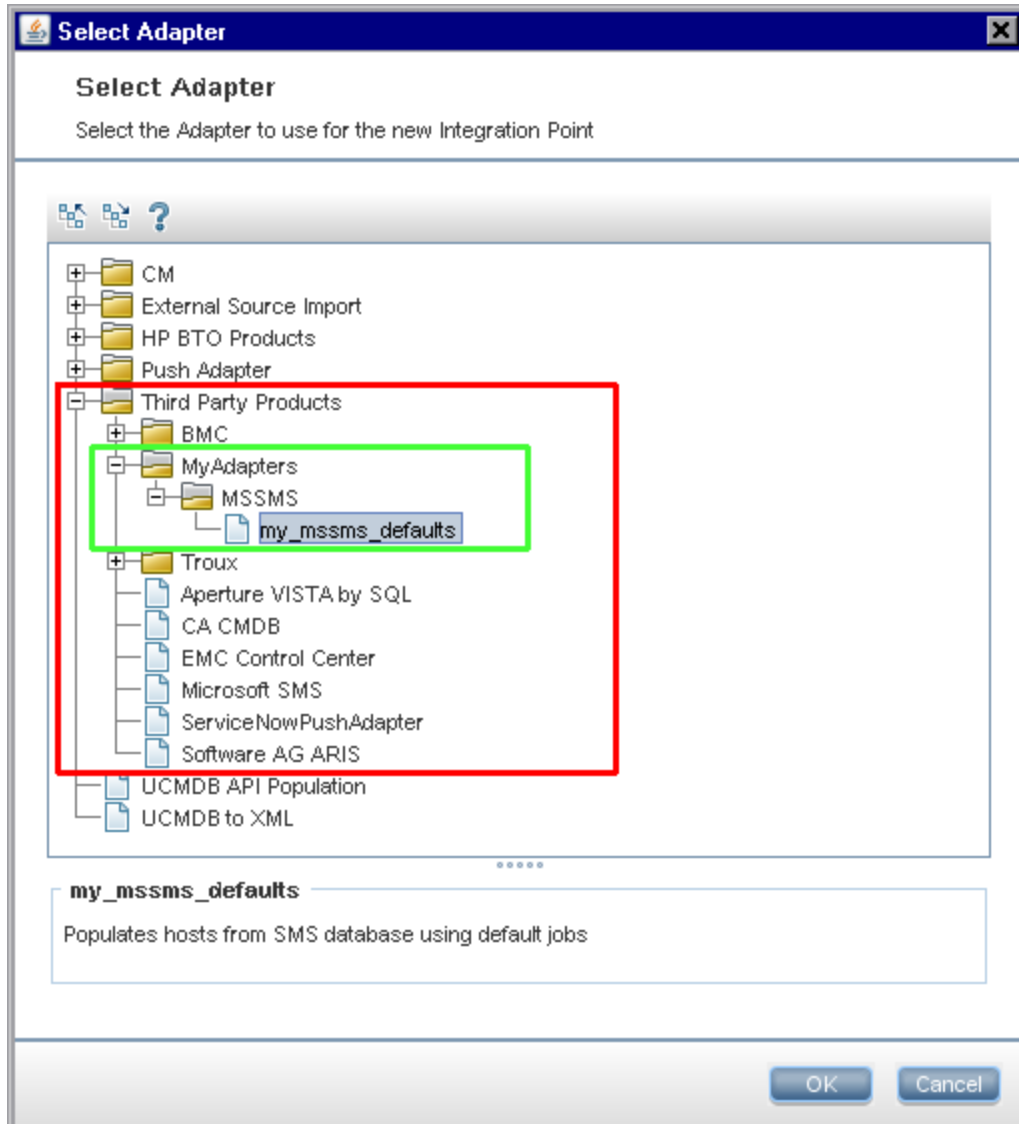
Note:

- Use only forward slashes (/) in the path.
- If you define a new folder in the path, the adapter default is displayed in that folder, under the same category as the original adapter.
- If you leave the path empty, the adapter default is displayed directly under the same category as the original adapter.

Using the MSSMS integration point example introduced in the Prerequisites section above, you could save this integration point as an adapter default, calling it **my_mssms_defaults** and defining the path as **MyAdapters/MSSMS**.



The next time you create a new integration point, the **my_mssms_defaults** adapter default is displayed under the **Third Party Products** category (because the out-of-the-box Microsoft SMS adapter appears under this category), in the **MyAdapters>MSSMS** folder, as you specified in the path:



3. Results

- When you save the adapter default, integration point parameters that are not related to the connection itself are saved in the adapter default definition.
- The code for the adapter default is added to the adapter's xml file. To delete the adapter default, see ["How to Remove Adapter Defaults" on the next page.](#)

How to Remove Adapter Defaults

To remove an adapter default, you must delete the code that defines it from its base adapter's .xml file.

To remove an adapter default:

1. Locate the adapter on which the adapter default was based. (**Adapter Management > Resources** pane).

Tip: Alternatively, you can access the adapter from the Integration Point pane by right-clicking the relevant integration point and selecting **Go To Adapter**.

2. Right-click the adapter and click **Edit Adapter Source**.
3. In the adapter's .xml file, locate the following line:

- o **Non-Jython adapters:**

```
<adapterTemplate name="<adapter_default>" description="">
```

- o **Jython adapters:**

```
<adapterJythonTemplate name="<adapter_default>" description="">
```

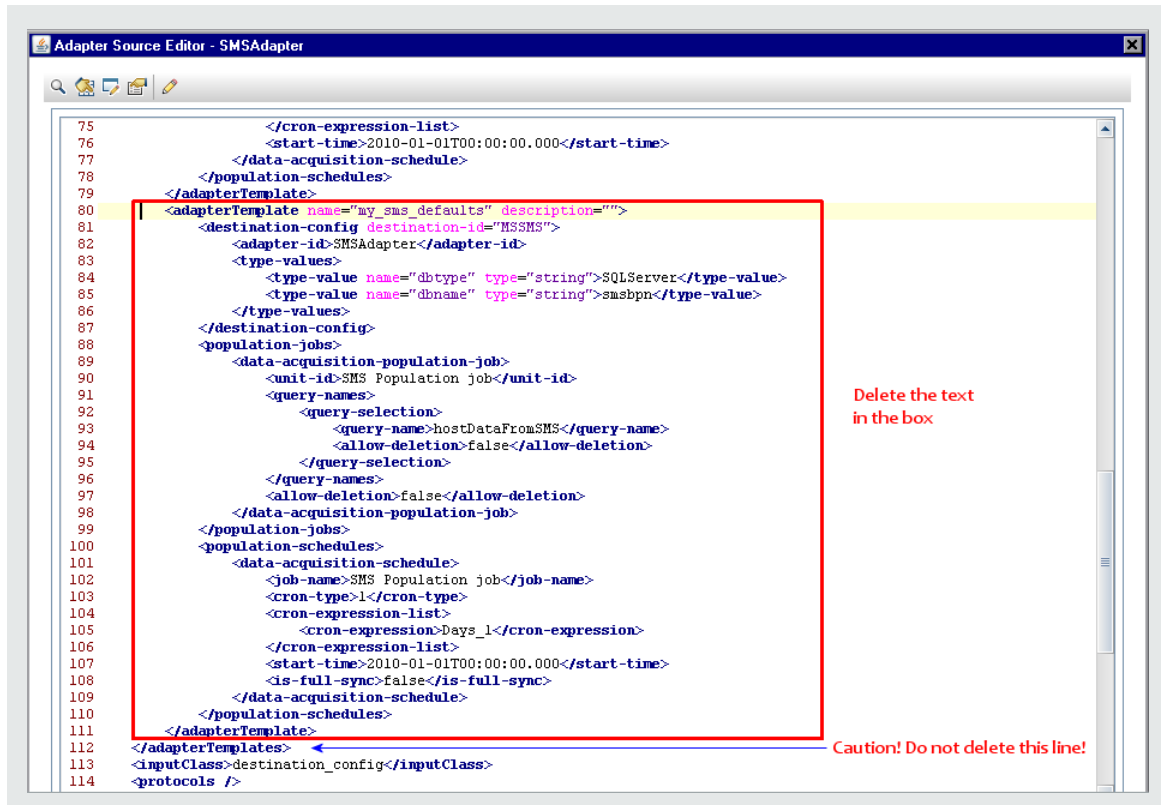
where **adapter_default** is the name of the adapter default.

4. Delete the all the code from this opening tag to the closing `</adapterTemplate>` (or `</adapterJythonTemplate>`) tag.

Caution: Do not delete the following line: `</adapterTemplates>`

5. Save your changes.

Example



How to Deploy a Package to a Remote Data Repository

You can deploy a package to a data repository located on a remote machine without logging in to the remote machine. This feature is useful if you need to deploy queries, views, or other UCMDB resources created on one machine to other machines running UCMDB.

Note: Perform the following procedure for each data repository to which the package is to be deployed.

This task includes the following steps:

- ["Prerequisites" on the next page](#)
- ["Change timeout - optional" on the next page](#)
- ["Select the integration point" on the next page](#)

- ["Select the package" below](#)
- ["View deployment results" on the next page](#)
- ["View Log files" on the next page](#)

1. Prerequisites

- Verify that the Data Flow Probe is configured correctly and is connected to UCMDDB.
- Verify that the version of UCMDDB running on the remote machine is version 9.02 or later.
- Verify that the UCMDDB Server on the remote machine is up and running.
- Create the package that must be deployed to the remote machine, and deploy this package to the local UCMDDB Server.

Note: By default, you cannot deploy a package that is larger than 10 MB.

- Create an integration point on the local UCMDDB Server, that uses the **UCMDDB 9.x/10.x** adapter.

2. Change timeout - optional

You can change the time after which UCMDDB times out package deployment. If UCMDDB cannot connect to the remote machine in 5 minutes, by default, the deployment is timed out.

To change the default: Select **Administration > Infrastructure Settings Manager > Integration Settings > Remote package deploy Timeout**. (The refresh rate indicates when the change takes effect in UCMDDB after the value is modified.)

3. Select the integration point

In the Integration Point pane, right-click the integration point that you created in ["Prerequisites" above](#). For details, see ["Integration Point Pane" on page 346](#), and select **Deploy Remote Package**.

4. Select the package

- a. In the Deploy Remote Package dialog box, select a package from the list of packages existing on the local UCMDDB Server. This is the package that you created in ["Prerequisites" above](#). For details, see ["Deploy Package to Remote Data Repository using <Integration Point>" on page 337](#).

- b. Click **OK** to deploy the package.

5. View deployment results

Answer the message that is displayed: click **OK** to begin deploying the package.

The status of the deployed package is displayed together with the status of each individual resource in the package.

- o **Successful deployment:** A package is successfully deployed if all its resources are successfully deployed.
- o **Failed deployment:** If even one resource fails, the package deployment is considered to have failed. Even if package deployment fails, all the successful resources are deployed on the remote machine.

The reason for the failure, for example, a missing CIT, is displayed in the **Deployed resources** section:

Deployed resources

Resource	Status
tql/View/testing.xml	✘ Class not in class model

6. View Log files

The following table shows the locations of the log files that record any issues that might arise during deployment:

Location	Log File Name
Remote UCMDB machine, version 9.02 or later	ucmdb-api.log mam.packaging.log
Data Flow Probe	probeTasks.log probe-infra.log adapters.log
Local UCMDB machine	ucmdb-api.log

If a resource fails to deploy, an error is displayed in the **Status** column as well as in the log file on the remote machine.

How to Configure Probe IP Ranges with Active Directory



This integration retrieves the latest site information (including IP subnets) from Active Directory. This lets you configure the IP ranges contained in the Data Flow Probe according to the contents of the Active Directory.

1. Run jobs

Run the following jobs:

- a. Range IPs by ICMP or Range IPs by NMAP
- b. TCP Ports
- c. Active Directory Connection by LDAP
- d. Active Directory Topology by LDAP

2. Add Active Directory Topology by LDAP to Integration

- a. Go to **Adapter Management > Resources** pane > expand **Packages**, expand **Active Directory**, click **LDAP Active Directory Connection**.
- b. In the Details pane, click **Used as an Integration Adapter**. In the **Adapter Category** field, type "Active Directory".
- c. Go to **Integration Studio > Integration Point** pane, click **Active Directory Topology**. In the **Integration Jobs** pane, click . The **Configure Probe Range by Active Directory** dialog box opens.
- d. In the list of Data Flow Probes, select the server that you want to configure. In the list of Active Directory servers, click the server that contains the site information you want to use to configure the Data Flow Probe. Click . A new dialog box opens.
- e. Accept the default IP range and save your changes.

How to Increase the Number of Threads for Data Push Jobs

Version 10.33 introduced a new JMX setting

com.hp.ucmdb.synchronizer.manager.SynchronizerManagerFactory, allowing you to increase the number of threads for data push jobs from the out-of-the-box value **3** to any desired value.

How to increase the number of threads for data push jobs

Note: Apply this change for large UCMDB deployments where the hardware resources for UCMDB server and data flow probe are assigned as documented in the *Universal CMDB Sizing Guide*.

To do so,

1. Log in to the UCMDB JMX console. (Launch the Web browser and enter the following address: **https://<server_name>:8443/jmx-console**. You may have to log in with a user name and password.)
2. Enter **setInternalSetting** in the Quick Search field and click the link that appears with the **UCMDB:service=Settings Services** category.
3. Invoke the **setInternalSetting** JMX method with the following parameters:
 - **customerID:** Enter your Customer ID. (**Default: 1**)
 - **key:** Enter **com.hp.ucmdb.synchronizer.manager.SynchronizerManagerFactory**.
 - **value:** Enter a desired value as the number of threads for push jobs. (**Default: 3**).
4. Double check the value set by invoking the **getInternalSettings** JMX method.
The returned result contains the **com.hp.ucmdb.synchronizer.manager.SynchronizerManagerFactory** setting and its value.
5. Restart the UCMDB Server.
6. The new value is loaded successfully if you see the following message logged in the **startup.log** file:

```
The number of threads for manager
```

```
com.hp.ucmdb.synchronizer.manager.SynchronizerManagerFactory was overridden  
to ...
```

Note: The **startup.log** file is located in the **<UCMDB_Install_dir>\runtime\logs** directory.

Revert the change

To revert the change and use the default value,

1. Perform either of the following from the UCMDB JMX console:
 - o Invoke the **setInternalSetting** JMX method with the following parameters:
 - **customerID:** Enter your Customer ID. (**Default: 1**)
 - **key:** Enter **com.hp.ucmdb.synchronizer.manager.SynchronizerManagerFactory**.
 - **value:** Enter the default value **3**.
 - o Delete the new setting by invoking the **listResources** method from the **UCMDB:service=URM Services** category.

If you delete the new setting, UCMDB will use the hard-coded default value.

To do so,

- i. Enter **listResources** in the Quick Search field and click the link that appears with the **UCMDB:service=URM Services** category.
 - ii. Invoke the **listResources** method with the following parameters:
 - **customerID:** Enter your Customer ID. (**Default: 1**)
 - **resourceType:** Enter **Settings_STATE_CUSTOMER_SETTING**.
 - iii. On the returned result page, click **delete** for the **com.hp.ucmdb.synchronizer.manager.SynchronizerManagerFactory** setting.
2. Restart the UCMDB Server for the change to take effective.

Integration Studio User Interface

This section includes (in alphabetical order):

Data Push Tab	336
Deploy Package to Remote Data Repository using <Integration Point>	337

Federation Tab	337
Integration Jobs Pane	339
Integration Point Pane	346
Integration Studio Page	348
New Integration Job/Edit Integration Job Dialog Box	349
New Integration Point/Edit Integration Point Dialog Box	353
Population Tab	356
Select Adapter Dialog Box	357
Topology CI Creation Wizard	358

Data Push Tab

This tab enables you to set up an integration point for pushing data to an external data repository.

To access	Select the Data Push tab on the Integration Studio page.
Important information	This tab is enabled only when data push is supported by the adapter on which you are basing your integration point.
Relevant tasks	"How to Work with Data Push Jobs" on page 320
See also	<ul style="list-style-type: none"> o "Integration Studio Overview" on page 310 o "UCMDB Integration Service" on page 30 o "New Integration Job/Edit Integration Job Dialog Box" on page 349

User interface elements are described below:

UI Element	Description
Integration Jobs pane	Enables you to specify the queries that are used to push data to external data repositories, and to schedule jobs that contain those queries. For details, see "Integration Jobs Pane" on page 339 .
Statistics tab	Displays results for integration jobs that have run. For details, see "Statistics Tab" on page 342 .
Query Status tab	Displays information about the queries defined for the integration job. For details, see "Query Status Tab" on page 343 .

Deploy Package to Remote Data Repository using <Integration Point>

Enables you to deploy a package to a remote data repository using an integration point, and to view the results of the deployment.

To access	Click the Deploy a Remote Package button in the Integration Point pane. For details, see " Integration Point Pane " on page 346.
Relevant tasks	"How to Deploy a Package to a Remote Data Repository" on page 330

User interface elements are described below:

UI Element (A-Z)	Description
Deployed resources	The status (success or failure) of each deployed resource in the package named under Deployment status .
Deployment status	The name and status (success or failure) of the complete package.
Package Name	A list of all available packages.





Federation Tab

This tab enables you to select which CITs or attributes are to be supported by the integration point. For example, if a TQL query includes a node that represents a specific CIT, the instances of this CIT are accepted from this external data repository.

For details about selecting CIs, see "CI Selector Overview" in the *Universal CMDB Modeling Guide*.

To access	Select the Federation tab on the Integration Studio page.
Important information	This tab is enabled only when data federation is supported by the adapter on which you are basing your integration point.
Relevant tasks	"How to Work with Federated Data" on page 317
See also	<ul style="list-style-type: none"> • "Integration Studio Overview" on page 310 • "New Integration Job/Edit Integration Job Dialog Box" on page 349

User interface elements are described below:






UI Element (A-Z)	Description
	Click to clear all selected items.
	Click to invert the selections.
	Click to expand the entire hierarchical tree structure.
	Click to collapse the hierarchical tree structure.
CI Type Retrieval Mode	<ul style="list-style-type: none"> • Retrieve CIs of selected CI Type. All a CI's data, including all its attributes, are retrieved from the data repository. • Retrieve selected attributes. The selected attributes are retrieved from the data repository. The CIs must already exist in the CMDB. <p>Note:</p> <ul style="list-style-type: none"> • A parent CIT and all its child CITs included in an integration point definition must use the same retrieval mode. • You cannot select both CITs and attributes for the same integration point.
Select Attributes	<p>You can define which attributes of an external CIT are to be included in the federation:</p> <ul style="list-style-type: none"> • In the CI Type Retrieval Mode pane, select Retrieve selected attributes. • In the Select Attributes list, select the attributes that are to be included in the federation. • Save the changes. <p>Note: Attributes are defined in the CIT Manager. For details, see "Add/Edit Attribute Dialog Box" in the <i>Universal CMDB Modeling Guide</i>.</p>
Supported and Selected CI Types	<p>Displays a hierarchical tree containing the supported and selected CI Types and attributes.</p> <p>When queried by an TQL query, the CITs you select here are configured to retrieve the data from this external data repository.</p> <p>Select the CITs to be supported by this integration point.</p>





Integration Jobs Pane

This pane enables you to schedule integration jobs to run with external data repositories. The Statistics, Query Status, and Job Errors tabs display runtime details about the selected jobs.

To access	<ul style="list-style-type: none"> • Select the Population or Data Push tab on the Integration Studio page. • To access the Statistics, Query Status, or Job Error tabs, select an integration point, select the Population or Data Push tab on the Integration Studio page, and then select a job.
Important information	This pane is displayed only when population or data push is supported by the adapter on which you are basing your integration point.
Relevant tasks	<ul style="list-style-type: none"> • "How to Work with Population Jobs" on page 318 • "How to Work with Data Push Jobs" on page 320
See also	<ul style="list-style-type: none"> • "Integration Studio Overview" on page 310 • "Discovery Scheduler Dialog Box" on page 496

User interface elements are described below:

UI Element (A-Z)	Description
	New Integration Job. Enables you to create an integration job. For details, see "New Integration Job/Edit Integration Job Dialog Box" on page 349 .
	Edit Integration Job. Enables you to edit an existing integration job.
	Delete Integration Job. Deletes the selected integration job from the list.
	<p>Refresh. Refreshes the list of integration jobs.</p> <p>Note: If you refresh the list of jobs before you save a new job, you are given a choice:</p> <ul style="list-style-type: none"> • Yes. The job is saved and the integration is refreshed. • No. The job is not saved and the integration is refreshed. • Cancel. The job is not saved and the integration is not refreshed.
	Run Job - Synchronize Changes. Runs the selected population or data push job and synchronizes only the changes in the data since the last time the job was run.

UI Element (A-Z)	Description
	<p>By default, scheduled jobs synchronize only changes except for the first time a job runs. In that case, a full population or data push job runs, in which all relevant data for the job is synchronized.</p> <p>Note:</p> <ul style="list-style-type: none"> • If the job is scheduled to run an all-data synchronization while you are running a changes synchronization, the scheduled all-data synchronization will run when the job has finished synchronizing the changes. • If CIs in a data push job fail, the query is displayed in the Query Status tab with the status: Passed with failures. You can drill down to see the errors that occurred and the CIs affected. This error data is saved in the system. When the job runs again to synchronize changes, UCMDDB remembers the failed CIs and repushes these as well. For details, see "Query Status Tab" on page 343.
	<p>Run Job - Synchronize All Data. Runs a full population or data push job. This job copies or pushes all the relevant data for the job.</p> <p>Note: If the job is scheduled to run a changes synchronization while you are running an all-data synchronization, the scheduled changes synchronization will run when the job has finished synchronizing all of the data.</p>
	<p>Stop Running Job. Stops running the selected job.</p> <p>Available for: Data Push jobs only</p>
	<p>Clear Probe Results Cache. Clears the cache of all job results for this integration from the Data Flow probe as well as the last time the data was synchronized. The next time you run a synchronization, all the data is synchronized again.</p> <p>Available for: Population jobs only</p>
	<p>View Integration Point Log. Displays the log of the integration point.</p>
<p><right-click integration job menu></p>	<p>In addition to the options described above, the right-click menu provides the following functionality:</p> <ul style="list-style-type: none"> • Show Results For Job. DFM sends an ad hoc request to the Probe and retrieves the latest results of the job. <p>This ad hoc request does not run the job, but brings the results of the previous job run that are stored in the Probe's database. If the job has not yet run, a message is displayed.</p> <p>Available for: Population jobs only.</p>

UI Element (A-Z)	Description
	<p>Note: Results are not displayed if the total number of results exceeds 10,000.</p> <ul style="list-style-type: none"> • View Communication log. Opens the log that includes information about the connection between the Probe and the remote machine. This is on condition that you have set the Create communication log to Always or On failure. For details, see "Execution Options Pane" on page 260. <p>Available for: Population jobs based on Jython adapters only.</p>
Job Name	Name given to the population or data push job.
Last Synchronization Type	<p>The type of the last run:</p> <ul style="list-style-type: none"> • None. The job has not yet run. • Changes. The job synchronized only the changes in the data since the last time it ran. • Full. The job synchronized all the relevant data for the job. <p>Available for: Data push jobs only</p>
Status	<p>Population jobs:</p> <ul style="list-style-type: none"> • Waiting for Probe. The job is waiting to be received by the Probe. • Did not run. The job has been received by the Probe but the Probe is not yet ready to run the job. • Preparing to run. The Probe is preparing to run the job. <p>Note: The status is preceded by another instance of the Waiting for Probe status, but this time Waiting for Probe indicates that the Probe is now ready to prepare the job for the run.</p> <ul style="list-style-type: none"> • Running. The job is running. • Completed Successfully. The job ran successfully. • Completed. The job ran successfully but errors or warnings were reported. See details on the errors or warnings in the "Query Status Tab" on page 343. • Failed. The job did not run successfully. • Disabled. The integration point is deactivated or the trigger CI is missing. <p>Data push jobs:</p> <ul style="list-style-type: none"> • Did not run. The job has not yet run. • Running. The job is currently running.




UI Element (A-Z)	Description
	<ul style="list-style-type: none"> • Ended. The period between Running and Succeeded or Failed. • Completed. The job ran successfully but errors or warnings were reported. See details on the errors or warnings in the "Query Status Tab" on the next page. • Completed Successfully. The last run was successful. • Failed. The last run was not successful.
Start time / Finish time	<p>The time that the integration job actually started running, and when it finished running. These columns are refreshed every time the job goes into the Running state.</p> <p>Available for: Population jobs only</p>

Statistics Tab

This tab displays information about the CIs synchronized by the job.

Note: Statistics for population jobs are accumulative and therefore can be filtered, whereas the data push statistics are always relevant for the last job run only.

User interface elements are described below (unlabeled elements are shown in angle brackets>):

UI Element (A-Z)	Description
	Refresh. Refreshes the details statistics displayed.
	<p>View Instances. Displays all new and updated CIs. Select a CIT and click:</p> <ul style="list-style-type: none"> • View Created Instances to display created CIs of the selected type • View Updated Instances to display updated CIs of the select type <p>Available for: Population jobs only</p>
	<p>Select the time range or Probe for which to display statistics about the selected job.</p> <ul style="list-style-type: none"> • By Time Range. <ul style="list-style-type: none"> ◦ All. Displays statistics for all job runs. ◦ From Now/Last Minute/Last Hour/Last Day/Last Week. Choose a period of time for which to display statistics about the CITs.







UI Element (A–Z)	Description
	<ul style="list-style-type: none"> ◦ Custom Range. Click to open the Change Timeframe dialog box: Enter the date or click the arrow to choose a date and time from the calendar, for the From and To dates (or click Now to enter the current date and time). Click Last Day to enter the current date and time in the To box and yesterday's date and time in the From box. Click OK to save the changes. • By Probe. To view statistics for a specific Probe, select to open the Choose Probe dialog box. <p>Available for: Population jobs only</p>
<Statistics table>	<ul style="list-style-type: none"> • CIT. (Population jobs only) The name of the discovered CIT. • Query Name. (Data push jobs only) The name of the query whose data is being pushed. • Created. The number of CIs created in the period selected or for the selected Probe. • Updated. The number of CIs that were updated in the period selected. • Deleted. The number of CIs deleted in the period selected or for the selected Probe. • Failed. The number of CIs that were not pushed. <p>Available for: Service Manager 9.3 adapter only</p> <ul style="list-style-type: none"> • Ignored. The number of CIs that were ignored because of the reconciliation rule in the external system. <p>Available for: Asset Manager Generic adapter 1.01 (or later) only.</p> <p>Note: For most adapters, when you repush the same CIs to a remote machine, the CIs are reported as Created in the Statistics table. For the Cmdb10xAdapter, AMPushAdapter and genericPushAdapter, the CIs are reported as Updated (actual status).</p>
Last updated	The date and time that the results for the selected job were last updated.
Valid to	The date when the data was last synchronized.





Query Status Tab

This tab displays information about the queries defined for the job.

Note: This tab is displayed for non-Jython data push and population integration adapters only.

User interface elements are described below:

UI Element (A–Z)	Description
	Refresh. Refreshes the list of queries.
	Push selected failed data. Enables you to repush the selected query/CI manually. Available: When a failed query or CI is selected
	Suppress selected failures/warnings. Enables you to suppress errors for a selected query/CI. Available: When a failed query or CI is selected Note: The Suppress feature removes the failed CI from the list of errors. The error is displayed again if the CI fails at the next synchronization attempt.
	Open the Query Editor. Enables you to view and edit the selected TQL query in the Integration Query Editor. Available: For Push jobs only.
<Query details>	Displays the details of the selected job's queries: <ul style="list-style-type: none"> • Query Name. The name of the query. • Status. <ul style="list-style-type: none"> ◦ Population jobs. The latest status of the query after the job finishes running. ◦ Data push jobs. The current status or the last known status of the query. If a query passed with failures, you can double-click the query to view the errors that occurred and on which CIs they occurred. To repush the query, click the Push selected failed data  button. To suppress all the errors for the query, click the Suppress selected failures/warnings  button. • Start Time/Finish Time. The time at which data push for this query started and finished. Available for: Data push jobs only
<Errors and warnings>	When you double-click a job that did not complete successfully, the table displays errors and warnings that occurred, the CI type affected, and the number of CIs that failed. Double-click a row to see the CIs that failed due to a particular error.



UI Element (A–Z)	Description
	<p>To repush the CIs, click the Push selected failed data  button. To suppress all the errors for the selected CI type, click the Suppress selected failures/warnings  button.</p> <p>Available for: Data push jobs only</p>
<Failed CIs>	<p>When you double-click an error or warning, the table displays the exact errors that occurred, the CIs on which they occurred, and when they occurred. The CIs are distinguished by their display label and external ID.</p> <p>To repush the CI, click the Push selected failed data  button. To suppress all the errors for the selected CI, click the Suppress selected failures/warnings  button.</p> <p>Available for: Data push jobs only</p>

Job Errors Tab

This tab displays the errors or warnings reported during the job run.

Note: This tab is displayed for Jython integration adapters only.

User interface elements are described below (unlabeled elements are shown in angle brackets):

UI Element (A–Z)	Description
	Refresh. Refreshes the list of errors.
	View Details. Displays details about the selected error.
<List of error messages>	<ul style="list-style-type: none"> • Message. A message describing warnings (if the job succeeded with warnings) or the cause for failure if the job failed. • Severity. For details, see Error Severity Levels in the <i>Universal CMDB Developer Reference Guide</i>. • Reported. The time at which the error is being reported by the job. • Query. Displayed for data push jobs only. The name of the query for which the error is being reported.

Integration Point Pane







This pane enables you to define integration points, and schedule population and data push jobs.














Integration points are based on adapters, each of which is predefined to transmit information in specific ways. For example, **CMDBAdapter** populates CIs and links from a remote CMDB, in which case the CMDB then has a local copy of these CIs, while the **ServiceManagerAdapter** adapter retrieves data from ServiceCenter and Service Manager, but ServiceCenter or Service Manager still retains control.


For details about defining a discovery adapter as an integration adapter, see the "[Used as Integration Adapter](#)" field in "[Adapter Definition Tab](#)" on page 253.

To access	Located in the left pane of the Integration Studio.
Relevant tasks	<ul style="list-style-type: none"> • "How to Set Up an Integration Point" on page 324 • "How to Save an Integration Point Configuration as an Adapter Default" on page 326 • "How to Deploy a Package to a Remote Data Repository" on page 330
See also	<ul style="list-style-type: none"> • "Data Push Tab" on page 336 • "Federation Tab" on page 337 • "Population Tab" on page 356

User interface elements are described below (unlabeled elements are shown in angle brackets>):

UI Element (A-Z)	Description
	New Integration point. Enable you to create an integration point. For details, see "New Integration Point/Edit Integration Point Dialog Box" on page 353 .
	Edit Integration Point. Enables you to edit an integration point's properties.
	Delete Integration Point. Deletes the selected integration point.
	Save Integration Point. Saves the changes you made to the definition of an integration point.
	Refresh All Integrations. Refreshes the list of integration points and fully refreshes the selected integration point.
	Reload supported configuration for adapter. Refreshes the supported classes and queries of the adapter for the selected integration point.

UI Element (A-Z)	Description
	Activate Integration Point. Activates the selected integration point.
	Deactivate Integration Point. Deactivates the selected integration point.
	Import From XML. Enables you to import the integration point's configuration in XML format.
	<p>Export To XML. Enables you to export the integration point's configuration in XML format.</p> <p>Note: You must save a new integration point before you can export its configuration.</p>
<List of integration points>	<p>Displays the list of previously-defined integration points.</p> <p>An icon appears next to each integration point indicating its status:</p> <ul style="list-style-type: none"> •  . Indicates that the integration is deactivated. •  . Indicates that there is an error for one or more of the jobs associated with the integration point. •  . Indicates that there were failures and/or warnings for one or more of the jobs associated with the integration point. •  . Indicates that there were no errors, failures, or warnings for the jobs associated with the integration point or that no job was executed for the integration. <p>Additionally, icons appears next to each third party integration point indicating its status.</p> <ul style="list-style-type: none"> •  . Indicates that there were no errors, failures, or warnings for the jobs associated with the integration point. •  . Indicates that there is an error for one or more of the jobs associated with the integration point. •  . Indicates that the adapters that are associated with the integration point were removed. •  . Indicates that the integration is deactivated.
<right-click integration point menu>	<p>In addition to some of the options described above, the right-click menu provides the following functionality:</p> <ul style="list-style-type: none"> •  Go to Adapter. Opens the adapter used by the integration job in the Adapter Management module.

UI Element (A-Z)	Description
	<ul style="list-style-type: none"> •  Reconciliation Priority Manager. Opens the Reconciliation Priority Manager, a centralized location for viewing and changing the reconciliation priority for all integration points. For details, see "Reconciliation Priority Window" on page 764. • Deploy Remote Package. Opens the Deploy Remote Package dialog box, enabling you to deploy a package to a data repository located on a remote machine without logging in to the remote machine. For details, see "How to Deploy a Package to a Remote Data Repository" on page 330. <p>Note: This button is enabled for integration points based on the UCMDB 9.x adapter (which supports package deployment capabilities).</p> <ul style="list-style-type: none"> • Save as Adapter Default. Opens the Save as Adapter Default dialog box, enabling you to save the configuration of the selected integration point as an adapter default that can be used as a basis for other integration points. <p>Enter a name and description for the adapter default, and specify the path where the default adapter should be saved.</p> <p>For example, to save an adapter default in a user-defined folder, in the Path box, enter:</p> <p>MyAdapters/Default</p> <p>Note:</p> <ul style="list-style-type: none"> ○ Use forward slashes (/) to separate folders in the path ○ If a path is not defined, the default adapter template is saved, by default, under the same category as the adapter that it was based on. <ul style="list-style-type: none"> • Edit Integration Resources. Opens the Adapter Management page where you can edit the adapter resources. Only the resources defined by the adapter as related to integrations are displayed in the Resources pane.

Integration Studio Page

This page enables you to create and manage integration points.

To access	Select Data Flow Management > Integration Studio .
Relevant tasks	<ul style="list-style-type: none"> • "How to Set Up an Integration Point" on page 324 • "How to Save an Integration Point Configuration as an Adapter Default" on page 326 • "How to Deploy a Package to a Remote Data Repository" on page 330


See also	"Integration Studio Overview" on page 310
-----------------	---

User interface elements are described below:

UI Element (A-Z)	Description
Integration Point pane	Enables you to manage integration points. For details, see "Integration Point Pane" on page 346 .
Right pane	Displays data transfer configuration options for an integration point. Depending on the adapter on which you base your integration point, one or more of the following tabs is enabled: <ul style="list-style-type: none"> • "Data Push Tab" on page 336 • "Federation Tab" on page 337 • "Population Tab" on page 356

New Integration Job/Edit Integration Job Dialog Box

This dialog box enables you to create or edit population and data push jobs and to schedule them to be run at specific times.





To access	Click  on the Population or Data Push tabs.
Relevant tasks	<ul style="list-style-type: none"> • "How to Work with Federated Data" on page 317 • "How to Work with Population Jobs" on page 318 • "How to Work with Data Push Jobs" on page 320
See also	<ul style="list-style-type: none"> • "Integration Studio Overview" on page 310 • "Integration Studio Page" on the previous page • "Integration Jobs Pane" on page 339

User interface elements are described below:

UI Element (A-Z)	Description
Name	Enter a name for the job. <p>Note: Naming conventions for jobs:</p> <ul style="list-style-type: none"> • Job names can contain the following characters: a-z, A-Z, 0-9, hyphen (-), underscore (_), space ()

UI Element (A-Z)	Description
	<ul style="list-style-type: none"> Job names must not start with a digit or an underscore (_)
Job Definition area	<p>Enables you select integration queries for the job definition. For details, see "New Integration Job/Edit Integration Job Dialog Box" on the previous page.</p> <p>Available for: Non-Jython adapters only.</p>
Scheduler Definition area	<p>Enables you to schedule when to run the integration job.</p> <p>For data push jobs, you can set different schedules for all-data synchronization and change synchronization.</p> <p>For details about the scheduling options, see "New Integration Job/Edit Integration Job Dialog Box" on the previous page.</p>


Job Definition


UI Element (A-Z)	Description
	Add Query. Opens the Add Query dialog box, enabling you to add an available integration query to the job definition.
	Delete Query. Enables you to delete the selected query from the job definition.
	Move Query Up/Down. Enables you to determine the order in which the queries should run.
	Edit Query Resources. Opens the Adapter Management page where you can edit the adapter resources. Only the resources defined by the adapter as related to the selected query are displayed in the Resources pane.
<Query table>	<p>Displays the queries selected for the integration job.</p> <p>For non-Jython-based Data Push jobs: Selecting a query's Allow Deletion check box enables the deletion of CIs or relationships for the query from the remote data repository. When you next perform a full synchronization, any CIs or relationships removed from the local CMDB are also deleted from the remote target.</p>
Allow Integration Job to delete removed data	<p>Enables the deletion of CIs or relationships per job from the local CMDB. When you next perform a full synchronization, any CIs or relationships removed from the remote source are also deleted from the local CMDB.</p> <p>Available for: Non-Jython-based Population jobs only.</p> <p>For details about defining CITs to be deleted by a Java-based population</p>

UI Element (A-Z)	Description
	adapter, see "How to Define CITs to be Deleted by Java-based Population Adapters" on page 235.
Select the Job Type	<p>Enables you to select the type of job queries to use for the integration.</p> <ul style="list-style-type: none"> • Changes - History-based. CIs and direct links, not virtual links. Has better performance. • RMI - Full Topology Comparison. Supports CIs and all links types. <p>Note: Calculated links are not supported.</p> <p>Available for: Service Manager Data Push jobs only</p>
Enable live job	<p>Select this option to set the job to a live data push job, which automatically performs delta synchronization when its TQL query result changes.</p> <p>Note: If you enable this option, the job's scheduler will be disabled.</p> <p>For more information about live data jobs, see "Live Data Push Jobs" on page 323.</p> <p>Available for: Data push jobs only.</p>

Scheduler Definition



UI Element (A-Z)	Description
All Data Synchronization tab	<p>Enables you to schedule a synchronization of all the data.</p> <p>Available for: Data Push jobs only</p>
Changes Synchronization tab	<p>Enables you to schedule a synchronization of the changes.</p> <p>Available for: Data Push jobs only</p>
Cron Expression	<p>Enter a Cron expression in the proper format. For a description of the fields used in Cron expressions and examples of how to use them, see Cron Expressions in the <i>Universal CMDB Modeling Guide</i>.</p>
Delta Synchronization tab	<p>Enables you to schedule a synchronization of the changes.</p> <p>Available for: Data Push jobs only</p>
Ends	<p>Enables you to select when the job should stop running.</p> <ul style="list-style-type: none"> • Never. The job continues to run until manually stopped. • Until. Enables you to select the date when the job should stop running.

UI Element (A-Z)	Description
	<p>Note: This option is disabled when you select Once.</p>
<p>Full Synchronization tab</p>	<p>Enables you to schedule a synchronization of all the data.</p> <p>Available for: Data Push jobs only</p>
<p>Repeat</p>	<p>Enables you to select how often to run the integration job. The available options are:</p> <ul style="list-style-type: none"> • Once. Runs the job only once. • Interval. Runs the job at a set time interval. • Day of Month. Runs the job on selected days of the month. • Weekly. Runs the job on a weekly basis, on the days of the week selected. • Monthly. Runs the job on a monthly basis, according to months selected. • Yearly. Runs the job every so-many years, according to the number of years specified. • Cron. Use a Cron expression to schedule a job. For a description of the fields used in Cron expressions and examples of how to use them, see Cron Expressions in the <i>Universal CMDB Modeling Guide</i>.
<p>Repeat every</p>	<p>Enables you to type a value for the interval between successive runs.</p> <p>Available: When you select Repeat > Interval or Yearly.</p> <p>Unit of time:</p> <ul style="list-style-type: none"> • Interval. Minutes; Hours; Days; Weeks • Yearly. Years
<p>Repeat on</p>	<ul style="list-style-type: none"> • Sun - Sat. When you select Repeat > Weekly, enables you to select the day or days of the week to run the job. • January - December. When you select Repeat > Monthly, enables you to select the months of the year to run the job.
<p>Repeat on the following dates every month</p>	<p>When you select Repeat > Day of Month, enables you select days of the month to run the job. The job runs every month.</p> <p>To clear the selection click  .</p>
<p>Scheduler enabled</p>	<p>When selected, you can choose scheduling options for the integration job.</p>
<p>Server Time</p>	<p>The time on the UCMDB server.</p>


UI Element (A-Z)	Description
Starts	Enables you to select the date and time when you want the job to begin running.
Time Zone	Enables you to set the required time zone. To reset default settings, click Refresh  .





New Integration Point/Edit Integration Point Dialog Box

This dialog box enables you to create a new integration point or edit the properties of an existing integration point.


To access	<p>Do one of the following:</p> <ul style="list-style-type: none"> Click the New Integration Point  button in the Integration Point pane. Click the Edit Integration Point  button in the Integration Point pane.
Important information	<p>The list of fields contains all of the items that may be specified when you create an integration point. Not all of the fields are displayed for all adapters.</p> <p>Each mandatory field is marked with an asterisk.</p>
Relevant tasks	<ul style="list-style-type: none"> "How to Set Up an Integration Point" on page 324 "How to Work with Federated Data" on page 317 "How to Work with Population Jobs" on page 318 "How to Work with Data Push Jobs" on page 320
See also	<ul style="list-style-type: none"> "Integration Studio Overview" on page 310 "UCMDB Integration Service" on page 30 For Multi-tenancy users: "Integration in a Multi-Tenancy Environment" on page 316

User interface elements are described below

UI Element (A-Z)	Description
	<p>Enables you to verify Probe connectivity using the parameters provided.</p> <p>Note: If you have defined additional Probes, these Probes are tested for connectivity as well.</p>

UI Element (A-Z)	Description
Additional Probes	<p>Enables you to select additional probes over which to run a data push or federation-type integration. Click  to select the additional probes.</p> <p>When the integration runs, if additional Data Flow Probes are defined, the server uses the most available Probe.</p> <p>Available for: Data push and federation-type integrations only.</p>
Adapter	<p>The adapter for the integration point. Click  to select an adapter. For details about each adapter, see the list of supported out-of-the-box integration adapters in the Supported Content section of the <i>Universal CMDB Discovery and Integrations Content Guide</i></p> <p>For help on the selected adapter, click the Show Content Help  button.</p>
CMDB State (Data Push)	<p>The state of the source machine. Values are:</p> <ul style="list-style-type: none"> • Actual • Authorized <p>Note: This field is visible only when using an adapter that supports data push and on a UCMDB for which authorized state has been defined.</p>
Credentials ID	<p>Enables you to select protocol credentials for relevant adapter integration points. Click  to open the Choose Credentials dialog box.</p> <p>Note: Only the required protocols for the selected integration adapter are displayed here. For information about protocols required for each integration adapter see "Required Discovery Protocols Pane" on page 258.</p>
Default Owner Name	<p>The name of the owner tenant that should be assigned to the federated, populated, or pushed CIs and relationships.</p> <p>Note:</p> <ul style="list-style-type: none"> • This field is displayed when creating a federation or population type integration point in a multi-tenancy environment only. • If no owner tenant is specified, but the Data Flow Probe selected for the integration point has an owner tenant, then the Data Flow Probe owner tenant is assigned to all discovered CIs. • The System Owner Tenant is assigned when: <ul style="list-style-type: none"> ◦ no owner tenant is specified, and no owner tenant is defined on the Data Flow Probe

UI Element (A-Z)	Description
	<ul style="list-style-type: none"> ○ the data source is not a multi-tenancy environment ● In case of push, the tenant assigned can be taken into consideration as explained in Tenant Assignment in a Multi-Tenant Scenario.
Integration Description	Enter a brief description of the integration point.
Integration Name	Enter a name for the integration point. <p>Note: The name may not exceed 45 characters.</p>
Is Integration Activated	Select this check box to create an active integration point. Clear the check box to deactivate an integration, for example, to set up an integration point without actually connecting to a remote machine. <p>Note: New integration points are set as inactive by default.</p>
Data Flow Probe	The name of the Data Flow Probe used to run integration jobs. <p>Do one of the following:</p> <ul style="list-style-type: none"> ● Use the Auto-Select option. In this case, the CMDB attempts to choose the correct Probe according to the IP ranges that were defined for the available Probes. ● Select the name of a specific Probe to use for these integration jobs. When you manually select a Probe, any ranges that you defined in the Probe settings are ignored. <p>Note:</p> <ul style="list-style-type: none"> ○ If your remote managed data repositories are accessible from the UCMDB server machine, you can use the UCMDB Integration Service option to run non-Jython-based integrations, instead of a Data Flow Probe. <p>If UCMDB Integration Service does not appear in the Data Flow Probe list, ensure that the UCMDB Integration Service is running on the UCMDB Server machine. For details, see "How to Check the UCMDB Integration Service Status" on page 62.</p> <ul style="list-style-type: none"> ○ If your Probe is an integration probe, and it does not appear in the Data Flow Probe list, ensure that it is connected.
Trigger CI Instance	Displays the CI that is to be used by the new integration point as a trigger during integration with CIs on a remote machine.

UI Element (A-Z)	Description
	<p>Click the Set Trigger CI  button, and select one of the following:</p> <ul style="list-style-type: none"> • Select Existing CI. Enables you to select the trigger CI through which data is collected during integration. For details, see "CI Instances Dialog Box" in the <i>Universal CMDB Modeling Guide</i>. • Create New CI. Enables you to create the topology of the CI to be used as the trigger. For details, see "Topology CI Creation Wizard" on page 358. <p>To manage or view the trigger CI, right-click the CI. For details on these operations, see "IT Universe Manager Page" in the <i>Universal CMDB Modeling Guide</i>.</p> <p>Available for: Jython-based integration adapters only</p> <p>Note: If the trigger CI instance used for the integration point is deleted, the integration point's jobs become disabled and cannot run. In this case, you must edit the integration point and select a new trigger CI for the integration.</p>

Note: Additional fields are available, depending on the adapter you select. Descriptions of each field may be viewed by holding your mouse over that field on the screen. See the *Universal CMDB Developer Reference Guide* for details about specific adapters.

Population Tab

This tab enables you to schedule population jobs and select the queries that are used to populate the CMDB with data.

- Schedule jobs that populate the CMDB with data from external data repositories. For details, see "[New Integration Job/Edit Integration Job Dialog Box](#)" on [page 349](#).
- View results for jobs that have run. For details, see "[Statistics Tab](#)" on [page 342](#).

To access	Select the Population tab on the Integration Studio page.
Important information	This tab is enabled only when data population is supported by the adapter on which you are basing your integration point.
Relevant tasks	"How to Work with Population Jobs" on page 318

See also	<ul style="list-style-type: none"> ◦ "Integration Studio Overview" on page 310 ◦ "UCMDB Integration Service" on page 30 ◦ "New Integration Job/Edit Integration Job Dialog Box" on page 349
-----------------	--

User interface elements are described below:


UI Element	Description
Integration Jobs pane	Enables you to specify the queries that are used to populate UCMDB with data, and to schedule jobs that contain those queries. For details, see "Integration Jobs Pane" on page 339 .
Statistics tab	Displays results for integration jobs that have run. For details, see "Statistics Tab" on page 342 .
Query Status tab	Displays information about the queries defined for the integration job. For details, see "Query Status Tab" on page 343 .
Job Errors tab	Displays the errors or warnings reported during the job run. For details, see "Job Errors Tab" on page 345 .

Select Adapter Dialog Box




This dialog box enables you to select from a list of predefined adapters that are provided out of the box.

You also have the option of adding a custom adapter for a new external data repository. For details, see ["Add an Adapter for a New External Data Source"](#) in the *Universal CMDB Developer Reference Guide*.

The Integration Framework SDK enables you to create new adapters that connect Universal CMDB with external products and services. For details, see ["Developing Java Adapters"](#) in the *Universal CMDB Developer Reference Guide*.

To access	Click  in the New Integration Point/Edit Integration Point Dialog Box.
Relevant tasks	<ul style="list-style-type: none"> • "How to Work with Federated Data" on page 317 • "How to Work with Population Jobs" on page 318 • "How to Work with Data Push Jobs" on page 320
See also	"New Integration Job/Edit Integration Job Dialog Box" on page 349

User interface elements are described below:

UI Element (A-Z)	Description
	Click to collapse the hierarchical tree structure.
	Click to expand the hierarchical tree structure.
	Click to display help about the selected adapter.
<list of adapters>	<p>Displays a list of out-of-the-box integration adapters.</p> <ul style="list-style-type: none"> For details about multiple-UCMDB integration adapters, see "Integrating Multiple CMDBs" on page 364. For details about adapters used to integrate UCMDB with other Micro Focus products and Third-Party products, and about integration tools, provided out-of-the-box with the Discovery and Integrations Content Pack, see <i>HPE UCMDB Discovery and Integrations Content Guide - HPE Integrations</i> and <i>HPE UCMDB Discovery and Integrations Content Guide - Third Party Integrations</i>.

Topology CI Creation Wizard

This wizard enables you to save a topology to the CMDB for a new adapter. This adapter can include elements from a defined topology already existing in the CMDB as well as new elements.

For example, say a node and its IP address exist in the CMDB as a defined topology. However, the adapter Input query defines a Microsoft SQL Server database element related to that node. This extended topology does not exist in the CMDB. When using the wizard to create the topology, CMDB identifies the existing node and IP address by the properties values you enter, connects the new MSSQL database CI to the topology, and saves the complete topology in the CMDB.

Note: You cannot use an abstract or federated CIT to create a Trigger CI.

To access	<p>Select a discovery Jython adapter in the New Integration Point dialog box. In the Trigger CI Instance menu, choose Create New CI.</p> <p>Note: This wizard is available for discovery Jython adapters only, when the Used as Integration Adapter check box is selected in Adapter Management. Moreover:</p> <ul style="list-style-type: none"> All conditions (attributes, cardinality, qualifiers, and so on) are disregarded in the Input query. Only regular links (that is, not join or compound links) are allowed in the
------------------	--


	<p>Input query.</p> <p>For details on the Used as Integration Adapter check box, see "Adapter Definition Tab" on page 253.</p>
Important information	<ul style="list-style-type: none"> • Prerequisite: To ensure that reconciliation rules work with the created topology, prepare details of the CIs (for example, values for key properties) as these details are needed during the wizard creation procedure. • If there are any errors during creation, the Summary page includes an error message and a link to the error details. • At the end of the topology creation, the source CI is defined as the Trigger CI instance.
See also	"New Integration Point/Edit Integration Point Dialog Box" on page 353
Wizard Map	<p>The Topology CI Creation wizard contains:</p> <p>"Topology Preview" > "Define CI: <CI name>" > "Define Credentials" > "Topology Creation" > "Summary"</p>

Topology Preview

Enables you to preview the topology definition of the integration point.

Wizard Map	<p>The Topology CI Creation wizard contains:</p> <p>Topology Preview > "Define CI: <CI name>" > "Define Credentials" > "Topology Creation" > "Summary"</p>
-------------------	--

User interface elements are described below:

UI Element (A–Z)	Description
	Show Legend. Toggles between hiding and displaying the topology legend.
<toolbar and legend>	For details, see Topology Map Sidebar in the <i>Universal CMDB Modeling Guide</i> .

Define CI: <CI name>

Enables you to define properties of a new CI instance of the CIT.

Important Information	<ul style="list-style-type: none"> • This page of the wizard is displayed for each element in the query. • Several elements of the same CIT may exist in the query.
------------------------------	---

Wizard Map	The Topology CI Creation wizard contains: "Topology Preview" > Define CI: <CI name> > "Define Credentials" > "Topology Creation" > "Summary"
-------------------	--

User interface elements are described below:

UI Element (A–Z)	Description
Define New CI Properties	Drill down to the property to be used to identify the CIT. Select the field next to the property name and enter a new value (or choose from existing values). Note: If the selected CIT is abstract or federated, the properties are not displayed.
Select CI Type	Select the CIT for which you are defining a new CI instance.

Define Credentials

Enables you to define credentials for the new CI.

Important Information	<ul style="list-style-type: none"> Any changes you make here to a protocol (updating, adding, or removing) affect the protocol throughout DFM. Therefore, you must ensure that changes you make (for example, to a password) are valid. If the change is not valid, the Data Flow Probe will fail to connect at the next attempt. Any updates you make here can be viewed in the Data Flow Probe Setup window. For details, see "<Protocol> Details Pane" on page 113. This page is displayed if the adapter writer has defined that credentials are needed to access the discovered component.
See Also	<p>For details on using the buttons and shortcut menus, see "<Protocol> Details Pane" on page 113.</p> <p>For details on each protocol, see the <i>Universal CMDB Discovery and Integrations Content Guide</i>.</p>
Wizard Map	The Topology CI Creation wizard contains: "Topology Preview" > "Define CI: <CI name>" > Define Credentials > "Topology Creation" > "Summary"

Topology Creation

Enables you to read through the topology details (the CIs and relationships that are to be created) and make changes if required.

Important Information	Review the topology. To make changes, click the Back button.
Wizard Map	The Topology CI Creation wizard contains: "Topology Preview" > "Define CI: <CI name>" > "Define Credentials" > Topology Creation > "Summary"

Summary

Displays the result of the topology creation.

Important Information	<ul style="list-style-type: none"> If a success message is displayed, click Finish. <div style="border-left: 2px solid black; padding-left: 10px; margin-left: 20px;"> <p>Note: For Population integration points, if at least one query ends with a warning and no errors are encountered, a Success with warnings message is displayed.</p> </div> A CI in the topology you create may be ignored by the reconciliation process if it matches an existing CI. If the SOURCE CI in the topology is ignored, the topology creation process fails. If another CI is ignored (any other node in the query), creation succeeds. This is because the SOURCE CI is needed by the query to create the Trigger CI. If it is ignored, the trigger cannot be identified and used for the integration. For details on the reconciliation process, see "Reconciliation Overview" on page 739. If DFM cannot create the topology, an error message is displayed. Click the link to review the error details in the ui-server.log file, located in the following folder: C:\hp\UCMDB\UCMDBServer\runtime\log\. Then, click Back to fix the error and run the wizard again.
Wizard Map	The Topology CI Creation wizard contains: "Topology Preview" > "Define CI: <CI name>" > "Define Credentials" > "Topology Creation" > Summary

Limitations – Integration Studio

This section describes certain limitations on the Integration Studio functionality.

This section includes the following topics:

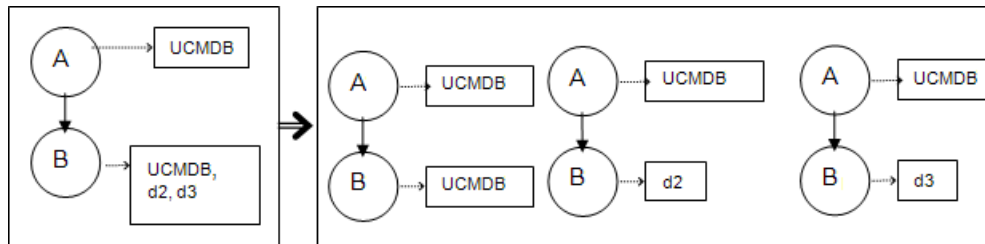
- ["Limitations on Population Integrations" below](#)
- ["Limitations on Federation Integrations" below](#)
- ["Limitations on Data Push Integrations" on the next page](#)

Limitations on Population Integrations

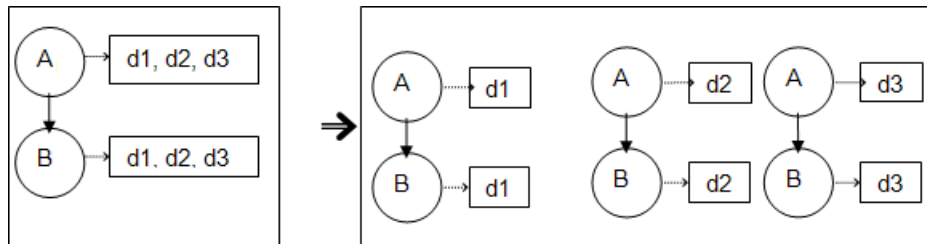
1. When configuring a population job between two CMDBs, verify that the synchronized CITs are the same in the two CMDBs.
2. When modifying a TQL query that is used in a population job, it is recommended to run a differential synchronization before modifying the TQL and a full synchronization after modifying the TQL. The differential synchronization removes any data that is no longer necessary as a result of the updated query, and the full synchronization creates new baseline data on the target system.
3. After a job runs successfully, its status remains **Succeeded** even after the job definition is changed (for example, selecting another TQL query or enabling deletion) and saved.

Limitations on Federation Integrations

1. When a virtual link exists between two data repositories, Universal CMDB supports mapping in the following cases only:
 - The UCMDDB integration point lies at one end of the link and multiple data repositories lie at the other end. The Cartesian product is calculated for A's data repository (UCMDDB) and B's data repositories (UCMDDB, d2, d3).



- o The same data repositories lie at both ends of the link. The link is an internal link of each data repository and no mapping is required.



2. When changes are made in the Modeling Studio and these changes affect the results of a TQL query, federated CIs in the view are not updated. This is because federated TQL queries are calculated ad hoc only and are not updated when a view is recalculated. To update the federated CIs, select the view in the CI Selector and click the **Refresh CIs Tree** button. (Note that the recalculation may take a long time.) For details, see "Browse Views Mode" in the *Universal CMDB Modeling Guide*.
3. You cannot edit the values of attributes that are configured to be retrieved from both an external data repository and UCMDB during federation.

Limitations on Data Push Integrations

1. After modifying a TQL query that is used in a data push job, it is recommended to run a differential synchronization before modifying the TQL and a full synchronization after modifying the TQL. The differential synchronization removes any data that is no longer necessary as a result of the updated query, and the full synchronization creates new baseline data on the target system.
2. The Universal CMDB cannot push static attributes.

Chapter 10: Integrating Multiple CMDBs

This chapter includes:

Integrating Multiple CMDBs Overview	364
Use Cases – Multiple CMDB Deployments: Discovery-CMS Solution	365
Multiple Deployments with Version 9.x/10.x CMDBs Using Population	366
Multiple Deployments with Version 9.x/10.x CMDBs Using Data Push	370
Federation in Version 9.x/10.x CMDBs	371
How to Perform Initial UCMDB-UCMDB Synchronization	372
How to Configure Global ID Generation	373
How to Use SSL with the UCMDB 9.x/10.x Adapter	374
How to Set Up Integrations Between Multiple CMDBs	375
How to Push Data from Authorized State to Actual State	380
How to Protect CIs from Being Deleted on Target CMDBs during Data Push	381
Troubleshooting and Limitations – Multiple CMDB Integration	383

Integrating Multiple CMDBs Overview

Multiple CMDBs is a solution that allows setting up a multiple number of CMDBs for delegating the workload and responsibility of the solution to the different CMDBs.

The Configuration Management System, **CMS**, is the central CMDB server and is the authority for configuration management in the multiple CMDBs solution. It is responsible for integrating between the different CMDB server instances and other services in the solution, as well as for generating global IDs.

The **global ID** is a unique CI ID that identifies that CI across the entire portfolio, making it easier to work in multiple CMDB environments. The global ID is generated by the CMS or another CMDB that has been designated as a global ID generator for that CI type. The class model contains the **global_id_scope** attribute, which is used to specify the scope to which a particular CI type belongs. In the JMX console, you can specify the scopes for which global IDs will be generated. For details, see ["How to Configure Global ID Generation" on page 373](#).

Most of the integrations are defined in the CMS, and other CMDBs or services only access the CMS to access the data from these CMDBs or services.

The CMS allows integration with other services using:

- Population
- Federation
- Data Push
- Data Flow Management Web Service API
- Soap Web Service

Note: Synchronization between multiple CMDBs of different versions can be performed only between UCMDB versions 9.02 or later.

Use Cases – Multiple CMDB Deployments: Discovery-CMS Solution

The Discovery-CMS solution enables the division of the workload and Discovery capacity over more than one CMDB.

- Discovery 1 CMDB
- Discovery 2 CMDB
- The central CMDB acting as the CMS

Both Discovery CMDBs are responsible for running different discovery jobs in the domain, and containing all the discovered topology. The CMS populates the node, interface, and IP from both Discovery CMDBs, and federates the node resource CIs (CPU, file system, and printer) from Discovery 1 CMDB. The CMS federates the node resource CIs (OS user, process, and printer) from Discovery 2 CMDB. When a user runs a view that requests these resources on the CMS, they are brought seamlessly using federation.

Multiple Deployments with Version 9.x/10.x CMDBs

Using Population

When you use the UCMDb 9.x or UCMDb 10.x adapter to create an integration point, you are able to synchronize data between different CMDB instances using either population or data push. For details on the data push method, see ["Multiple Deployments with Version 9.x/10.x CMDBs Using Data Push" on page 370](#).

This section includes:

- ["Population from UCMDb 9.x/10.x \(CMS Synchronization\)" below](#)
- ["Query Support" below](#)
- ["Global ID Synchronization" on the next page](#)
- ["Automatic Completion of Reconciliation Data" on page 369](#)

Population from UCMDb 9.x/10.x (CMS Synchronization)

During population, global IDs are synchronized. For details, see ["Global ID Synchronization" on the next page](#).

For details on population, see ["How to Work with Population Jobs" on page 318](#).

Query Support

In the population flow, the job queries are retrieved from the remote UCMDb.

Two types of queries are supported for population jobs:

- **Live queries.** All non-federated TQL queries, when they are used for population with the UCMDb 9.x/10.x adapter.

Live queries require less bandwidth, and cause less load on the source system. There may be a short delay from the time the change is made until the live query mechanism or the population job receives the change (this may take up to several minutes).

Subgraphs and compound relationships are supported in queries. When using compound relationships, you must select **Show full path between source and target CIs** in the Compound Relationship properties of the query.

- **Federated queries.** Queries that contain at least one federated node or attribute.

When the UCMDb 9.x/10.x adapter is used, federated queries may also be used for population.

Federated queries are calculated each time the integration is performed; the entire result set is retrieved and filtered by the Probe.

The deletion of CIs is not supported. The aging mechanism must be used, since no information about the deletion of CIs or links is populated. For details, see CI Lifecycle and the Aging Mechanism in the *Universal CMDB Administration Guide*.

You can create TQL queries for integration. For details, see Topology Query Language in the *Universal CMDB Modeling Guide*.

Global ID Synchronization

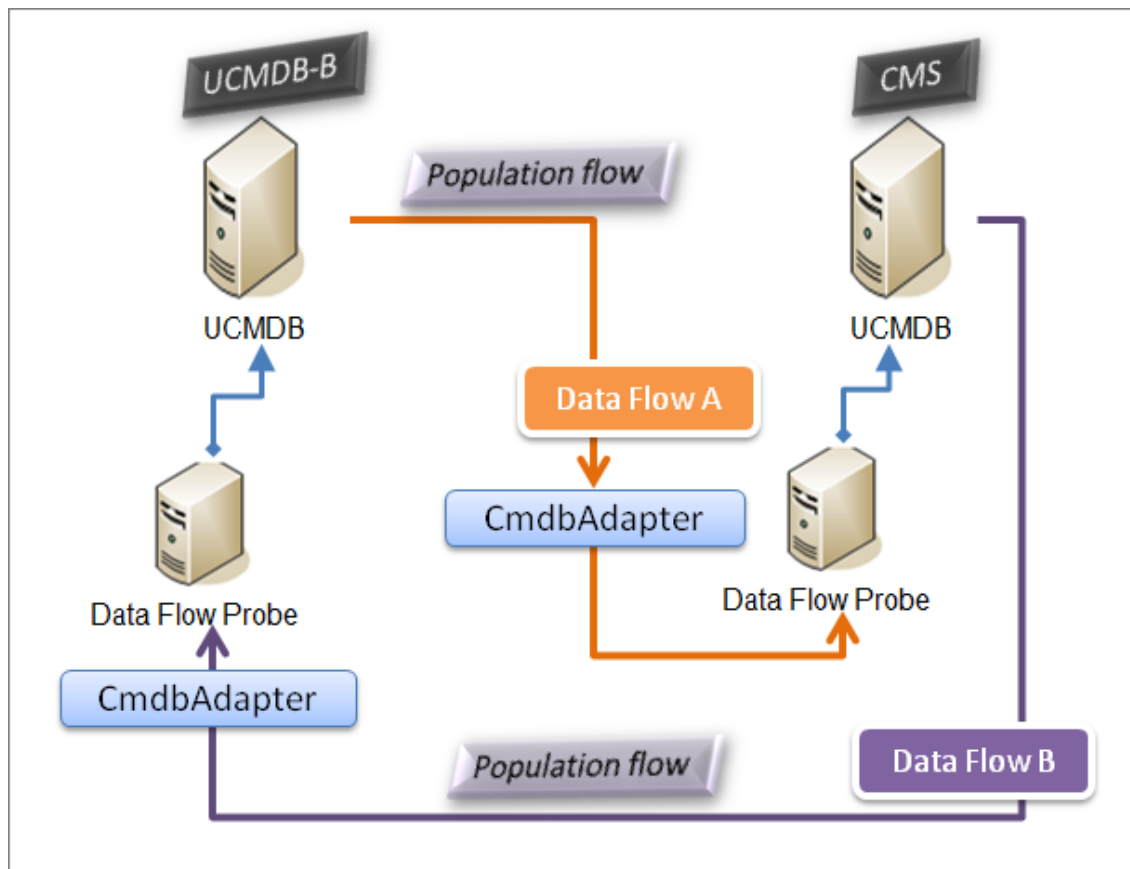
The following examples describe two types of synchronization that can be performed:

- Two-way ID synchronization

Synchronization of data occurs in both directions between two UCMDb instances.

The CMS uses the population flow to retrieve data from UCMDb-B, which may be any UCMDb. UCMDb-B uses the population flow to populate data from the CMS.

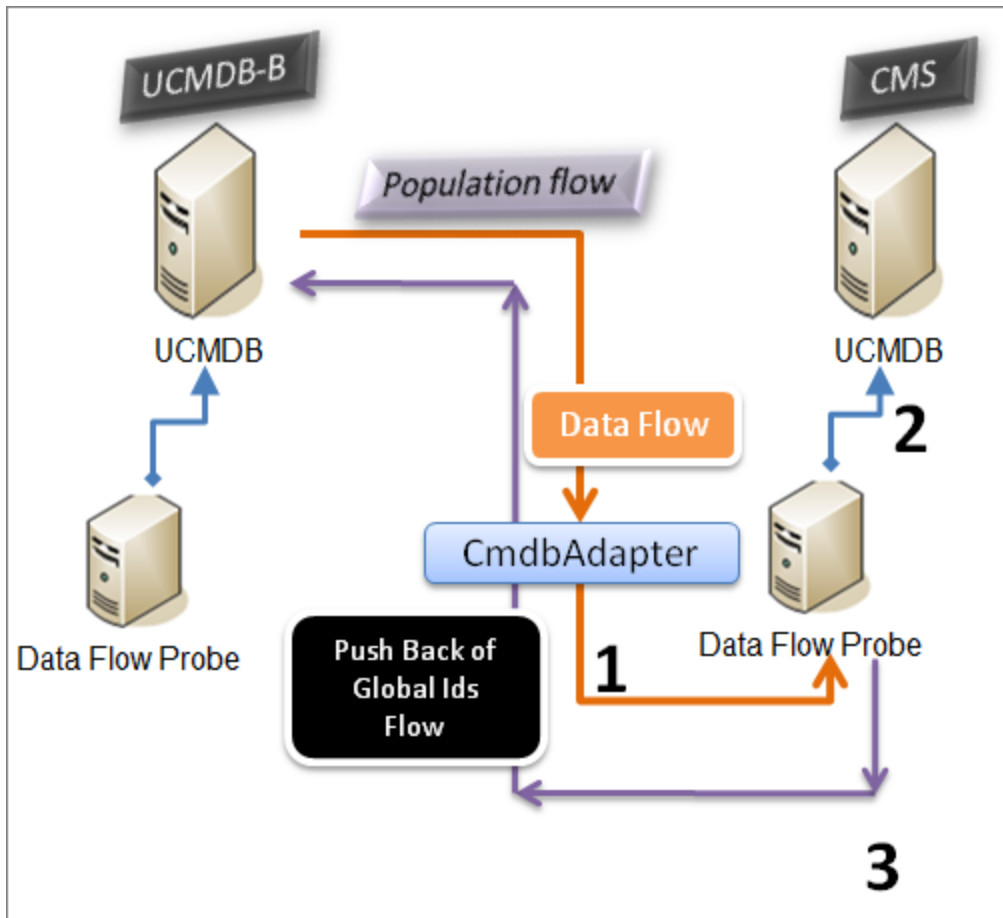
Because synchronization is performed in two directions, global IDs are also updated on UCMDb-B.



- Pushback of IDs

The CMS uses the population flow to retrieve data from UCMDB-B. CIs are reconciled with the data in the CMS.

The global-ID in the CMS for each CI received is pushed back to UCMDB-B.



The default state of this option is disabled.

For details about enabling the pushback of IDs, see "[How to Set Up Integrations Between Multiple CMDBs](#)" on page 375.

Automatic Completion of Reconciliation Data

The UCMDB 9.x/10.x adapter automatically retrieves data needed for the reconciliation process of the CIs brought by the population flow. The actual data retrieved is determined by the reconciliation rule defined for the CITs of the TQL query. This is necessary to ensure that the identification process is executed accurately and no CIs are incorrectly merged.

For example, if your population TQL query includes a node but does not have any layout selected, the actual data that enters the CMDB is:

- Nodes, with layout
 - name
 - bios_uuid
 - serial_number
 - additional data, according to the defined reconciliation rule
- IP Addresses, with layout
 - name
 - routing_domain
- Interfaces, with layout
 - mac_address
 - interface_name

Note:

- The automatic completion feature may actually synchronize many more CIs or links than you intend.
- The automatic completion feature always retrieves the Global ID.
- By default, if data required for the reconciliation of a particular CI cannot be retrieved (for example, if the data is missing in the source), that CI is ignored without causing the entire job to fail. You can change this behavior in the CmdbAdapter configuration. For details, see ["Adapter Configuration Tab" on page 259](#).

Multiple Deployments with Version 9.x/10.x CMDBs Using Data Push

When you use the UCMDDB 9.x or UCMDDB 10.x adapter to create an integration point, you are able to synchronize data between different CMDB instances using either population or data push. For details on the population method, see ["Multiple Deployments with Version 9.x/10.x CMDBs Using Population" on page 366](#).

For details on the data push flow for setting up an integration between multiple CMDBs, see ["How to Set Up Integrations Between Multiple CMDBs" on page 375](#).

Limitations

The following limitations apply to the data push method:

- An integration point for data push can only be defined in UCMDb version 10.01 or above.
- The target CMDB must be either UCMDb version 9.05 CUP 9 and later CUPs, or UCMDb version 10.01 and above (it is not supported for UCMDb version 10.00).
- A single TQL query in the data push flow is limited to 5 million CIs and relationships. This limitation is only for a single query; multiple TQL queries in multiple jobs may exceed this limit.
- Data Push is not supported for virtual links.

In the data push flow, a local TQL query collects data from the local CMDB and pushes this data to the remote CMDB. The adapter filters out unsupported CITs and relationships, and it also filters out any invalid-links and attributes.

Note: Data push is also supported for CIs and relationships from federation adapters with their **LastModifiedTime** property.

Auto Complete Reconciliation

When pushing CIs or relationships to a remote CMDB, any CI or attribute that is needed for reconciliation (according to the remote CMDB reconciliation rules) is automatically added to the CIs and attributes already requested. This is necessary to ensure that the identification process is executed accurately and no CIs are incorrectly merged.

Note: This may cause more data than originally selected in the TQL query to be transferred.

Federation in Version 9.x/10.x CMDBs

Federation allows the CMDB to retrieve data in real time (on-the-fly) from any remote data repository, and combine it with the CMDB's internal data to show a complete picture of the configuration it manages, including multiple sources. For more information about federation, see ["How to Work with Federated Data" on page 317](#).

Using the UCMDb 9.x/10.x adapter to federate data from different CMDBs, enables the federation of any CIT in the model. This means that only a small portion of data from the remote CMDBs can be populated, and the rest of the data is federated on demand. This ability enables the delegation of the

information to multiple CMDBs, with the CMS always showing the most updated data available and at the same time not overloading its capacity.

A CMS populates the Node, Interface, and IP from a Discovery CMDB (a CMDB whose role is to run Discovery), and defines the CPU, File System, OS, User, Printer, and Process CIs as federated from the same source. When a user runs a TQL query or view that has any federated CIs, these specific CIs are brought in real time from the Discovery CMDB. They are therefore as updated as the Discovery CMDB and do not depend on the population schedule to receive updated information. In addition, these CIs only reside on the Discovery CMDB, and do not burden the capacity of the CMS.

The CMDB 9.x/10.x adapter supports the delegation of the federation capabilities, providing the ability to set up a single point for data retrieval (usually the CMS). Any CMDB or service that uses the CMDB's ability to delegate federation uses the CMDB as a virtual black box, and is unaware of whether data comes directly from the CMS or from an external integration.

Note: When you set up a federation flow, be careful not to cause an endless loop. For example, do not set up CMDB-X to federate data from CMDB-Y, and at the same time CMDB-Y to federate data from CMDB-X.

How to Perform Initial UCMDB-UCMDB Synchronization

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

1. On the UCMDB server, launch a Web browser and enter the following address:
https://localhost:8443/jmx-console.
2. Locate **UCMDB:service=Multiple CMDB Instances Services** to open the JMX MBEAN View page.
3. Click the **fetchAllDataFromAnotherCMDB** operation.
4. Enter values as required for the following fields:

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

- **customerID:** The customer ID.
 - **remoteUserName:** The remote user name.
 - **remotePassword:** The remote password.
 - **remoteHostProtocolHttps:** Click **True** if the remote host protocol is HTTPS; click **False** if the remote host protocol is HTTP.
 - **remoteHostName:** The remote host name.
 - **remotePort:** The remote port. If no value is given, the default is **8443**.
 - **remoteCustomerName:** The remote customer name (the default value is **Default Client**).
 - **chunkSize:** The maximum chunk size. (the default value is 20000)
 - **ciTypeToSync:** The CI type to sync (the default value is **managed_object**, causing all CI types to be synchronized).
 - **linkTypeToSync:** The relation type to sync (the default value is **managed_relationship**, causing all relation types to be synchronized).
 - **remoteVersion:** The major version of the remote machine (9 or 10. Local machine version by default).
5. Click **Invoke**.

How to Configure Global ID Generation

1. Launch the Web browser and enter the following address:
https://<CMS server>:8443/jmx-console.
2. Click **UCMDB:service=Multiple CMDB Instances Services** to open the JMX MBEAN View page.

3. Click one of the following methods and enter values as required:

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

4. Click **Invoke**.

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

How to Use SSL with the UCMDB 9.x/10.x Adapter

If the remote UCMDB server uses a certificate signed by a known certificate authority, selecting the HTTPS (SSL) value in the **Protocol** field is sufficient.

If not, add the remote UCMDB server certificate to the local UCMDB JVM Trusted Stores as follows:

1. Export the remote UCMDB self-signed certificate by executing the following command (on the remote server machine):

```
c:\hp\UCMDB\UCMDBServer\bin\jre\bin\keytool.exe -exportcert -  
keystore c:\hp\UCMDB\UCMDBServer\conf\security\server.keystore -  
alias hpcert -storepass <keystore pass> -file remoteServer.cert
```

2. Copy the certificate to UCMDB at **C:\hp\UCMDB\UCMDBServer\bin\jre\bin** and to the Data Flow Probe at **C:\hp\UCMDB\DataFlowProbe\bin\jre\bin**.
3. Locate the JRE security folder, by default located in **C:\hp\UCMDB\UCMDBServer\bin\jre\lib\security** and also at **C:\hp\UCMDB\DataFlowProbe\bin\jre\lib\security**.
4. Back up the **cacerts** file by copying it to another folder.
5. Open a command line window and execute the following commands on the local UCMDB and Data Flow Probe (to import the previously created or copied certificate):


```
cd C:\hp\UCMDB\<UCMDBServer/DataFlowProbe>\bin\jre\bin
keytool.exe -import -storepass <truststore pass> -keystore
c:\hp\UCMDB\<UCMDBServer/DataFlowProbe>\bin\jre\lib\security\
cacerts -trustcacerts -file
C:\hp\UCMDB\<UCMDBServer/DataFlowProbe>\bin\jre\bin\remoteServer.cert
```

6. At the command line prompt "Trust this certificate?", enter **yes**.
7. Restart the UCMDB service and the Data Flow Probe service.

How to Set Up Integrations Between Multiple CMDBs

The following steps describe how to create integration points and jobs to integrate between multiple CMDBs:


- ["Define an integration point" below](#)
- ["Define and run a population job" on page 378](#)
- ["Define and run a data push job" on page 378](#)
- ["Select CI types and attributes to be federated" on page 379](#)

1. Define an integration point
 - a. Navigate to **Data Flow Management > Integration Studio**.
 - b. Click the **New Integration Point**  button to open the New Integration Point Dialog Box. For details, see ["New Integration Point/Edit Integration Point Dialog Box" on page 353](#).

Enter the following information:

Name (A-Z)	Recommended Value	Description
Integration Name	<user defined>	The name you give to the integration point.
Integration Description	<user defined>	Free text that describes the integration point.

Name (A-Z)	Recommended Value	Description
Adapter	UCMDB 9.x or UCMDB 10.x	The adapter that is used to integrate between multiple CMDBs.
Is Integration Activated	selected	Select this check box to create an active integration point.
Hostname/IP	<user defined>	The name or IP address of the remote CMDB machine. Note: For a push synchronization, if the remote UCMDB machine is a High Availability environment, use the remote UCMDB Write-VIP URL.
Port	8443	The port listened to by the UCMDB API.
Web application Root Context	<user defined>	The root context value of the remote CMDB. If no root context is defined on the remote CMDB, leave this field empty.
Protocol	HTTPS (SSL)	Selects the protocol to be used for connecting to the remote CMDB. Valid values are: <ul style="list-style-type: none"> • HTTP • HTTPS (SSL)
Credentials ID	Remote UCMDB	If you must create a new credential protocol, use the Generic Protocol as a basis. For details, see <i>Universal CMDB Discovery and Integrations Content Guide</i> .
Customer Name	<user defined>	The name of the remote UCMDB from which you want to retrieve data.
Remote Machine State	<user defined>	The state with which you want to connect when integrating with multi-state CMDBs. <ul style="list-style-type: none"> • Actual • Authorized
Push Back Ids For Population	<user defined>	Introduced in version 10.21, allows you to schedule the pushback of global IDs after CIs are populated into UCMDB, without creating an integration point when using UCMDB 10.x adapter. Valid values: Enabled, Disabled. Default: Disabled.

Name (A-Z)	Recommended Value	Description
Push Back Ids For Push	<user defined>	<p>Introduced in version 10.21, allows you to schedule the pushback of global IDs after CIs are pushed into UCMDB, without creating an integration point when using UCMDB 10.x adapter.</p> <p>Valid values: Enabled, Disabled. Default: Disabled.</p>
Data Flow Probe	<user defined>	<p>Specifies which data flow probe will be used by the integration.</p>
Default Owner Name	<user defined>	<p>The name of the owner tenant that should be assigned to the federated, populated, or pushed CIs and relationships.</p> <p>Note:</p> <ul style="list-style-type: none"> • This field is displayed when creating a federation or population type integration point in a multi-tenancy environment only. • If no owner tenant is specified, but the Data Flow Probe selected for the integration point has an owner tenant, then the Data Flow Probe owner tenant is assigned to all discovered CIs. • The System Owner Tenant is assigned when: <ul style="list-style-type: none"> • no owner tenant is specified, and no owner tenant is defined on the Data Flow Probe • the data source is not a multi-tenancy environment • In case of push, the tenant assigned can be taken into consideration as explained in Tenant Assignment in a Multi-Tenant Scenario.
Additional Probes	<user defined>	<p>Additional probes over which to run a federation-type integration. Click  to select the additional probes.</p> <p>When the integration runs, if additional Data Flow Probes are defined, the server uses the most available Probe.</p>

- c. Click **Test Connection** to ensure that the integration point has been successfully created, and then click **OK**.
- d. Click **OK**.

You can use your integration point with any of the methods described below, population jobs, data push jobs, or federation.


2. Define and run a population job

An out-of-the-box integration point already contains population jobs. This step is relevant only when creating additional population jobs.

Select the **Population** tab to define a population job that uses the integration point you defined above. For details, see ["New Integration Job/Edit Integration Job Dialog Box" on page 349](#).

Note:

- When integrating between multiple CMDBs, population queries must be set up for the source CMDB.
- Select the **Allow Integration Job to delete removed data** check box if you want your population job to allow deletion of CIs and links from the source CMDB.
- By default, infrastructure CIs and containment relationships are deleted. All other CIs and relationships are retained.
- **For Multi-tenancy users:** When running population with the Cmdb10xAdapter in a multi-tenancy environment, the tenants are automatically synchronized. To receive changes about the tenants (owner and user), **Owner Tenant** and **Consumer Tenants** must be defined in the TQL query layout.

Click the **Run Changes Sync**  button to make sure that the integration has been successfully configured.

3. Define and run a data push job


Select the **Data Push** tab to define a data push job that uses the integration point you defined above. For details, see ["New Integration Job/Edit Integration Job Dialog Box" on page 349](#).

Note:

- When integrating between multiple CMDBs, data push queries must be set up on the local CMDB.
- Select the **Allow Deletion** check box for each query if you want your data push job to allow deletion of CIs and links from the remote CMDB.
- By default, infrastructure CIs and containment relationships are deleted. All other CIs and

relationships are retained.

- **For Multi-tenancy users:** When running data push with the Cmdb10xAdapter in a multi-tenancy environment, the tenants are automatically synchronized. To receive changes about the tenants (owner and user), **Owner Tenant** and **Consumer Tenants** must be defined in the TQL query layout.

Click the **Run Changes Sync**  button to make sure that the integration has been successfully configured.

4. Select CI types and attributes to be federated
 - a. Navigate to **Data Flow Management > Integration Studio**.
 - b. Click the **Federation** tab.
 - c. Select the CI types you want to federate from the source CMDB.

If desired, you can select only attributes to be federated. For details, see ["Federation Tab" on page 337](#).

- d. Click **Save Integration Point** .

How to Enable Scheduling Pushback of Global IDs When Using UCMDB 10.x Adapter

As an integration administrator, starting from version 10.21, you are able to schedule the pushback of global IDs without creating an integration point when using UCMDB 10.x adapter.

Two new settings are added to the Create/Edit Integration Point dialog box if you select the UCMDB 10.x adapter (**Cmdb10xAdapter**):

- **Push Back Ids For Population.** Specifies whether you want to push back global IDs after CIs are populated into UCMDB. Valid values: Enabled, Disabled. Default: Disabled.
- **Push Back Ids For Push.** Specifies whether you want to push back global IDs after CIs are pushed into UCMDB. Valid values: Enabled, Disabled. Default: Disabled.

Note:

- For links, these two settings work only if you create integrations between the following UCMDB versions:
 - From 10.21 to 10.21
 - From 10.21 to 10.11 CUP5
 - From 10.11 CUP4 to 10.11 CUP5
 - From 10.11 CUP5 to 10.21Otherwise this functionality does nothing, it will just log an error message “Push back ids for links is not supported. Probably the target server version does not support this functionality”.
- For CIs, the new settings work on all versions of UCMDB.

To enable scheduling pushback of global IDs,

1. Check and make sure that the `<push-back-ids>` tag as follows is present in the `adapter-capabilities` section of the adapter configuration file:

```
<support-replicatioin-data>
  <target>
    <push-back-ids/>
  </target>
</support-replicatioin-data>
```

2. Configure the integration point.
 - Open an existing integration point and set **Push Back Ids For Population** or **Push Back Ids For Push** to **Enabled**.
 - Create a new integration point and set **Push Back Ids For Population** or **Push Back Ids For Push** to **Enabled**.

How to Push Data from Authorized State to Actual State

UCMDB allows you to create an integration point by using a new adapter called **Local State Push Adapter** to push data from the authorized state to the actual state. You can use a TQL query to specify the data being pushed.

To do this, follow these steps:

1. Log in to UCMDB in the authorized state, and then go to **Data Flow Management > Integration Studio**.
2. Click **New Integration Point**, and then specify the following integration properties:
 - Integration Name:** Specify the name of the new integration point.
 - Adapter:** Select Local State Push Adapter.
 - Is Integration Activated:** Select this option
3. Specify the adapter properties:
 - Local Customer Name:** Specify the customer.
 - Local State:** Select Actual.
4. Click **OK**.

After you create the integration point, you need to create an integration job and specify the TQL query in the Job Definition. For more information about how to do this, see the following topics:

- ["New Integration Job/Edit Integration Job Dialog Box" on page 349](#)
- ["How to Work with Data Push Jobs" on page 320](#)




How to Protect CIs from Being Deleted on Target CMDBs during Data Push

For data push integrations of multiple CMDBs using Cmdb10xAdapter, you can protect CIs of specified CI Types from being deleted on the target CMDBs during data push to keep a record of historical changes, by specifying CI Types that you want to protect from deletion in the `<remove-cis>` tag section of the Cmdb10xAdapter source.

Note: This feature is supported for data push integrations from CMDBs of version 10.30 (or later) to other CMDBs of version 10.xx using Cmdb10xAdapter.

To protect CIs from being deleted on target CMDBs during data push:

1. Log in to the source UCMDB server of version 10.30 (or later), and access Cmdb10xAdapter in either of the following ways:

- o Go to **Data Flow Management > Integration Studio**. In the Integration Point pane, right-click the integration point of your choice, and select  **Go To Adapter** from the context menu. Then right-click the selected **Cmdb10xAdapter** in the Resources pane of the Adapter Management module, and select  **Edit adapter source** from the context menu.
 - o Go to **Data Flow Management > Adapter Management**. In the Resources pane, right-click **Cmdb10xAdapter** and select  **Edit adapter source** from the context menu.
2. Edit the **Cmdb10xAdapter** source to enable CI Type protection and to specify CI Types to protect.

- a. In the Adapter Source Editor, locate the `<remove-cis>` tag section, which looks like the following:

```
<remove-cis isEnabled="false">  
  <ci-type>link</ci-type>  
  <ci-type>object</ci-type>  
</remove-cis>
```

- b. Change the value of the **isEnabled** setting from **false** to **true**.
- c. Modify the values in the `<ci-type>` tags to include the CI Types that you want to protect from deletion only.

Add more `<ci-type>` tag lines if necessary.

Note:

- CI Types names are case-sensitive. You can get the correct CI Types names from **Modeling > CI Type Manager**
- You can only specify and protect CI Types that already exist on the target CMDBs. Otherwise you will see warning messages that the CI type may not exist on target UCMDb in **C:\hp\UCMDB\UCMDBServer\integrations\runtime\log\<integration_point>.log**.

- d. Click **Save**.
- e. Click **Finish**.

The changes take effect right away, and the specified CI Types are protected from being deleted on the target CMDBs during the future data push.

3. (Optional) Delete a CI of protected CI Type from the source CMDB, and then go to **Data Flow Management > Integration Studio**, and run the data push integration job by clicking **Run Job** -

Synchronize Changes  or **Run Job - Synchronize All Data** .

The CI of the protected CI Type should still exist on the target CMDB.

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
 - cldb.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 UCMDDB 9.x /10.x adapter uses the UCMDDB API for connection, set up an integration user to ensure that you provide proper credentials. For details, see "Create an Integration User" in the *Universal CMDB Developer Reference Guide*.

- **Problem.** The Data Push job fails with the message "Remote UCMDDB version is not supported."

Solution. The Data Push flow only supports pushing to UCMDDB version 9.05 CUP 9 and later CUPs, or UCMDDB version 10.01 and later (it does not support pushing to UCMDDB version 10.00). Upgrade your remote UCMDDB or alternatively, run the integration using the population flow.

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.

Chapter 11: Integrating UCMDB with CyberArk Enterprise Password Vault

This section includes:

Overview	387
Deployment	387
How the CyberArk Integration Works	388
Supported Versions	388
Supported CyberArk Versions	388
Supported Probe Types	388
Supported Protocols	389
How to Configure CyberArk Integration	389
CyberArk Integration Configuration Workflow	391
How to Configure CyberArk Integration	392
How to Create and Configure CyberArk Account for the Integration	399
How to Add CyberArk Credential for Protocols from JMX	407
How to Calculate Hash Code for JARs with Annotation	408
How to Set a Default List of CyberArk Properties Using JMX	409
CyberArk Integration Troubleshooting and Limitations	411

Overview

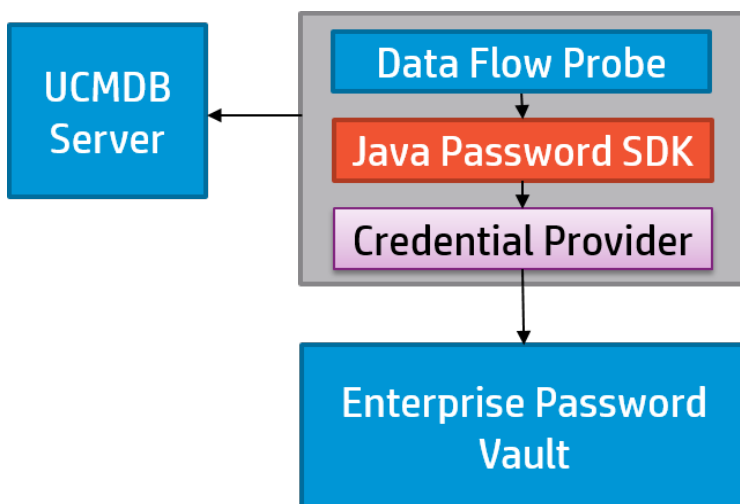
CyberArk's Application Identity Management solution uses the Privileged Account Security solution to eliminate the need to store application passwords embedded in applications, scripts or configuration files, and allows these highly-sensitive passwords to be centrally stored, logged and managed within the Vault. This unique approach enables organizations to comply with internal and regulatory compliance requirements of periodic password replacement, and monitor all activities associated with all types of Privileged Identities whether on-premise or in the cloud, across operating systems, databases, applications, hypervisors, network devices, and more.

The integration between UCMDB and CyberArk's Application Identity Management allows Universal Discovery administrators to configure credentials for supported Universal Discovery protocols, which enables administrators to manage the credentials in a secure and easy way.

Instead of storing the passwords themselves in UCMDB/UD, this integration involves storing only references (in the CyberArk Enterprise Password Vault part of the Privileged Account Security Solution) to the passwords, and retrieving (using CyberArk's AIM SDK) the passwords when they are needed from the digital vault using the stored references.

Deployment

The following diagram illustrates the overall deployment.



How the CyberArk Integration Works

The CyberArk integration enables UCMDB/UD to retrieve usernames and passwords from the CyberArk Enterprise Password Vault as follows:

1. Administrators to create a Safe, Application, and Account on the CyberArk Server, including username, password, and unique reference ID.
2. Universal Discovery administrators to create a credential on UCMDB Server, using the same CyberArk Safe, Application, and Account values created in step 1 as reference ID in the following format: **<Safe_Name>\<Folder_Path>\<Reference_ID>**
3. The CyberArk integration synchronizes the CyberArk references to Data Flow Probes. No password information contained.
4. Universal Discovery administrators to run discovery jobs using the unique referenceID to retrieve username and password from CyberArk.

Supported Versions

Supported CyberArk Versions

This integration supports CyberArk's Digital Vault v7.x, v8.x, and v9.x.

Supported Probe Types

This integration supports probes on the Windows platform only.

Platform	Probe Mode	Supported?
Windows	Union	Yes
	Separate	Yes
Probes on Linux		No
Integration Services		No

Supported Protocols

The following table describes protocols supported by CyberArk integration from UCMDB UI or supported from JMX console.

Protocols Supported from UCMDB UI (with CyberArk-related fields available)	Protocols Supported from JMX (no UI fields)
<ul style="list-style-type: none"> • AS400 • AWS • CA CMDB • Generic DB • Generic • HPE SIM • HTTP • NetApp • NTCMD • Powershell • Remedy • SAP JMX • SAP • SNMP • SSH • Telnet • vCloud • VMware VIM • WMI 	<ul style="list-style-type: none"> • Asset Manager • CIM • Network Automation Java • JBOSS • LDAP • NNM • SANSscreen • ServiceNow • Siebel Gateway • TIBCO • UCS • WebLogic • WebSphere

- **Protocols Supported from UCMDB UI.** When CyberArk integration is enabled, two radio buttons (**Regular Credential** and **External Vault**) are enabled in the Protocol Parameters dialog box. The existing attributes **Username** and **Password** are grouped under the **Regular Credential** radio button, and two new attributes (**Type** and **Reference**) are grouped under the **External Vault** radio button. For details about the protocol attributes, see the section about the supported protocols in the *HPE UCMDB Discovery and Integrations Content Guide - Supported Content*.
- **Protocols Supported from JMX.** There are no CyberArk related fields in the Protocol Parameter dialog box when the CyberArk integration is enabled, but you can run add CyberArk credential reference to these protocols with the help of JMX methods. For details, see ["How to Add CyberArk Credential for Protocols from JMX" on page 407](#).

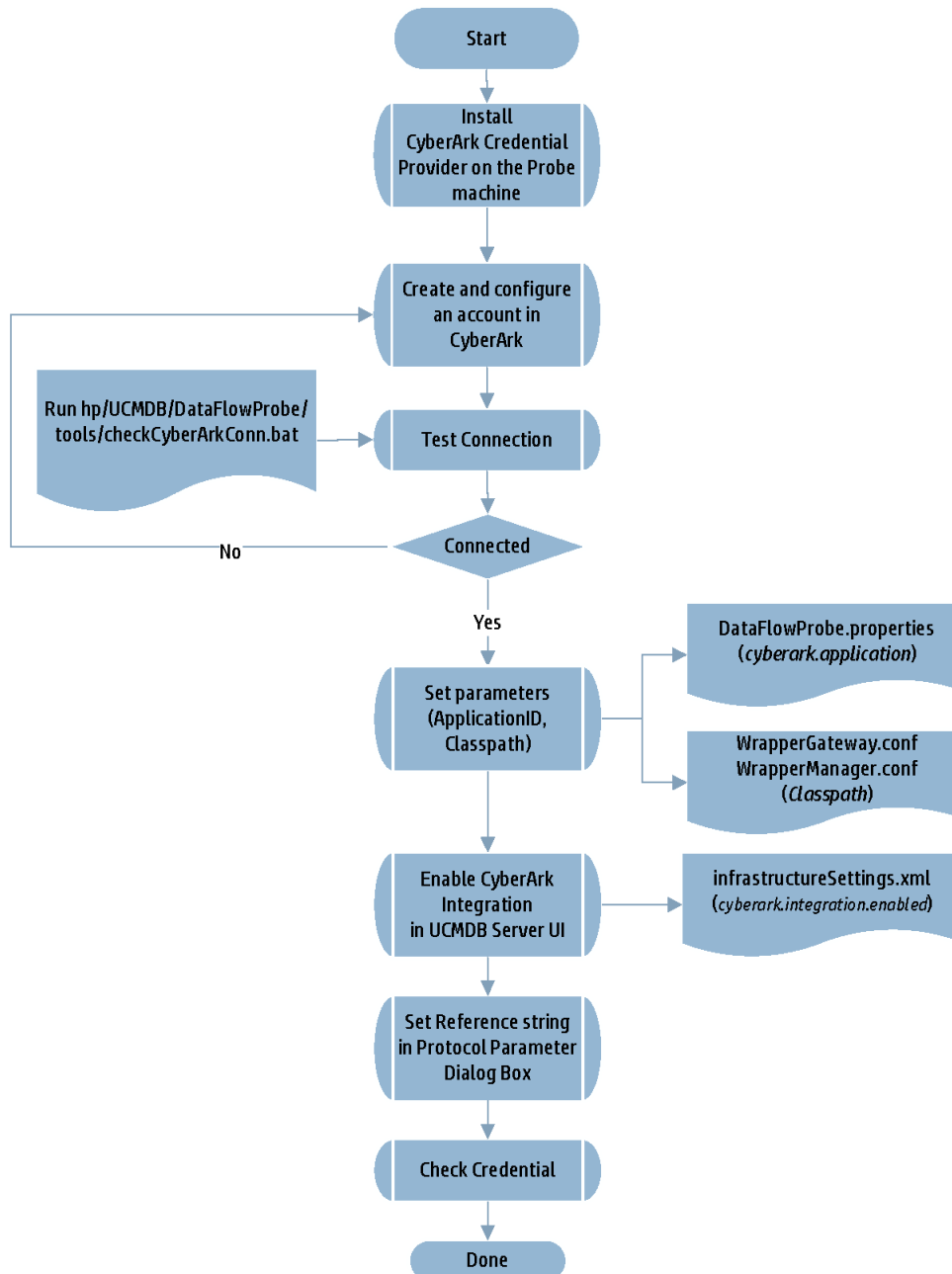
How to Configure CyberArk Integration

This section includes:

CyberArk Integration Configuration Workflow	391
How to Configure CyberArk Integration	392
How to Create and Configure CyberArk Account for the Integration	399
How to Add CyberArk Credential for Protocols from JMX	407
How to Calculate Hash Code for JARs with Annotation	408
How to Set a Default List of CyberArk Properties Using JMX	409

CyberArk Integration Configuration Workflow

The diagram below illustrates the overall workflow for configuring CyberArk integration.



How to Configure CyberArk Integration

This section contains detailed instructions about how to configure the CyberArk integration.

Note: Make sure that only administrators have the write permission to the **<DataFlowProbe_Home>** directory.

1. Install CyberArk Credential Provider

Install CyberArk Credential Provider (in AIM mode) on each of the supported Probe servers. For detailed instructions about how to install CyberArk Credential Provider, refer to the *Credential Provider and ASCP Implementation Guide*.

Note: If the Probe is Manager, install the CyberArk Credential Provider on the Probe Manager.

For a Probe in separate mode, install the CyberArk Credential Provider together with the Probe Manager.

For detailed instructions, refer to the CyberArk *Credential Provider and ASCP Implementation Guide*.

2. Configure CyberArk for the integration

Create a Safe, a CyberArk account, and an application ID in CyberArk, and configure CyberArk for the integration.

For detailed instructions, see ["How to Create and Configure CyberArk Account for the Integration" on page 399](#).

3. Test connection

Go to the Probe server, run the **checkCyberArkConn.bat** tool using the following command:

```
<DataFlowProbe_Home>\tools\checkCyberArkConn.bat "<SDK_Path>" <Safe_Name>  
<Folder_Path> HPE_UniversalDiscovery <ReferenceID>
```

where,

<SDK_Path> is the path of the CyberArk Java Password SDK.

<Safe_Name> is the name of the CyberArk Safe you created in [step 2](#).

<Folder_Path> is the folder for CyberArk Safe. If not specified, it is **Root** by default.

HPE_UniversalDiscovery is the CyberArk application ID you created in [step 2](#).

<ReferenceID> is the name of the CyberArk account you specified or auto-generated in CyberArk. It can be found in the properties of the account you created in [step 2](#).

For example,

```
C:\hp\UCMDB\DataFlowProbe\tools\checkCyberArkConn.bat "C:\Program Files
(x86)\CyberArk\ApplicationPasswordSdk\JavaPasswordSDK.jar" NancySafe Root
HPE_UniversalDiscovery nancy-cyberark-testing-refid
```

```
c:\hp\UCMDB\DataFlowProbe\tools>checkCyberArkConn.bat "C:\Program Files (x86)\CyberArk\ApplicationPasswordSdk\JavaPasswordSDK.jar" NancySafe Root HPE_UniversalDiscovery nancy-cyberark-testing-refid
Mon 05/28/2016 11:27:15.17
Checking CyberArk connection.....
Connecting the password vault...
UserName is : Nancy
Password is : *****
Address is : 16.187.187.187
PolicyID is : WinDomain
Connection can be established successfully.
```

4. Set ApplicationID and Classpath parameters manually

Set the following parameters manually on the Probe server:

- Set **ApplicationID** in the probe configuration file **DataFlowProbe.properties**.

Note: Skip this step if you already completed [step 2](#).

- Open the probe configuration file **hp\UCMDB\DataFlowProbe\conf\DataFlowProbe.properties** using a text editor.
- Locate the following line and set the application ID:

```
cyberark.application=HPE_UniversalDiscovery
```

Note: If the line does not exist, manually add the line at the end of the file.

- Set **Classpath** in the wrapper configuration files.
 - Open the **WrapperGateway.conf** or **WrapperManager.conf** file in a text editor.
 - If the current probe is in **union** mode, open the **WrapperGateway.conf** file;
 - If the current probe is in **separate** mode (gateway and manager), open the **WrapperManager.conf** file on the manager.

- ii. Locate the following line:

```
wrapper.java.classpath.8=<CyberArk_Install_
Dir>\ApplicationPasswordSdk\JavaPasswordSDK.jar
```

Note: If the above line does not exist, add it manually after the following line:

```
wrapper.java.classpath.7=%COMMON_CLASSPATH%
```

- iii. Set **Classpath**.


For example, set classpath in the **WrapperGateway.conf** file as follows:

```
wrapper.java.classpath.7=%COMMON_CLASSPATH%
wrapper.java.classpath.8=C:\Program Files
(x86)\CyberArk\ApplicationPasswordSdk\JavaPasswordSDK.jar
```

- iv. Save the file.
v. Restart the probe.

5. (SSH and Telnet protocols only) Add SU parameters manually to update class model

Note: This step is required only when your Content Pack version is on CP18 or CP19. If you are on CP20 or CP21, simply ignore this step.

- a. Locate the **SSH** or **Telnet** CI type. Go to **Modeling > CI Type Manager**, in the CI Types pane, expand **Root > Data > Object > Configuration > protocol > SSH/Telnet**.
- b. On the **Attributes** tab, click **Add**  to add two super user attributes to the SSH/Telnet protocol as follows:

	Attribute 1	Attribute 2
Attribute Name	su_external_vault_type	su_external_password_static_key
Display Name	External Vault Type for SU	External Password Static Key for SU
Description	External AAPM tool used for authentication for SU	Reference ID/string used in AAPM for SU
Attribute Type	string	string
Value Size	50	1024


- c. Click **OK**.
-
6. (VMware VIM protocol only) Download and copy VIM jar files
 - a. Download [CMS_vim.zip](#).
 - b. Extract the zip package and copy the two VIM jar files into the following location:
<DataFlowProbe_install_dir>\runtime\probeManager\discoveryResources\vmware
 - c. Copy the **JavaPasswordSDK.jar** file from the **C:\Program Files (x86)\CyberArk\ApplicationPasswordSdk** folder to the **<DataFlowProbe_install_dir>\lib** folder.
 - d. Locate the **basic_discovery_minimal_classpath** setting in the **DataFlowProbe.properties** file, and update its value by appending the following:

```
;../lib/JavaPasswordSDK.jar
```
 - e. Restart the Probe service and check the Probe status is "Connected".

7. Enable CyberArk integration on UCMDDB server

You can enable CyberArk integration using either of the following:

- o Change the **Enable CyberArk integration** infrastructure setting value from **false** to **true**.
 - i. In UCMDDB, go to **Administration > Infrastructure Setting Manager**.
 - ii. Locate the **Enable CyberArk integration** infrastructure setting and change its value from **false** to **true**.

The default value for the setting is false.
 - iii. Click **Save** .


The setting is synchronized to all probes.
- o Enable CyberArk integration from JMX console.
 - i. On the UCMDDB Server, go to **JMX console > UCMDDB:service=Settings Services**.
 - ii. Locate and invoke the **setGlobalSettingValue** JMX method with the following parameters:
 - **name:** cyberark.integration.enabled
 - **value:** true

8. Set CyberArk Reference String in the protocol credential UI for supported protocols

To do so,


- a. In UCMDB UI, go to **Data Flow Management > Data Flow Probe Setup**.
- b. In the Domains and Probes tree, expand **DefaultDomain(Default) > Credentials**, select a supported protocol.

In this example, select **AS400 Protocol**.

- c. In the AS400 Protocol pane, click .
- d. In the AS400 Protocol Parameters dialog box, provide values as necessary.

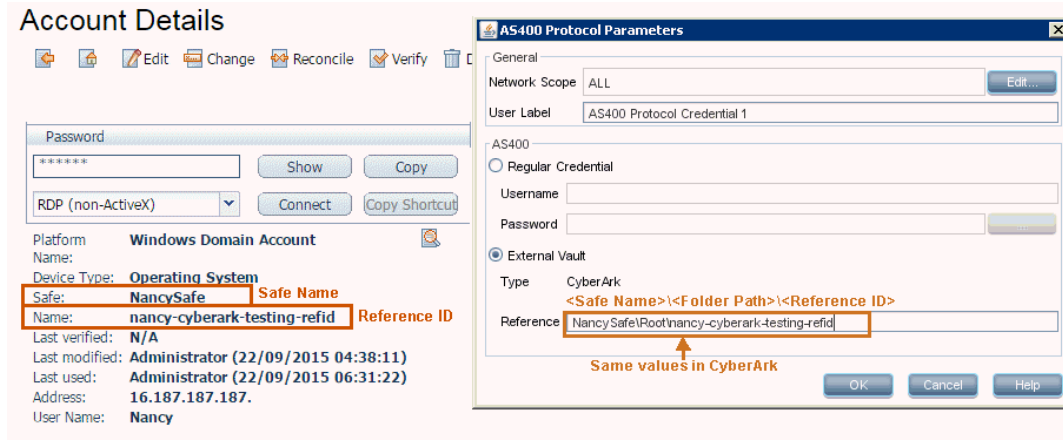
When CyberArk integration is enabled, two radio buttons (**Regular Credential** and **External Vault**) are enabled in the Protocol Parameters dialog. The existing **Username** and **Password** parameters are grouped under the **Regular Credential** radio button, and CyberArk integration specific parameters **Type** and **Reference** are enabled and grouped under the **External Vault** radio button, as described in the table below.

Parameter	Description
Regular Credential	<p>Select this radio button if you prefer to use regular credential as before.</p> <ul style="list-style-type: none"> • Username. See description for the protocol in the <i>HPE UCMDB Discovery and Integrations Content Guide - Supported Content</i>. • Password. See description for the protocol in the <i>HPE UCMDB Discovery and Integrations Content Guide - Supported Content</i>.

Parameter	Description
External Vault	<p>Select this radio button if you prefer to use an external credential vault.</p> <ul style="list-style-type: none"> • Type. The external vault type. Currently only CyberArk is supported. • Reference. Click  to open the Configure dialog box. <ul style="list-style-type: none"> • Reference. Select this option to configure the reference ID that will be used by UCMDDB/UD to retrieve the passwords from the CyberArk Enterprise Password Vault when they are needed. <p>Set the reference ID in the CyberArk Enterprise Password Vault in the following format: <Safe Name>\<Folder Path>\<Reference ID>.</p> <p>Where <Safe Name> is the Safe value in CyberArk, <Folder Path> is the folder where the Safe belongs to, and <Reference ID> is the name of the CyberArk account you specified or auto-generated in CyberArk.</p> <p>For example, NancySafe\Root\nancy-cyberark-testing-refid.</p> • Parameter. Select this option to configure a list of editable CyberArk properties as a query string for UCMDDB/UD to retrieve passwords from the CyberArk Enterprise Password Vault. <p>To configure a CyberArk property value, click in the Value column for the property, and specify the value in string.</p> <p>Note: The CyberArk properties values must not contain any of the following characters: \ / : * ? " < > ' . ;</p> <p>The out-of-the-box list of CyberArk properties displayed in the Configure dialog box is editable. You can set selected CyberArk properties as the default list using JMX method setGlobalSettingVaule. For instructions, see "How to Set a Default List of CyberArk Properties Using JMX".</p> <ul style="list-style-type: none"> • Regex. Enables configuring CyberArk properties values in regular expressions. <p>For examples of how to use regular expression syntax, see "Examples of Regular Expressions" in the <i>Universal CMDB Modeling Guide</i>.</p> <p>Note: The CyberArk properties values in regular expressions must not contain any of the following characters: : ;</p>

In this case, select **External Vault** and set the **Reference** value as described in the table above.

The following screenshots illustrate the exact CyberArk values you should use in setting the reference string:



e. Click **OK**.

9. Check credential

To do so,

- a. In UCMDB UI, go to **Data Flow Management > Data Flow Probe Setup**.
- b. In the Domains and Probes tree, expand **DefaultDomain(Default) > Credentials**, select a supported protocol.

In this example, select **AS400 Protocol**.

- c. Right-click an AS400 protocol in the protocols list, and select **Check credential** from the context menu.
- d. In the Check Credential dialog, provide the values as described below:
 - **IP/Hostname:** Enter the IP address or hostname of the Probe server.
 - **Timeout:** Keep the default value.
 - **Data Flow Probe:** Select **DataFlowProbe**.
- e. Click **OK**.

A "Connection successful" message is returned.

If CyberArk integration is not enabled, this action returns the following warning message:
CyberArk is disabled.

How to Create and Configure CyberArk Account for the Integration

To successfully integrate UCMDB/UD with CyberArk, follow the instructions below strictly to create and configure a safe, an account, and an application ID in CyberArk for the integration.

1. Sign in to CyberArk Password Vault

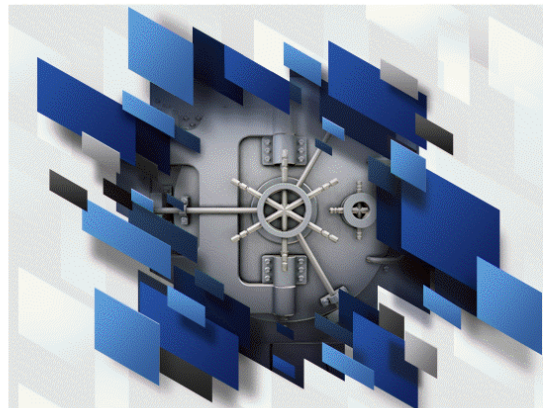
- a. In your Web browser, enter **http://<IP address of CyberArk Password Vault Web Access machine>/PasswordVault**.



- b. Select **CyberArk** as the authentication method.



Privileged Account Security



SIGN IN

Specify your authentication details

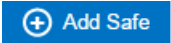
Sign in

Copyright © 1999-2014 Cyber-Ark Software Ltd. All Rights Reserved.
Version 8.6.0 (8.60.0.147) [About](#) | [Mobile version](#)

- c. Provide your user name and password, and click **Sign in**.

2. Create and configure a Safe

To do so,

- a. Go to the **POLICIES** tab and create a safe.
 - i. On the **POLICIES** tab, from the navigation pane select **Access Control (Safes)**, and then click **Add Safe** .

- ii. On the Add Safe page, provide values as described below:
 - **Safe name:** Provide a Safe name. For example, **NancySafe**.
 - **Description:** Provide a description for the Safe name.
 - **Saved Passwords:** Keep the default **Save password versions from the last [7] days** option selected.
 - **Assigned to CPM:** Keep the default **PasswordManager** option selected.

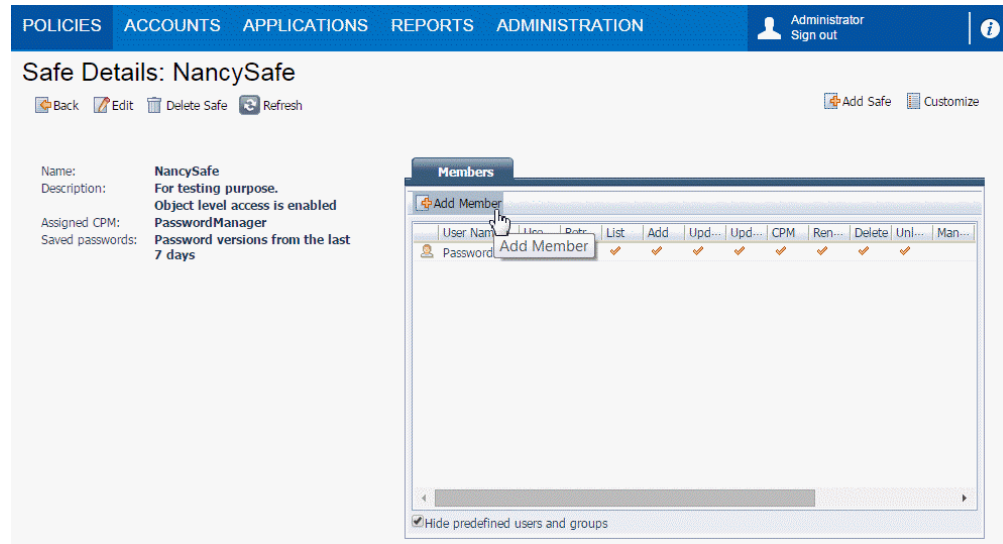
The screenshot shows the 'Add Safe' configuration page. At the top, there is a blue navigation bar with the following tabs: POLICIES, ACCOUNTS, APPLICATIONS, REPORTS, and ADMINISTRATION. Below the navigation bar, the page title is 'Add Safe'. The form contains the following fields and options:

- Safe name:** A text input field containing 'NancySafe'.
- Description:** A text input field containing 'For testing purpose.'.
- Enable Object Level Access Control:** An unchecked checkbox.
- Saved passwords:** Two radio button options:
 - Save the last password versions (unselected)
 - Save password versions from the last days (selected)
- Assigned to CPM:** A dropdown menu showing 'PasswordManager'.

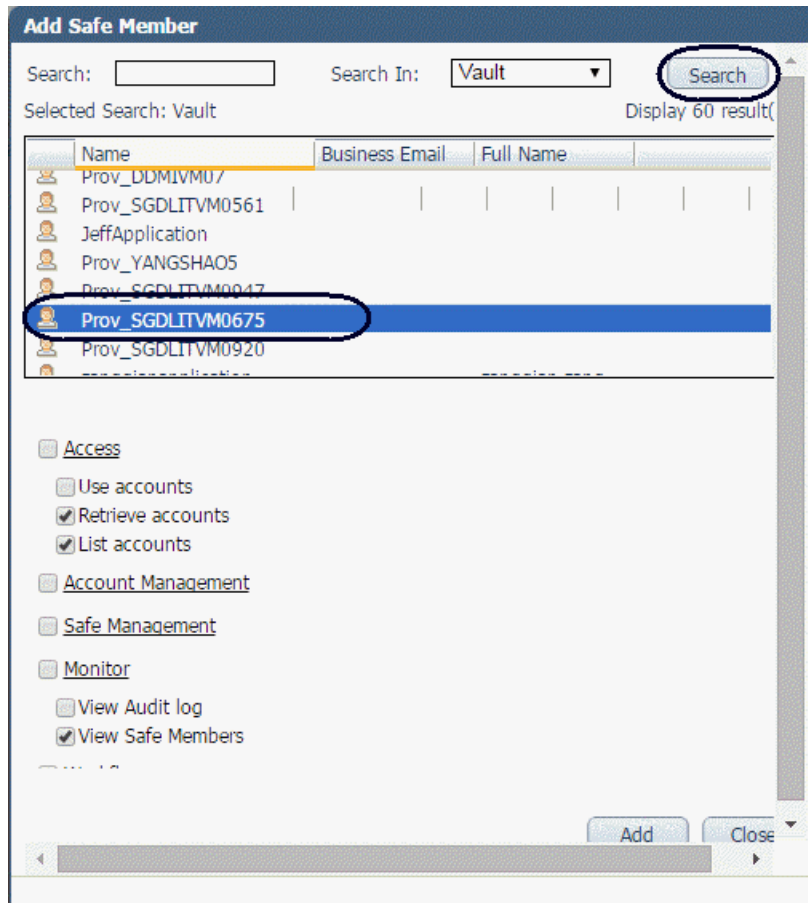
At the bottom of the form, there are two buttons: 'Save' and 'Cancel'.

- iii. Click **Save**
- b. Add the new Safe to the Safe Members list.

- i. On the Safe Details: <Safe Name> page, click **Add Member**.



- ii. In the **Add Safe Member** dialog, click **Search**, and then from the returned list select the desired Credential Provider Username (usually **Prov_<server>**).



Note: The credential provider user only needs the following permissions:

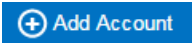
- Retrieve accounts
- List accounts
- View Safe Members

iii. Click **Add**.

iv. Click **Close**.

The Credential provider username you just added should now display in the Members list.

3. Create and configure an account

- a. Go to the **ACCOUNTS** tab, click **Add Account** .
- b. On the Add Account page, provide values as described below:

- **Store in Safe:** Select the Safe name you just created in [step 2](#).
- **Device Type:** Select **Operating System** from the drop-down list.

Note: The required properties and optional properties may vary with the device type you select. In this document, **Operating System** and Windows Domain Account are selected for **Device Type** and **Platform Name** respectively as an example. For details about other properties, refer to the CyberArk *Credential Provider and ASCP Implementation Guide*.

- **Platform Name:** Select a platform name value from the drop-down list. In this example, **Windows Domain Account** is selected.
- **Address:** (Optional) Enter the IP address of the target server that you want to discover.
- **User Name:** Specify the user name for the account you configure in CyberArk. This is the account used by the UCMDB Server to connect to the target server that you want to discover.
- **Password:** Enter the password for the account you configure in CyberArk.
- **Confirm Password:** Enter your password again.
- **Name:** Select an **Auto-generated** or **Custom** name for your Safe account.


If you select **Custom**, provide a custom account name. For example, **nancy-cyberark-testing-refid**.

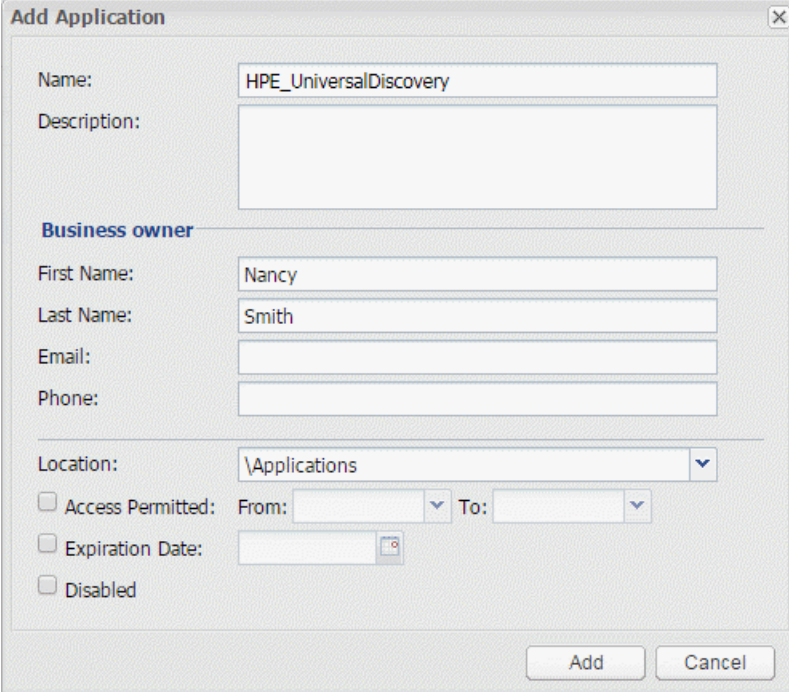
For example,

The screenshot shows the 'Add Account' form in the CyberArk interface. The form is titled 'Add Account' and is part of a navigation menu with tabs for POLICIES, ACCOUNTS, APPLICATIONS, REPORTS, and ADMINISTRATION. The user is logged in as Administrator. The form fields are: Store in Safe (NancySafe), Device Type (Operating System), Platform Name (Windows Domain Account), Address (16.187.187.187), User Name (Nancy), Password (masked), Confirm Password (masked), and Name (Custom: nancy-cyberark-testing-refid). There are also checkboxes for 'Optional Properties' (Logon To, User DN, Port) and 'Disable automatic management for this account'.

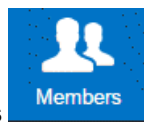
- c. Click **Save**.

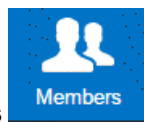
4. Create and configure an application ID



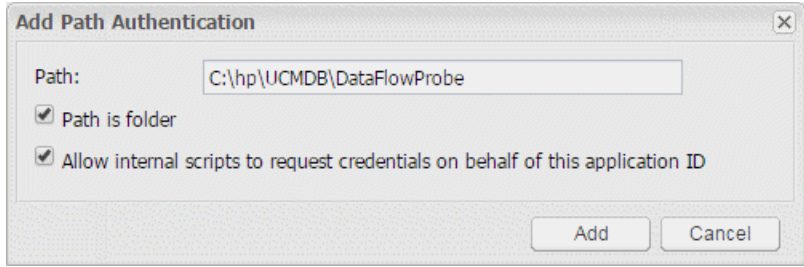

- a. Go to the **APPLICATIONS** tab and create an application ID.
 - i. On the **APPLICATIONS** tab, click  **Add Application**.
 - ii. In the Add Application dialog, provide values as described below:
 - **Name:** Specify **HPE_UniversalDiscovery** as the application ID for UCMDB.
 - **Description:** Provide a description for the application ID.
 - **Location:** Select **\Applications**.
 - **Other fields:** Provide values as necessary.

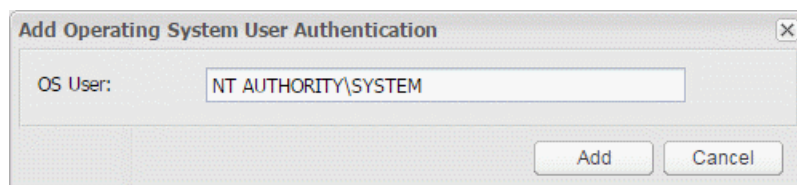


- iii. Click **Add**.
 - b. Add the new application ID to the Safe members list.
 - i. Go to the **POLICIES** tab, from the navigation pane select **Access Control (Safes)**, and then select **NancySafe** from the Safe Name list.



- ii. Click **Members**  in the lower right corner of the page.
 - iii. On the **Safe Details: NancySafe** page, click **Add Member**.

- iv. In the **Add Safe Member** dialog, select **HPE_UniversalDiscovery**.
 - v. Click **Add**.
- c. Add the full name of the Credential Provider Servers to the **Allowed Machines** list.
- i. Go to the **APPLICATIONS** tab, select **HPE_UniversalDiscovery**.
 - ii. On the **Application Details: HPE_UniversalDiscovery** page, go to the **Allowed Machines** tab.
 - iii. Click **Add Machine** .
 - iv. In the **Add allowed machine** dialog, enter IP, host name, or DNS.
 - v. Click **Add**.
- d. Add path authentication for **HPE_UniversalDiscovery**.
- i. Go to the **Authentication** tab, click **Add authentication details** , and then select **Path**.
 - ii. In the **Add Path Authentication** dialog,
 - In the **Path** field, enter the path, for example, **C:\hp\UCMDB\DataFlowProbe**.
 - Make sure you select the check box for both of the following options:
 - **Path is folder**
 - **Allow internal scripts to request credential on behalf of this application ID**.
- For example,
- 
- iii. Click **Add**.
- e. Add operating system user authentication for the new application ID.
- i. On the **Authentication** tab, click **Add authentication details** , and then select **OS user**.
 - ii. In the **Add Operating System User Authentication** dialog, provide OS user information, for example, **NT AUTHORITY\SYSTEM**.

**Note:**

- If the Probe is running as a service, specify **NT AUTHORITY\SYSTEM** as OS user.
- If the Probe is running as console, specify **<hostname\username>** as OS User. For example, **HPSWVM0999\Administrator**.

iii. Click **Add**.

How to Add CyberArk Credential for Protocols from JMX

For the protocols that do not have the CyberArk related fields available after you enable CyberArk integration from the UCMDB Server, you can add CyberArk credential for these protocols with the help of JMX methods.

To do so,

1. Export the existing credential

- a. 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.
- b. Click **UCMDB:service=DiscoveryManager** to open the JMX MBEAN View page.
- c. Locate the **exportCredentialsAndRangesInformation** operation. Do the following:
 - Enter your customer ID (the default is 1).
 - Enter a name for the exported file.
 - Leave the password field empty.
 - Set **isEncrypted=False** since we want to edit the exported file and import it back later.
 - Set **includeProbeRange=True**
- d. Click **Invoke** to export.

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

2. Add CyberArk credential to the exported file

- a. Navigate to the **C:\hp\UCMDB\UCMDBServer\conf\discovery\ directory.**
- b. Open the exported file using a text editor.
- c. At the end of the file, before the last `</object>` tag, manually add the following:

```
<attribute name="external_vault_type"
type="string">CyberArk</attribute><attribute name="external_password_
static_key" type="string">HPSupportSafe\Root\support-cyberark-
refid</attribute></object>
```

- d. Save the file.

3. Import the updated credential file back to UCMDB
 - a. Go to the JMX Console.
 - b. Click **UCMDB:service=DiscoveryManager** to open the JMX MBEAN View page.
 - c. Locate the **importCredentialsAndRangesInformation** operation. Do the following:
 - Enter your customer ID (the default is 1).
 - Enter a name for the exported file.
 - Leave the password field empty.
 - Set **isEncrypted=False** since we want to edit the exported file and import it back later.
 - Set **includeProbeRange=True**.
 - Set **notAllowOverlap=False**.
 - d. Click **Invoke** to import.

How to Calculate Hash Code for JARs with Annotation

It is now possible to provide support for the application signature using the annotation in the CyberArk integration class.

To calculate the Hash Code for JARs with annotation,

1. Generate the application hash value by running the following command.

```
java -Xms500m -Xmx1200m -jar JavaAIMGetAppInfo.jar GetHash
/AppExecutablesPattern="C:\hp\UCMDB\DataFlowProbe\lib"
/ClassPath="C:\hp\UCMDB\DataFlowProbe\lib;C:\hp\UCMDB\DataFlowProbe\jython"
/OnlyExecutablesWithAIMAnnotation=yes /LogFileDirectory="c:\temp"
```

Note that the above command is an example, you might need to update it according to your environment, the installation location of the UCMDB Server, and so on.

2. Add the newly generated hash value to the application authentication.

How to Set a Default List of CyberArk Properties Using JMX

The enhanced CyberArk integration in version 10.30 allows you to configure selected CyberArk properties as a query string for UCMDB/UD to retrieve passwords from the CyberArk Enterprise Password Vault. The out-of-the-box list of CyberArk properties displayed in the Configure dialog box is editable, you can set selected CyberArk properties as the default list to display by using the new parameter **cyberark.parameter.list** of the **setGlobalSettingVaule** JMX method.

This task describes how to set a default list of CyberArk properties for the CyberArk integration using JMX console.

1. Access the UCMDB JMX console

Launch a Web browser and enter the following address: **https://<UCMDB machine name or IP address>:8443/jmx-console**. You may have to log in with a user name and password (default is sysadmin/sysadmin).

2. (Optional) Display the OOTB list of CyberArk properties

- a. Search and locate the **getSettingDefaultValue** operation in the **UCMDB:service=Settings Services** category.

- b. Invoke the **getSettingDefaultValue** operation using the following parameter values:

- **customerId:** 1
- **name:** cyberark.parameter.list

3. Set the default list of CyberArk properties

- a. Search and locate the **setGlobalSettingValue** operation in the **UCMDB:service=Settings Services** category.

- b. Invoke the **setGlobalSettingValue** operation using the following parameter values:

- **name:** cyberark.parameter.list
- **value:** Specify a list of CyberArk properties, separated by comma, for example, **Folder,Port,Domain**.

setGlobalSettingValue*Set global setting value*

Name	Type	Value	Description
name	java.lang.String	cyberark.parameter.list	Setting Name
value	java.lang.String	Folder,Port,Domain <input type="button" value="x"/>	Setting Value

The change takes effective right away, and the OOTB list of CyberArk properties is overridden with this new list.

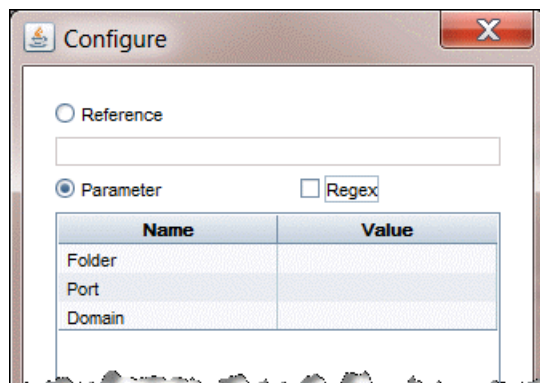
4. Check the CyberArk properties list in the Configure dialog box

If the Configure dialog box is already open, simply close it and open it again by clicking **Configure**

in the Protocol Parameters dialog box. Otherwise, follow the instructions below.

- a. In UCMDB UI, go to **Data Flow Management > Data Flow Probe Setup > Domains and Probes > DefaultDomain(Default) > Credentials**.
- b. Select a CyberArk integration enabled protocol, and open the Protocol Parameters dialog box.
- c. Select **External Vault**, and then click **Configure** .

The Configure dialog box now lists three CyberArk properties only.



CyberArk Integration Troubleshooting and Limitations

- **Symptom:** Received an error message "User <ApplicationID> is not defined" when running the `checkCyberArkConn.bat` script to test connection.

Possible Cause: The application ID is not added to the Safe in CyberArk.

Solution: Add the application ID to the Safe in CyberArk. For detailed instructions, see [Create and configure an application ID](#).

- **Symptom:** Checking credential failed with an error message similar to the following:

Failed to get credential XYZ, please check the related error logs in probe side.

Scenarios:

- Found the following error messages in the **WrapperProbeGw.log**:
 - ... Failed to get credential for id 52_1_CMS - Failed querying CyberArk Password, Application ID is empty.
 - ...Failed to get credential for id 2_1_CMS - Failed querying attribute from CyberArk Password.

Possible Cause: Application ID or Classpath is not properly set.

Solution: Set application ID and classpath properly. For detailed instructions, see [Set ApplicationID and Classpath parameters manually](#).

- Found the following error message in the **WrapperProbeGw.log**: Query string not legal. Should be "safe\folder\name".

Possible Cause: The format of the Reference ID is not correct.

Solution: Update the reference ID by strictly following the reference ID format:

<Safe_Name>\<Folder Path>\<ReferenceID>

Where **<Safe_Name>** is the Safe value in CyberArk, **<Folder Path>** is the folder where the Safe belongs to, and **<ReferenceID>** is the name of the CyberArk account you specified or auto-generated in CyberArk.

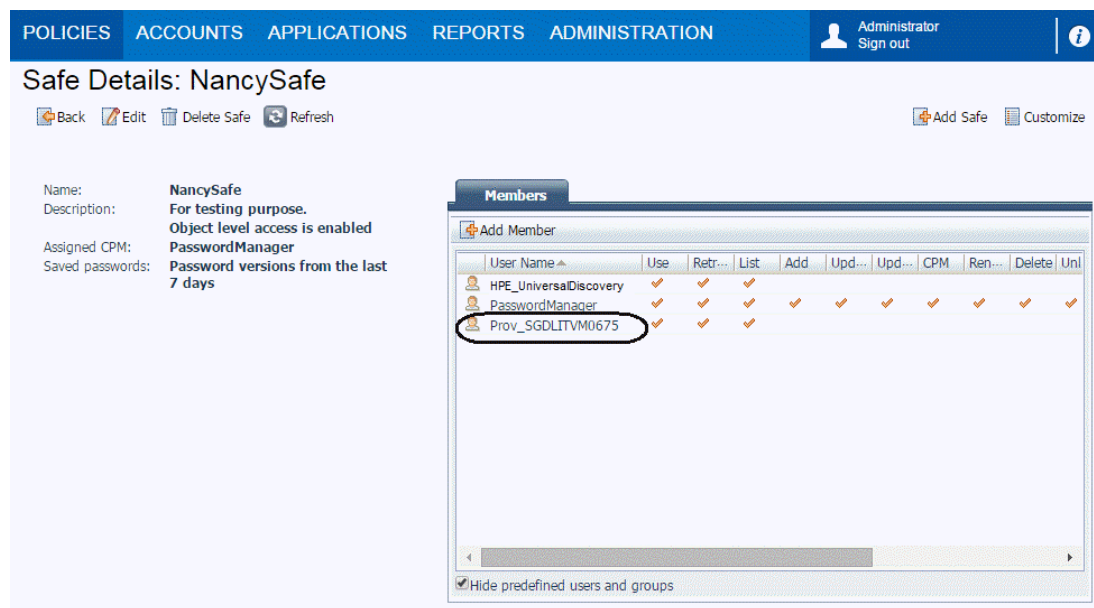
For example, **NancySafe\Root\nancy-cyberark-testing-refid**.

- Found the following error message in the **WrapperProbeGw.log**:

Password object matching query [object=ABC;Folder=Root;Safe=XYZ] was not found (Diagnostic Info: 9). Please check that there is a password object that answers your query in the vault and that both the provider and the application user have the appropriate permissions needed in order to use the password.

Possible Cause: The CyberArk Credential Provider user was not added as a member to the Safe.

Solution: Add the CyberArk Credential Provider user as a member to the Safe in CyberArk, as follows:



For detailed instructions, see ["How to Create and Configure CyberArk Account for the Integration"](#) on page 399.

- Found the following error message in the **WrapperProbeGw.log**: Error: CASVL012E User Name [ApplicationID] is invalid.

Possible Cause: This is related to the authentication. The OS user was not properly set when creating the Application ID in CyberArk.

Solution: If the Probe is running as a service, add **NT AUTHORITY\SYSTEM** as OS user.

If the Probe is running as console, add the **<hostname\username>** as OS User.

- **PROBLEM:** After enabling CyberArk integration, there are no CyberArk related fields in the Protocol Parameters dialog for some protocols. Is it possible to add CyberArk credential reference to those protocols?

Solution: Yes. Apart from UDDI Registry and Universal Discovery protocols (which have no passwords at all), we can add CyberArk credential reference to these protocols with the help of JMX methods. For a list of protocols that are supported from JMX, see ["Supported Protocols" on page 389](#). For detailed instructions, see ["How to Add CyberArk Credential for Protocols from JMX" on page 407](#).

- **Limitation:** Probe will not be able to retrieve passwords from CyberArk if it is running on the local system account and that this account is not added as a member to the CyberArk Safe.
- **PROBLEM:** After enabling CyberArk integration and the FIPS mode, check credential for CyberArk failed on Windows platform. This is because the file path separator "\" in the conf files cannot be properly processed on Windows platform. (QCCR1H104637)

Solution: When enabling CyberArk integration and the FIPS mode on Windows platforms, make sure you replace the file path separator "\" with "/" in the conf files.

For example, replace the file path separator "\" in the following setting:

```
wrapper.java.classpath.8=C:\Program Files
(x86)\CyberArkApplication\PasswordSdk\JavaPasswordSDK.jar
```

with "/", as shown below:

```
wrapper.java.classpath.8=C:/Program Files
(x86)/CyberArkApplication/PasswordSdk/JavaPasswordSDK.jar
```

- **PROBLEM:** After adding a new probe to the UCMDB server that was already switched to the FIPS mode, the automatic FIPS switch process for the new probe might fail. This is because once the newly installed probe is started, it downloads all the resources from the UCMDB server, and when the probe gets the probe upgrade package, it would schedule a restart, which blocks the automatic FIPS Switch process. (QCCR1H106595)

Workaround: Once you find that the automatic FIPS Switch process for a new probe failed,

- a. Copy the jar files of JCE Unlimited Strength Jurisdiction Policy Files 8 into the `%DataFlowProbe_HOME%\bin\jre\lib\security` directory on the Data Flow Probe machine.

For more information about how to obtain the files, see the *Universal CMDB FIPS Deployment Guide*.

- b. Add the following line into the `DataFlowProbe.properties` file on the Data Flow Probe machine, and then save the file.

```
probe.fips.status=1
```

- c. Restart the Data Flow Probe.

Note: If the Data Flow Probe is in separate mode, you need to perform the above steps for both the Probe Manager and Probe Gateway instances.

- **PROBLEM:** When running discovery jobs or checking credentials, the following error occurs:

```
Failed to verify application authentication data: Hash XXX is unauthorized.
```



```
at com.hp.ucmdb.discovery.probe.tools.CyberArkVaultTool.main(CyberArkVaultTool.java:113)
Caused by: class javapasswordsdk.exceptions.PSDKException: APPAPI33E Failed to verify application authentication data: Hash "39D6CB2233F6853FE78816EF4A245597561722F" is unauthorized
at javapasswordsdk.passwordsdk.getPassword(passwordsdk.java:57)
at sun.reflect.NativeMethodAccessorImpl.invoke0(Native Method)
at sun.reflect.NativeMethodAccessorImpl.invoke(NativeMethodAccessorImpl.java:62)
```

This is caused by inconsistent hash values between UCMDB and CyberArk Server.

Workaround: Check if the hash value is the same as the one you configured on the CyberArk server. If different, regenerate the hash value and then fill the new hash value in the CyberArk server. For instructions, see ["How to Calculate Hash Code for JARs with Annotation" on page 408](#).

Part V: Universal Discovery

Chapter 12: Introduction to Universal Discovery

This chapter includes:

Universal Discovery Overview	416
Universal Discovery Community	416
Agent-based vs. Agentless Discovery Overview	417
Script-based vs Scanner-based Discovery	417

Universal Discovery Overview

Universal Discovery enables you to discover components that make up your system. You can discover zones in your environment by running discovery activities in those zones. Alternatively, you can set up and run individual discovery jobs on any node in your environment.

For more information, see:

- ["Zone-based Discovery" on page 420](#)
- ["Module/Job-based Discovery" on page 466](#)
- ["Just-In-Time Discovery" on page 655](#)
- ["Inventory Discovery" on page 505](#)

Universal Discovery Community

The [Universal Discovery Community](https://marketplace.microfocus.com/itom/content/ud-content-packs) (<https://marketplace.microfocus.com/itom/content/ud-content-packs>) on the ITOM Marketplace provides customers with a convenient way to obtain the latest UCMDB Discovery and Integrations Content Packs and related documentation.

Agent-based vs. Agentless Discovery Overview

Agent-based Discovery

To collect inventory information, you can deploy Universal Discovery agents on client or server machines. The UD agent provides a secured communication channel between the Data Flow Probe and the Nodes being discovered. After setting up the secure communication channel, Universal Discovery deploys and activates scanners onto the Nodes being discovered. The Scanners scan the Nodes for inventory information and store the scanned results in scan files which are downloaded to the Data Flow Probe through the secured communication channel established with the UD agent.

When the UD agent is installed, collection of software utilization information is enabled. The UD Agent also enables you to benefit from the Call Home feature. Call Home is useful in the case where a Node was unavailable for scanning for a long period. It enables the UD agent to notify the Data Flow Probe that the Node is currently available for scanning.

Agentless Discovery

Although agentless discovery does not require the installation of dedicated agents on the servers that are to be discovered, it does depend on native OS or standard agents that are already installed such as SNMP, WMI, TELNET, SSH, NETBIOS, and others. Other discovery capabilities are based on application-specific protocols such as SQL, JMX, SAP, Siebel, and so on. For more information, see "Supported Protocols" in the *HPE UCMDB Discovery and Integrations Content Guide - Supported Content*.

Script-based vs Scanner-based Discovery

Universal Discovery performs inventory discovery using the following discovery methods.

Note:

- Selecting a discovery method depends on your organization's policy and business goals.
- More than one discovery method can be used.

Script-based discovery

This type of discovery was originally implemented in DDMA.

Script-based discovery is often called "agentless" because it is typically implemented without agents installed on remote nodes. However, it is possible to run these jobs with a Universal Discovery Agent installed.

This type of discovery is best suited for organizations where deployment effort must be minimal, footprints on remote nodes are a primary concern, and information about running software is critical.

Scanner-based discovery

This type of discovery was originally implemented in DDML.

Scanner-based discovery uses a software component called the Scanner- an executable file that runs on the remote node. The Scanner is deployed to remote machines and runs according to a schedule that you configure. It can run automatically using Activities, or run manually.

Scanner-based discovery is best suited for organizations where a high degree of details about installed software and hardware is needed.

Script-based vs Scanner-based Discovery Comparative Matrix

Attribute/Discovery Method	Script	Scanner
Deployment Component	None	Executable file
Connection Method	Agent or Agentless	Agent or Agentless
Execution Methods	Automatic (Activities) or Manual	Automatic (Activities) or Manual
Discovery Method	APIs	Executable file (Scanner)
Scan Type	Specific data sets	Entire file system
Information Collected	Running software	Installed software, Hardware
Information Detail	Moderate	High
Performance Impact	None	Minimal

Attribute/Discovery Method	Script	Scanner
on Node		
Scalability	High. Discovery job quickly triggers subsequent jobs.	Minimal. Scanning job must wait to finish before triggering subsequent jobs.
Footprint on Node	None	Minimal

For details on Universal Discovery Agents, see ["Universal Discovery Agent Overview" on page 163](#).

For details on Scanners, see ["Inventory Discovery Scanners" on page 509](#).

Chapter 13: Zone-based Discovery

This chapter includes:

Zone-based Discovery Overview	420
Management Zone Ranking	421
Discovery Troubleshooter	424
Configure IP Ranges for Management Zones at Domain Level	425
How to Run Zone-based Discovery	428
How to Create Management Zones	429
How to Define Discovery Activities in a Management Zone	431
How to Create Discovery Activity Templates	431
How to Define Custom Discovery Activities from an Activity Template	432
How to Rank Management Zones	434
How to Configure Global Management Zone Settings	435
How to Organize the Management Zones Tree	436
How to Migrate Management Zone Folders	437
How to Migrate Management Zones	438
How to Rename Management Zones	439
How to Rename Activities	440
Zone-based Discovery User Interface	441

Zone-based Discovery Overview

Zone-based discovery enables you to:

- Limit the scope of a discovery activity to a sub-set (zone) of the entire network
- Run multiple instances of the same discovery activity on different zones in the network
- Configure each discovery activity instance with different settings (parameters, scheduling)
- Diagnose discovery problems (using the Discovery Troubleshooter)

Definitions

- **Management Zone.** A Management Zone is a region in the network defined by a collection of IP ranges. A region of an organization's infrastructure should be defined as a Management-Zone when you want to discover all the managed objects of the region using the same scheduling policy and parameters.
- **Discovery Activity.** You configure Discovery activities to perform discovery inside a specific Management Zone. The activities discover infrastructure (IPs, nodes), basic software (shallow running software including application servers, databases, and web servers), deep database configuration, and inventory (for example, CPUs, installed software, logical volumes), among other information. A Discovery activity includes:
 - Discovery parameters that are specific to the type of the Discovery activity
 - A scheduling policy

For more information on discovery activities and instructions on how to activate them, see the *Universal CMDB Discovery and Integrations Content Guide*.

Example: How to Define Management Zones

Organization-X has two data-centers: DC-A and DC-B. Each data center is owned/managed by a different administration group: Admin-Group-A and Admin-Group-B. Each administration group would like to run its own "instance" of a Discovery activity within its data center. On DC-A, you want to discover all machines operating on Windows once every week using the same discovery parameters. Therefore, DC-A should be defined as a Management Zone. On DC-B, you want to discover all the J2EE servers once every day using the same discovery parameters. DC-B should also be defined as a Management Zone.

For details on how to run zone-based discovery, see "[How to Run Zone-based Discovery](#)" on page 428.

For details on creating a Management Zone, see "[New/Edit Management Zone Dialog Box](#)" on page 446.

For details on the Discovery Troubleshooter, see "[Discovery Troubleshooter](#)" on page 424.

Management Zone Ranking

Management Zone ranking is used when a job's trigger belongs to more than one Management Zone. This could occur when Management Zone ranges overlap, or when a trigger has more than one related IP address and each of these IP addresses belongs to a different Management Zone.

In order to better handle discovery in Management Zones where, for example, overlaps occur, Management Zones can be ranked. When Management Zones are ranked, activities defined in the Management Zones with the highest rank are run in the overlapping IP ranges, while activities in the lower ranking Management Zones do not run in the overlapping IP ranges.

Note:

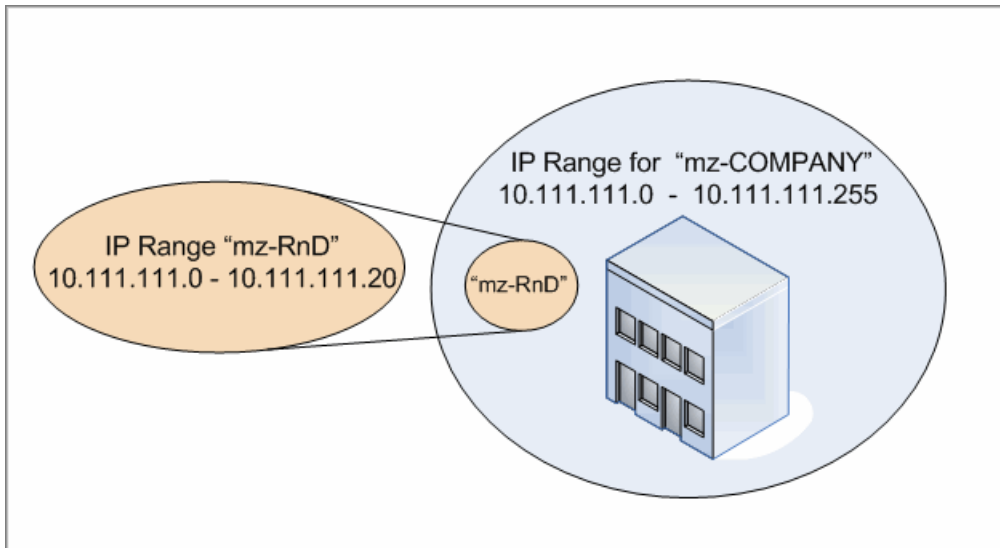
- Management Zones with a ranking of level 1 are the highest ranking Management Zones.
- (Version 10.30 or later) Management zone ranking does not work for management zones with partial overlapping ranges when the ranges of management zones are different from the domain range. For example, the domain range is 100.100.100.100-100.100.100.200, the range of MZ1 is defined as 100.100.100.100-100.100.100.150, and the range of MZ2 is defined as 100.100.100.130-100.100.100.160, then regular discovery jobs in the activities are running in both MZ1 and MZ2 on the overlapping range.

The following use-case scenarios demonstrate how ranking comes into play:

Scenario 1: Overlapping Management Zone Ranges

Say you define a large Management Zone, "mz-COMPANY," over IP range 10.111.111.0 - 10.111.111.255, covering all of the desktops in your company. You define an Inventory Discovery activity in mz-COMPANY to scan the desktops in the entire IP range for hardware and installed software.

In the R&D department of the company, discovery needs to be managed differently. Hardware discovery is of no interest to you in this range of IPs but you do want to scan the desktops in this department for installed software, as well as for software utilization. To do this, you define a smaller Management Zone, "mz-RnD", that covers the IP range of the R&D desktops only: 10.111.111.0 - 10.111.111.20. You define an Inventory Discovery activity to scan for installed software and for software utilization.



When you activate the activities in both Management Zones:

- the results for mz-COMPANY include data about hardware and installed software discovered on all desktops in mz-COMPANY's range
- the results for mz-RnD include data about installed software discovered on the desktops in mz-RnD's range, as well as information about software utilization

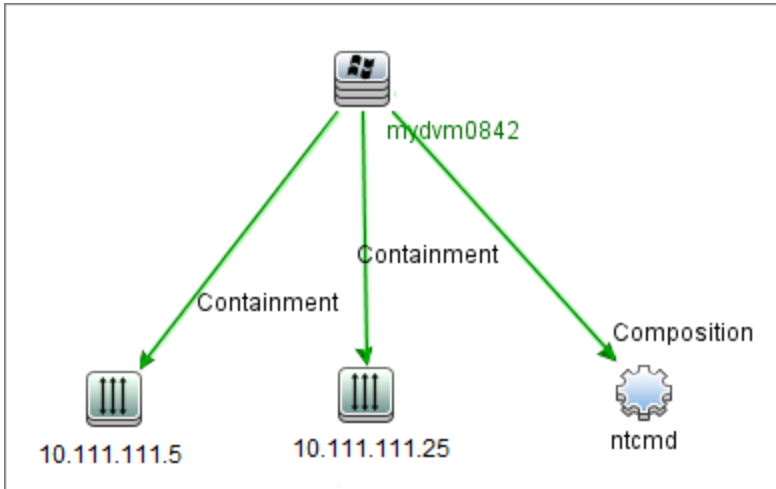
Notice how both sets of discovery results include information about the installed software on the desktops in the overlapping range 10.111.111.0 - 10.111.111.20.

Because mz-RnD requires a more specialized discovery, you can assign mz-RnD a ranking of 1, and lower the ranking of mz-COMPANY to 2. This way, because mz-RnD has a higher ranking than mz-COMPANY, only the discovery activities defined for mz-RnD will run in the overlapping IP range, 10.111.111.0 - 10.111.111.20. Discovery activities defined for mz-COMPANY will run in mz-COMPANY's remaining IP range—10.111.111.21 - 10.111.111.255.

Note: After deactivating a discovery activity in a higher ranking management zone, make sure you reset the ranking of management zones with overlapping IP ranges, otherwise jobs in the lower ranking management zones with overlapping IP ranges will not be triggered.

Scenario 2: Discovery Node has multiple IP Addresses in different Management Zones

Using the scenario above, say the desktop, Node **mydvm0842**, has multiple IP addresses, including 10.111.111.5 and 10.111.111.25. Note that both of these IP addresses belong to mz-COMPANY, but 10.111.111.5 belongs to mz-RnD as well.



Only one of these IP addresses is recorded in the Protocol CI in the Application IP attribute, which **mydvm0842** then uses for communicating with the Data Flow Probe and for determining which Management Zone **mydvm0842** will belong to.

If IP address 10.111.111.5 is selected, the activities from mz-RnD are used for discovery because mz-RnD has a higher ranking.

Note: In the case of multiple IP addresses on a node, the IP address selected for communication with the node is that which determines which Management Zone the discovery node will belong to. In the scenario above, if 10.111.111.25 is selected, even though the Management Zone it belongs to, mz-COMPANY, is lower ranking than mz-RnD, mz-COMPANY's activities will still run on the node, and may lead to unexpected discovery results. This is because the second IP address, 10.111.111.5, that was not selected for communicating with the node, is not taken into account for ranking purposes.

It is strongly recommended to define your Management Zones in such a way that if a discovery node has multiple IP addresses, all of the IP addresses are included in the same Management Zone. For details about defining Management Zones, see ["New/Edit Management Zone Dialog Box" on page 446](#).

Discovery Troubleshooter

It is possible that after running discovery, you will not find a particular CI in the discovery results. There are various types of errors that can occur that would cause this to happen. The Discovery Troubleshooter allows you to search for the missing CI, and even if you are unable to locate the missing

CI, the Discovery Troubleshooter also detects and lists errors that occurred during the discovery process. By attempting to solve these errors, this can lead you to the missing CI.

Currently the Discovery Troubleshooter allows you to locate missing Running Software CIs. When invoking the Discovery Troubleshooter, you are requested to enter the IP of the target host you are looking for and choose a detection method before searching for the missing running software CI. If the Discovery Troubleshooter does not initially succeed in connecting to the target host, it allows you to rerun discovery with a different detection method. If the Discovery Troubleshooter does succeed in connecting to the target host, it lists all the running software currently connected to the detected Node CI. If the CI you are looking for is not in the list, the Discovery Troubleshooter lets you update available application signatures, which may provide a more extensive list of all running software connected to the detected Node CI and enable you to find the missing CI.

Note: The Discovery Troubleshooter can be run on a Management Zone only after the Infrastructure and Basic Software Configuration discovery activities have been run on that Management Zone.

Configure IP Ranges for Management Zones at Domain Level

Starting from UCMDB version 10.30, it is possible to configure IP ranges for management zones at domain level, instead of Data Flow Probe/probe clusters level. This enables discovery administrators to define management zones with more flexibility to reflect business discovery strategy.

The enhancements implemented in UCMDB 10.30 include the following:

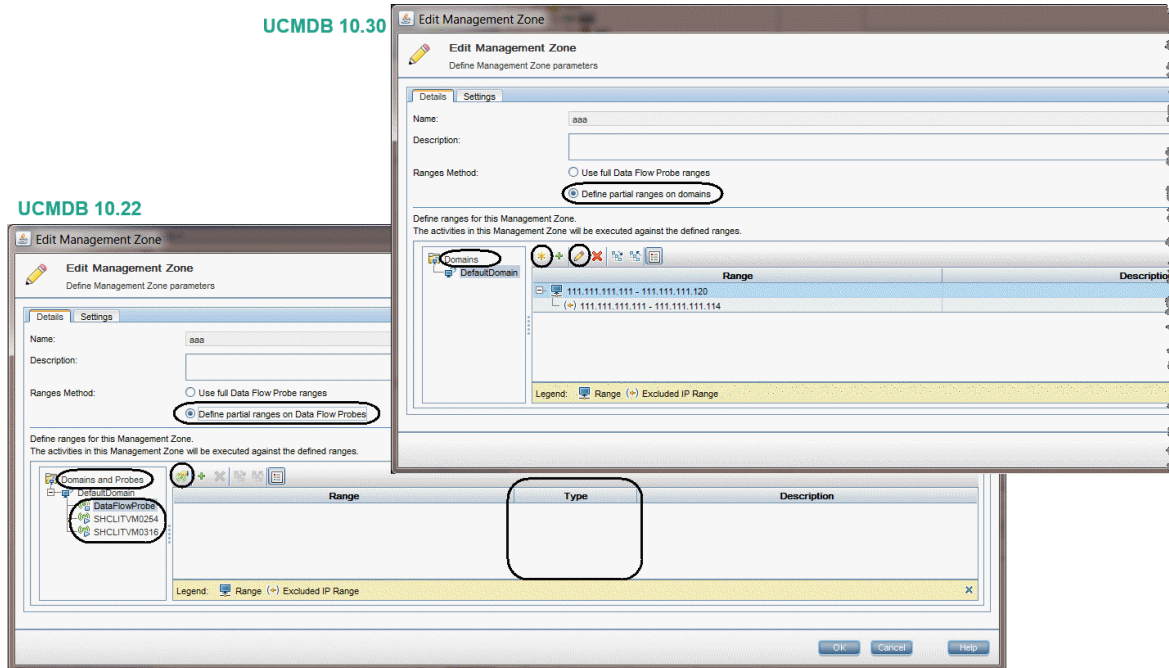
- Decoupled IP Range configuration from Data Flow Probe/probe clusters level for management zones
- Removed IP range type setting for management zones, and
- Allow binding of excluded IPs from one IP range to a different IP range as a sub-range at domain level



All this adds flexibility in managing IP ranges with management zones and eliminates the limitation of IP ranges bound to Data Flow Probe/probe clusters. Now you can perform the following on management zones easily:




- Configure independent IP ranges at domain level for management zones
- Bind IPs excluded from one IP range to a different IP range as sub-range for management zones, without the limitation of types of IP addresses

UI Change

The screenshots and the table below illustrates UI changes implemented for the enhancements:



UCMDB 10.22	UCMDB 10.30	Behavior Change
Define partial ranges on Data Flow Probes	Define partial ranges on domains	In 10.30, you can define partial IP ranges at domain level, instead of at probe level.
Domains and Probes	Domains	Removed "Probes" in 10.30, and only domains are displayed in the Domains tree. You select a domain and define IP ranges at domain level for the management zone.
 Open Data Flow Probe Setup	n/a	Removed in 10.30. No need to configure IP ranges at probe level. Note that this change has no impact to the existing Data Flow Probe Setup dialog box where you can define IP ranges for Data Flow Probes/probe clusters.
n/a	 New Range	Opens the New Range dialog box, enabling you to set sub-ranges for management zones. For details on creating new ranges for management

UCMDB 10.22	UCMDB 10.30	Behavior Change
		<p>zones, see "New/Edit Range Dialog Box" on page 450.</p> <p>Compared to the New Range dialog box you open from Data Flow Management > Data Flow Probe Setup, the Type setting is removed.</p>
n/a	 Edit Range	<p>Opens the Edit Range dialog box, enabling you to edit the sub-ranges you want to include or exclude from the full range of the selected domain. This button is available only if you have previously added at least one sub-range of the domain to the Management Zone. For details on editing the existing ranges for management zones, see "New/Edit Range Dialog Box" on page 450.</p> <p>Compared to the Edit Range dialog box you open from Data Flow Management > Data Flow Probe Setup, the Type setting is removed.</p>
 Select Range	 Select Range	<p>In UCMDB version 10.22 and earlier, you select and add sub-ranges at probe level, and those sub-ranges are not editable; In version 10.30 you can edit the sub-ranges after selecting and adding them to the selected domain.</p>
Type column	n/a	<p>Removed in 10.30. It means that, unlike range configuration at probe level, IP ranges configured at domain level are not bound to any type. This offers flexibility in IP range configuration for management zones.</p>

Zone-Based Discovery Behavior Change

When saving IP ranges on management zones, UCMDB server automatically calculates the corresponding probe IP ranges to which the discovery jobs should be dispatched.

When changing the probe IP ranges, UCMDB server adjusts the dispatching of IP ranges of the management zones.

Export and import of a management zone using JMX methods **getManagementZone** and **addManagementZone** are also supported. During the import, probe-based IP ranges will be converted to domain-based IP ranges.

Also, during UCMDB server upgrade, for example, from UCMDB 10.22 to UCMDB 10.30, probe-based IP ranges are converted to domain-based IP ranges.

When running a zone-based discovery, the system dynamically dispatches discovery jobs to live IP addresses only in the IP ranges defined for management zones. During the dispatch, domain-based IP ranges will be converted to probe-based IP ranges, and invalid IP addresses will be skipped.

How to Run Zone-based Discovery

This task describes a recommended workflow for running discovery in a Management Zone.

To run Zone-based discovery:

1. Prerequisites

- Verify that the Data Flow Probe is installed.
- (UNIX only) If you want to specify the locations of data or temporary folders when installing Universal Discovery Agent, see ["How to Specify Data and Temp Folder Locations when Installing or Updating the Universal Discovery Agent for UNIX" on page 180](#).
- Ensure that you have a Management Zone defined in UCMDB. For details about creating Management Zones, see ["How to Create Management Zones" on the next page](#).

2. Set up and activate discovery activities

In the Management Zone:

a. Set up and activate the **Infrastructure Discovery Activity**.

For agent-based discovery, you must ensure that the Universal Discovery (UD) Agent is installed on the node being discovered. You can configure the Infrastructure Discovery activity to install the UD Agent automatically. For more information, see the section describing the Infrastructure Discovery activity in the *Universal CMDB Discovery and Integrations Content Guide*.

Alternatively, if you want to install the UD Agent manually, follow the instructions described in ["How to Install the Universal Discovery Agent Manually" on page 174](#).

b. Set up and activate other activities required for discovering the Management Zone. For more information, see the *Universal CMDB Discovery and Integrations Content Guide*.

3. Results

- To verify the discovery ran successfully, select the Management Zone in the Management Zones tree and, in the **Discovery Status** pane, click the **Results** tab.

For user interface details, see ["Discovery Results Tab/Pane" on page 678](#).

If you do not find a particular CI in the discovery results, you can run the Discovery Troubleshooter to search for the missing CI. For more information about running the Discovery Troubleshooter, see ["Discovery Troubleshooter Wizard" on page 441](#).

Note: The Discovery Troubleshooter can be run in a Management Zone only after the Infrastructure and Basic Software Configuration discovery activities have run in that Management Zone.

- The following events occur as a result of installing the Universal Discovery Agent:
 - The UD Agent generates a Unique ID, which is stored locally on the discovery node and in UCMDB as follows:
 - **Windows and UNIX.** For more information on where the Unique ID is stored, see ["Universal Discovery Agent File Locations" on page 195](#).
 - **UCMDB.** Stored in the `ud_unique_id` attribute of Node CI.

For more information on Unique ID, see ["Universal Discovery Agent Overview" on page 163](#).

- Software Identification Tag files are created and stored on the discovery node. For more information about Software Identification Tags, see ["Hardware and Software Recognition" on page 532](#).

How to Create Management Zones

This task describes how to create a Management Zone.

1. **Prerequisites.** Verify that one or more Data Flow Probes/probe clusters have been added to UCMDB and that **their network ranges are defined**.

This is not a must, but the management zone activities will discover nothing if no valid ranges are defined in related probes.

For details, see ["How to Add Data Flow Probes to UCMDB" on page 54](#).

2. In the Data Flow Management module, go to **Universal Discovery > Zone-based Discovery** tab, right-click the folder under which you want to create the Management Zone, and then click **New Management Zone** from the context menu.
3. In the New Management Zone dialog box, enter a name for the Management Zone.

Note: Naming conventions:

- The name can contain the following characters: **a-z**, **A-Z**, **0-9**, hyphen (-), underscore (_), and space ().
 - The name is not case sensitive; for example, **mz1/mZ1/Mz1** are all the same.
 - The name must not start with a digit.
 - The name must be limited to a length of 50 characters.
4. Select a method for defining ranges for the Management Zone, and define the ranges.
 - To bind the full range of selected Data Flow Probes/probe clusters to the Management Zone, select **Use full Data Flow Probe ranges**, and select the Probes/probe clusters to bind to the Management Zone.
 - To select partial ranges from selected domains, select **Define partial ranges on domains**. Select the domains, and in the right pane, define the partial ranges to bind to the Management Zone.

For more details, see ["New/Edit Management Zone Dialog Box" on page 446](#) and ["New/Edit Range Dialog Box" on page 450](#).

Note: In order to get predictable discovery results, we recommend that when defining the ranges for your Management Zones, they are configured in such a way so that all related IP addresses for a particular discovery node belong to the same Management Zone.

If IP addresses belonging to one discovery node span more than one Management Zone, and the Management Zones are ranked at different levels, unpredictable discovery results may occur. This is because the IP address that was selected to communicate with the discovery node is used to determine which Management Zone the discovery node belongs to, and that address may not always belong to the Management Zone with the highest rank.

5. (Optional) Click the **Settings** tab to configure settings for the Management Zone. For details, see ["New/Edit Management Zone Dialog Box" on page 446](#).
6. Click **OK** to save the Management Zone.

How to Define Discovery Activities in a Management Zone

This task describes how to define discovery activities in a Management Zone.

1. In the Management Zone tree, right-click the Management Zone where you want to create the activity, and select **New Discovery Activity**.
2. Select the type of discovery activity to create:
 - To create a discovery activity from the out-of-the-box activities, select the activity, and follow the wizard. For details on each of the out-of-the-box activities, see the *Universal CMDB Discovery and Integrations Content Guide*.
 - To create a custom discovery activity from a discovery activity template, select **Templates**, and select the discovery activity template. For details, see "[How to Define Custom Discovery Activities from an Activity Template](#)" on the next page.

Note: Before you can create a custom activity, a discovery activity template must be defined. For details about creating discovery activity templates, see "[How to Create Discovery Activity Templates](#)" below.

How to Create Discovery Activity Templates

This task describes how to create a discovery activity template, a collection of jobs on which to base new user-defined discovery activities.

Note: For details about discovery activities provided out-of-the-box with Universal Discovery, see *Universal CMDB Discovery and Integrations Content Guide*.


See also "[How to Define Custom Discovery Activities from an Activity Template](#)" on the next page.

To create a discovery activity template:


1. Go to **Data Flow Management > Universal Discovery > Zone-based Discovery > Management Zones**.
2. Select the Management Zones tree root.

3. In the Management Zone Actions pane on the right, click the **View/Edit Discovery Activity**


Templates  button.

4. In the Discovery Activity Templates dialog box that opens, click **Create Discovery Activity Template** .

The New Discovery Activity Template wizard opens.

5. Enter a name for the discovery activity template and click **Next**.
6. On the **Select Discovery Jobs** page, click **Add Job** .
7. In the Select Jobs dialog box, select jobs to include in the discovery activity template.

Tip:

- To find a specific job, click the **Find Jobs**  button.
 - You can also select entire job modules.
8. Click **Finish** to save the activity template.

How to Define Custom Discovery Activities from an Activity Template


This task describes how to define a custom discovery activity in a Management Zone based on a discovery activity template.

Note: For details about discovery activities provided out-of-the-box with Universal Discovery, see *Universal CMDB Discovery and Integrations Content Guide*.


To create a custom discovery activity from a discovery activity template

1. **Prerequisite:** Ensure that the template upon which you want to base the custom discovery activity has been created. See "[How to Create Discovery Activity Templates](#)" on the previous page.
2. Go to **Data Flow Management > Universal Discovery > Zone-based Discovery**.
3. In the Management Zone tree, select the Management Zone where you want to define the new


discovery activity.


4. Click , select **New Discovery Activity > Templates**, and select a discovery activity template.
5. The New Discovery Activity wizard opens. Give the activity a name and click **Next**.
6. The Select Activity Jobs page opens. The jobs listed under **Selected Jobs** are those included in the activity template you selected above.
 - a. For each job, define job parameters:

Note: For details about each job's parameters, see the *Universal CMDB Discovery and Integrations Content Guide*.

- i. Select the job in the **Selected jobs** list.
 - ii. In the Job Parameters pane, in the relevant parameter's row, select **Override**.
 - iii. In the **Value** column, enter the overriding value.
 - b. (Optional) To add more jobs to the discovery activity, click **Add Job** . The Select jobs dialog box opens. Select the jobs required for the activity, and set the override values for the job parameters.

Tip:

- To find a specific job, click the **Find Jobs**  button.
- You can also select entire job modules.

- c. (Optional) To remove a job from the activity, select the job in the **Selected jobs** list and click the **Remove Job**  button.

Click **Next**.

7. On the Schedule Discovery page, edit the discovery schedule as desired, and click **Next**.
8. On the Summary page, review the summary.
9. To activate the activity upon creation, select **Activate activity**.
10. Click **Finish** to save the activity. The activity appears in the Management Zone tree, under the relevant Management Zone.

How to Rank Management Zones

Management Zone ranking is used when a job's trigger belongs to more than one Management Zone. This could occur when Management Zone ranges overlap, or when a trigger has more than one related IP address and each of these IP addresses belongs to a different Management Zone.

Note: As noted when defining ranges for your Management Zones, if you are aware of a discovery node having multiple IP addresses, we recommended that all of these IP addresses are included in the ranges of only one Management Zone. If IP addresses belonging to one discovery node span more than one Management Zone, and the Management Zones are ranked at different levels, unpredictable discovery results may occur.

For more information and an example, see "[Management Zone Ranking](#)" on page 421.

This task describes how to assign ranks to Management Zones.

1. In the Zone-based Discovery view, select the Root folder in the Managements Zones tree.
2. In the Management Zone Actions pane on the right, click **View/Edit Management Zone Ranks**




The Management Zone Ranking dialog box opens:

- The Ranks tree displays all the defined Management Zones.

Note: By default, when Management Zones are created, they are ranked at level 1.

- When you select a Management Zone in the tree, the right pane displays the Management Zones whose IP ranges overlap with the selected Management Zone.
- The IP ranges of the selected Management Zone are displayed in the lower area of the right pane.

Note: The ranges displayed in the lower area of the right pane belong to the Management Zone selected in the Ranks tree, and not to Management Zones selected in the overlapping Management Zones area.

3. To assign a different ranking to a Management Zone, select the Management Zone in the Ranks tree and click the **Rank Higher**  / **Rank Lower**  button.




Note: After deactivating a discovery activity in a management zone of a higher ranking, make sure you reset the ranking of management zones with overlapping IP ranges, otherwise jobs in the lower ranking management zones with overlapping IP ranges will not be triggered.

How to Configure Global Management Zone Settings


This task describes how to set global settings for Management Zones.


Note: This task is optional. Management Zones can be used with the default values assigned to global settings without any changes by the user.

For more information on global settings for Management Zones, see "[Global Settings Dialog Box](#)" on [page 455](#).

1. In the Universal Discovery window, click the **Zone-based Discovery** tab.
Ensure that the root node of the Management Zone tree is selected.
2. In the **Management Zone Actions** section, click **View/Edit Global Settings** .
3. To modify Management Zone general settings, in the left pane, select **General Settings**.
 - a. Select a category and a setting, and click **Properties** .
 - b. In the Properties dialog box that opens, change the **Current Value** as desired, and click **Save**.
4. To manage Management Zone application signatures, in the left pane select **Application Signatures**, and select the relevant application signatures from the tree.
5. To manage ports for Management Zones, select **Ports**.
 - o To add a new port, click **Add Port** . Enter a name, and port number. If the port should be detected using TCP/UDP port scanning, select **Discover Port**.




Note: Naming conventions for the port:


 - The port name can contain the following characters: **a-z**, **A-Z**, **0-9**, hyphen (-), underscore (_), and space ()
 - Max length: 255 characters
 - o To modify a selected port, click **Edit Port** .

- Change the port number.
 - If the port should be detected using TCP/UDP port scanning, select **Discover Port**,
 - To remove a selected port, click **Remove Port** .
6. Click **OK** to save all changes.

How to Organize the Management Zones Tree

The following table describes the tasks that allow you to organize the Management Zones tree.

Tasks	Actions
Create a new folder	<ol style="list-style-type: none"> 1. Perform one of the following actions: <ul style="list-style-type: none"> ◦ Select the folder under which you want to create the new folder, and then click New Folder . ◦ Right-click the folder under which you want to create the new folder, and then click New Folder from the context menu. 2. Enter the folder name, and then click OK. <p>Note: The folder name cannot contain any of the following characters: <code>^% :"<>?</code></p>
Rename a folder	<ol style="list-style-type: none"> 1. Right-click the Management Zone folder, and then click Rename Folder from the context menu. 2. Enter the new folder name, and then click OK.
Rename a management zone	<ol style="list-style-type: none"> 1. Deactivate the selected management zone and all activities in the management zone. 2. Right-click the Management Zone, and then select Rename  from the context menu. 3. Enter the new management zone name, and then click OK. 4. Go to the C:\hp\UCMDB\DataFlowProbe\runtime\communicationLog directory, perform a backup of the communication log directories belonging to the jobs with the old management zone naming (if necessary), and manually clean up these directories.
Rename an activity	<ol style="list-style-type: none"> 1. Deactivate the selected discovery activity that you want to rename. 2. Right-click the deactivated activity, and then select Rename  from the context menu.

Tasks	Actions
	<ol style="list-style-type: none">3. Enter the new activity name, and then click OK.4. Go to the C:\hp\UCMDB\DataFlowProbe\runtime\communicationLog directory, perform a backup of the communication log directories belonging to the jobs with the old management zone naming (if necessary), and manually clean up these directories.
Move a Management Zone into a different folder	Drag the Management Zone to the target folder.
Move a folder into another folder	Drag the folder to the target folder.
Delete a folder	<p>Use one of the following methods to delete a folder:</p> <ul style="list-style-type: none">• Select the Management Zone folder, and then click Delete .• Right-click the Management Zone folder, and then click Delete Folder from the context menu. <p>Note: When you delete a folder, all the Management Zones under the folder are also deleted.</p>

How to Migrate Management Zone Folders

This topic describes how to migrate Management Zone folders from one instance to another.

If the Management Zone tree contains customized folders, you need to migrate all these folders before migrating Management Zones.

Migrate folders

To migrate Management Zone folders,

1. Log in to the UCMDB JMX console of the source instance. (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. In the UCMDB JMX Quick Search box, enter **listResourceTypes**, and then click the result that appears below the search box to locate the **listResourceTypes** operation.

3. Enter your Customer ID. (**Default: 1**)
4. Click **Invoke**.
5. From the returned list of resource types, locate and click **Discovery_FOLDER_MZ**.
6. Click the **Resource ID** link for each resource in the returned list, and then back up the code in the **Resource XML** text box for later use.

Repeat this step until you back up the XML code for all folders.

7. Log in to the UCMDDB JMX console of the target instance, and then perform the same operations as described in [step 2](#) through [step 5](#).
8. Click **Add new resource**, paste the backup XML code for one of the folders into the **Resource XML** text box, and then click **Save resource**.

Repeat this step until you add all the folders.

Note: Always add higher-level folders before adding lower-level folders. For example, add the folders in the following order if the Management Zone tree has three layers under Root:

- a. The first-layer folders, which are directly under the Root folder.
- b. The second-layer folders.
- c. The third-layer folders.

How to Migrate Management Zones

This topic describes how to migrate Management Zones from one instance to another.

If the Management Zone tree contains customized folders, you need to migrate all these folders before migrating Management Zones. See "[How to Migrate Management Zone Folders](#)" on the previous page.

Note: This feature is available with UCMDDB version 10.30 and later.

Migrate Management Zones

1. **Prerequisites:** Make sure the source and target instances are in the same domain and use the same credentials.

Otherwise, use the **exportCredentialsAndRangesInformation** and **importCredentialsAndRangesInformation** JMX methods to set domain and credentials on the



source and target instances. For detailed instructions, see "How to Export and Import Credential and Range Information in Encrypted Format" in the *Universal CMDB JMX Reference Guide*.

2. Log in to the UCMDB JMX console of the source instance. (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.)
3. Export the selected Management Zone from the source instance.
 - a. In the UCMDB JMX Quick Search box, enter **getManagementZone**, and then click the result that appears below the search box.
 - b. Enter your Customer ID. (**Default: 1**)
 - c. Enter the name of the Management Zone that you want to migrate, and then click **Invoke**.
 - d. On the returned result page, select and copy all the XML code in the **Resource XML** text box for later use.

Note: The path ID in the XML code indicates the ID of the parent folder that the Management Zone belongs to. The folder ID is calculated based on the folder name and path. If the folder keeps the name and path during the migration, the ID should be the same between the source instance and the target instance.

4. Log in to the UCMDB JMX console of the target instance. (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.)
5. Import the Management Zone to the target instance.
 - a. In the UCMDB JMX Quick Search box, enter **addManagementZone**, and then click the result that appears below the search box.
 - b. Enter your Customer ID. (**Default: 1**)
 - c. Paste the XML code you copied earlier into the **Value** field of Management Zone XML.
 - d. Click **Invoke**.
6. Repeat [step 3](#) and [step 5](#) until you export and import all the Management Zones.

How to Rename Management Zones

You can rename existing management zones by using the new **Rename**  option in the management zone context menu. The **Rename**  option is enabled when the selected management zone and all


jobs in the corresponding activities in the management zone are deactivated.



Renaming a management zone might last longer for management zones with larger number of discovery activities/jobs.

Also, renaming the management zones would result in renaming of all of the jobs in the corresponding discovery activities. It means that new directories for these jobs will be created in the **C:\hp\UCMDB\DataFlowProbe\runtime\communicationLog** directory of the probes. This can result in much increased disk usage as the size of the logs (if always enabled) could run into gigabytes. So manual cleanup of the communication log directories belonging to the jobs with the old management zone naming would be required .

Rename Management Zones



To rename a Management Zone,

1. Go to **Data Flow Management > Universal Discovery > Zone-based Discovery**.
2. Right-click the Management Zone you want to rename, and then select **Rename**  from the context menu.

Note: If the **Rename**  option is disabled, click **Deactivate**  to deactivate the selected Management Zone and all of the corresponding discovery activities.

3. Enter the new management zone name, and then click **OK**.
4. Go to the **C:\hp\UCMDB\DataFlowProbe\runtime\communicationLog** directory, perform a backup of the communication log directories belonging to the jobs with the old management zone naming (if necessary), and manually clean up these directories.

How to Rename Activities

You can rename existing activities by using the new **Rename**  option in the activity context menu. The **Rename**  option is enabled when the selected activity and all jobs in the activity are deactivated.


Renaming a activity might last longer for activities with larger number of discovery jobs.



Also, renaming the activities would result in renaming of all of the jobs in the corresponding discovery activities. It means that new directories for these jobs will be created in the **C:\hp\UCMDB\DataFlowProbe\runtime\communicationLog** directory of the probes. This can result in much increased disk usage as the size of the logs (if always enabled) could run into gigabytes. So

manual cleanup of the communication log directories belonging to the jobs with the old management zone naming would be required .

Rename Activities

To rename an activity,

1. Go to **Data Flow Management > Universal Discovery > Zone-based Discovery**.
2. Right-click the activity you want to rename, and then select **Rename**  from the context menu.

Note: If the **Rename**  option is disabled, click **Deactivate**  to deactivate the selected activity and all of the jobs in the discovery activity.

3. Enter the new activity name, and then click **OK**.
4. Go to the **C:\hp\UCMDB\DataFlowProbe\runtime\communicationLog** directory, perform a backup of the communication log directories belonging to the jobs with the old activity naming (if necessary), and manually clean up these directories.

Zone-based Discovery User Interface


This section includes:

Discovery Troubleshooter Wizard	441
New/Edit Management Zone Dialog Box	446
Find Management Zone Dialog Box	454
Management Zone Ranking Dialog Box	454
Global Settings Dialog Box	455
Zone-based Discovery View	457

Discovery Troubleshooter Wizard

The Discovery Troubleshooter allows you to troubleshoot for running software CIs that do not show up when you run an activity on the Management Zone. This is useful for customers who are running activities for discovering running software, and they see that the running software is not found.

This wizard page allows you to initiate the Discovery Troubleshooter.

To access	Select a Management Zone in the Management Zones tree structure on the left and click the Troubleshooting  button.
Important information	<ul style="list-style-type: none"> • The Discovery Troubleshooter wizard can be activated only within the context of a Management Zone. • The Discovery Troubleshooter wizard can be run on a Management Zone only after the Infrastructure and Basic Software Configuration Discovery activities have been run on that Management Zone. • If any discovery activities are still running when you start this wizard, the Wait for Jobs screen appears after clicking Next in the first screen of this wizard. If the Wait for Jobs screen appears, wait until the activities finish and then continue with the wizard.
Relevant tasks	"How to Run Zone-based Discovery" on page 428
Wizard map	The Discovery Troubleshooter Wizard contains: Discovery Troubleshooter Wizard > "Activity Instances Mapping Page" > "Target Host Page" > "Additional Information Is Required Page" > "Investigate Missing Node CI Page" > "Retrieve Running Software CIs Page"
See also	<ul style="list-style-type: none"> • "Discovery Troubleshooter" on page 424 • "Universal Discovery Overview" on page 416 • "Zone-based Discovery View" on page 457

Activity Instances Mapping Page

This wizard page allows you to select a Discovery Activity Instance associated with the Management Zone on which you are running the Troubleshooter.

Important information	This wizard page only appears if you have more than one Infrastructure or Basic Software Configuration Discovery activity associated with the Management Zone.
Wizard map	The Discovery Troubleshooter Wizard contains: "Discovery Troubleshooter Wizard" > Activity Instances Mapping Page > "Target Host Page" > "Additional Information Is Required Page" > "Investigate Missing Node CI Page" > "Retrieve Running Software CIs Page"

User interface elements are described below:

UI Element (A-Z)	Description
Activity	Lists the instances of the Activity Type. If there is more than one instance, they

UI Element (A-Z)	Description
Instance	are listed in a drop-down menu.
Activity Type	Lists the types of Discovery Activities that are prerequisites for running the Troubleshooter. Currently, only Infrastructure and Basic Software Configuration Discovery activity types are listed here.
Troubleshooter Log	This log lists all actions performed by the Troubleshooter that occur in the background and do not appear in the user interface.

Target Host Page

This wizard page allows you to enter the name or IP address of the host that you want to discover.

Important information	<ul style="list-style-type: none"> The name or IP address that you enter on this page should be within the range of at least one of the probes in the Management Zone. If it is not, an error message appears. After clicking Next on this page, the Validate Target Host IP Address page appears. Wait briefly while the Discovery Troubleshooter validates the target host IP address. If the target host you entered is not within the range of the Management Zone, the Validate Target Host IP Address page offers you an option to choose a different target host, or close the wizard. If you choose a different target host, the Target Host page appears again. Once an IP address is defined, the Discovery Troubleshooter checks if a CI exists for that IP. If no CI exists, the Discovery Troubleshooter automatically creates a CI for that IP address.
Wizard map	<p>The Discovery Troubleshooter Wizard contains:</p> <p>"Discovery Troubleshooter Wizard" > "Activity Instances Mapping Page" > Target Host Page > "Additional Information Is Required Page" > "Investigate Missing Node CI Page" > "Retrieve Running Software CIs Page"</p>

User interface elements are described below:

UI Element (A-Z)	Description
Target host:	Enter here the name or IP address of the host that you want to discover.
Troubleshooter Log	This log lists all actions performed by the Troubleshooter that occur in the background and do not appear in the user interface.

Additional Information Is Required Page

This wizard page allows you to select a method for detecting the target host.

Important information	<ul style="list-style-type: none"> • After clicking Next on this page, the Discovery Troubleshooter attempts to activate a specific job. If this job is not active, a message appears stating that the job is about to be activated and that if you activate it, this may invoke the job on all potential trigger CIs that are relevant to this job. • After clicking Next on this page, the Discovery Progress screen appears and informs you that Discovery is currently running.
Wizard map	The Discovery Troubleshooter Wizard contains: "Discovery Troubleshooter Wizard" > "Activity Instances Mapping Page" > "Target Host Page" > Additional Information Is Required Page > "Investigate Missing Node CI Page" > "Retrieve Running Software CIs Page"

User interface elements are described below:

UI Element (A-Z)	Description
Select detection method for the requested host:	Discovery uses detection methods to communicate with the remote machine. Choose from one of the following detection methods: WMI, Shell, Power Shell, SNMP.
Troubleshooter Log	This log lists all actions performed by the Troubleshooter that occur in the background and do not appear in the user interface.

Investigate Missing Node CI Page

This wizard page lists errors found if the Troubleshooter does not succeed in connecting to the host, and offers options for trying to resolve those errors.

Important information	This page only appears if the Troubleshooter does not succeed in connecting to the host.
Wizard map	The Discovery Troubleshooter Wizard contains: "Discovery Troubleshooter Wizard" > "Activity Instances Mapping Page" > "Target Host Page" > "Additional Information Is Required Page" > Investigate Missing Node CI Page > "Retrieve Running Software CIs Page"

User interface elements are described below:

UI Element	Description
<error messages>	<p>Various error messages can occur when running the Troubleshooter.</p> <p>One of the more common types of error messages is Permission Denied. This error occurs if there is a problem with the user credentials. You can attempt to fix this error by clicking Fix by the error message. If you do this, the Update Credentials dialog box appears, and you can update the user credentials as explained in "Protocol Details Pane" on page 113. After updating user credentials, you should choose Rerun relevant discovery job to find missing CI in this wizard page and continue with the wizard.</p>
Rerun relevant discovery job to find missing CI	<p>Choose this option if you see an error in the list for which rerunning a job might help (for example, a timeout error). If you choose this option, the Discovery Progress screen appears.</p>
Choose a different detection method to find missing CI	<p>If you choose this option, the wizard returns to the "Additional Information Is Required Page" on the previous page.</p>
Close the Troubleshooter and save support log	<p>Choosing this option exits the wizard and saves the log file to a location on the server machine (the exact location is indicated on the page that follows).</p>
Troubleshooter Log	<p>This log lists all actions performed by the Troubleshooter that occur in the background and do not appear in the user interface.</p>

Retrieve Running Software CIs Page

This wizard page lists all running software that is currently listed as connected to the detected Node CI.

Wizard map	<p>The Discovery Troubleshooter Wizard contains:</p> <p>"Discovery Troubleshooter Wizard" on page 441 > "Activity Instances Mapping Page" > "Target Host Page" > "Additional Information Is Required Page" > "Investigate Missing Node CI Page" > Retrieve Running Software CIs Page</p>
-------------------	--



User interface elements are described below:

UI Element	Description
Yes, the CI was discovered	<p>Check this option if the running software CI that you are looking for is in the list, or just close the Troubleshooter since you have successfully completed troubleshooting.</p>

UI Element	Description
No, the CI is still missing	<p>Check this option if the running software CI that you are looking for is not in the list. If you choose this option, the Software Identification Rules Management screen appears, and you can continue the search for the missing CI as follows:</p> <ol style="list-style-type: none"> 1. In the Software Identification Rules Management screen, update the available application signatures as explained in "Software Identification Rule Editor Dialog Box" on page 290. 2. The Troubleshooter then attempts again to find the missing CI (by re-running its corresponding job) and this wizard page appears with a potentially more extensive list of all running software that is connected to the detected Node CI. 3. If the running software CI that you are looking for is still not in the list, select again No, the CI is still missing, and the Additional Information Is Required page appears (see below).
Additional Information Is Required page	<p>If after updating the available application signatures the Troubleshooter still does not find the missing CI, this page appears. You can choose either Update software identification rules and rerun discovery or Close the Troubleshooter and save support log.</p> <p>If you choose Update software identification rules and rerun discovery, the Software Identification Rules Management screen appears again and you can continue to update the software identification rules.</p>
Troubleshooter Log	<p>This log lists all actions performed by the Troubleshooter that occur in the background and do not appear in the user interface.</p>

New/Edit Management Zone Dialog Box

This dialog box enables you to create or edit a Management Zone.







To access	<p>Select Data Flow Management > Universal Discovery > Zone-based Discovery tab.</p> <ul style="list-style-type: none"> • To create a Management Zone: Click New Management Zone . • To edit an existing Management Zone: Select the Management Zone and click Edit .
Important information	<p>You must have at least one Data Flow Probe defined to create a Management Zone.</p>
Relevant tasks	<ul style="list-style-type: none"> • "Configure IP Ranges for Management Zones at Domain Level" • "How to Create Management Zones" on page 429 • "How to Run Zone-based Discovery" on page 428




	<ul style="list-style-type: none"> • "New/Edit Range Dialog Box" on page 450
See also	<ul style="list-style-type: none"> • "Universal Discovery Overview" on page 416 • "Zone-based Discovery View" on page 457 • "Discovery Troubleshooter" on page 424

Details Tab

User interface elements are described below:

UI Elements	Description
Name	<p>The name of the Management Zone. This field is mandatory.</p> <p>Note: Naming conventions:</p> <ul style="list-style-type: none"> • The name can contain the following characters: a-z, A-Z, 0-9, hyphen (-), underscore (_), and space (). • The name is not case sensitive; for example, mz1/mZ1/Mz1 are all the same. • The name must not start with a digit. • The name must be limited to a length of 50 characters.
Description	<p>The description of the Management Zone. This field is optional. This description appears in the Details tab in the right pane after creating the Management Zone.</p> <p>Note: The length of the description is limited to 600 characters.</p>
Ranges Method	<p>Enables you to select a method for defining ranges for the Management Zone.</p> <ul style="list-style-type: none"> • Use full Data Flow Probe ranges. Displays all the Data Flow Probes/probe clusters in the lower pane, enabling you to select Data Flow Probes/probe clusters—with their full ranges—for the Management Zone. To select Data Flow Probes/probe clusters for the Management Zone, see "Data Flow Probe Selection Area" below. <p>Note:</p> <ul style="list-style-type: none"> ○ Data Flow Probes/probe clusters must have a defined range before being bound to a Management Zone. ○ If changes are made to the range of a bound Data Flow Probe/probe cluster, these changes are applied to the Management Zone's range only after deactivating and reactivating the Management Zone. <p>Similarly, if you add a Probe to a bound probe cluster, the Probe is, in</p>

UI Elements	Description
	<p>effect, added to the probe cluster only after and reactivating the Management Zone.</p> <ul style="list-style-type: none"> • Define partial ranges on domains. Displays the Select Ranges area in the lower pane, enabling you to define ranges for the Management Zone that are subsets of the ranges defined for the existing domains. For details, see "<Define Domain Ranges area>" below. <p>Default: Use full Data Flow Probe ranges is selected</p> <p>Note: In order to get predictable discovery results, we recommend that when defining the IP ranges for your Management Zones, they are configured in such a way so that all related IP addresses for a particular discovery node belong to the same Management Zone.</p> <p>If IP addresses belonging to one discovery node span more than one Management Zone, and the Management Zones are ranked at different levels, unpredictable discovery results may occur. This is because the IP address that was selected to communicate with the discovery node is used to determine which Management Zone the discovery node belongs to, and that address may not always belong to the Management Zone with the highest rank.</p>
<p>Data Flow Probe Selection Area</p>	<p>Displayed when Ranges Method > Use full Data Flow Probe ranges is selected. It displays the all of the Data Flow Probes/probe clusters available in UCMDb, and enables you to select Data Flow Probes/probe clusters for the Management Zone. Discovery in the Management Zone is run over the full ranges of the selected Data Flow Probes/probe clusters .</p> <ul style="list-style-type: none"> • Non-selected Probes list. Lists the Data Flow Probes/probe clusters in UCMDb that can be added to the Management Zone. Select a Data Flow Probe/probe cluster and click  to move it to the Selected Probes list. Click  to move all of the Data Flow Probes/probe clusters to the Selected Probes list. • Selected Probes list. Lists the Data Flow Probes/probe clusters selected for the Management Zone. Select a Data Flow Probe/probe cluster and click  to remove it from the Selected Probes list. Click  to remove all of the Data Flow Probes/probe clusters from the Selected Probes list.
<p><Define Domain Ranges area></p>	<p>Displayed when Ranges Method > Define partial ranges on domains is selected.</p> <ul style="list-style-type: none"> • Domains tree. Displays the domains available for the Management Zone. •  New Range. Opens the New Range dialog box, enabling you to set sub-ranges for management zones. For details on creating new ranges for management zones, see "New/Edit Range Dialog Box" on page 450. •  Select Range. Opens the Select Range dialog box, enabling you to select the

UI Elements	Description
	<p>sub-ranges you want to include or exclude from the full range of the selected domain.</p> <p>If the selected domain contains Data Flow Probes/probe clusters with IP ranges defined, when you open the Select Range dialog box, it displays all IP ranges belonging to the Data Flow Probes/probe clusters under the domain as sub-ranges. In the Select Range dialog box, you can select multiple sub-ranges. After clicking OK, the selected sub-ranges are added to the selected domain. Then, you can select a sub-range and click Edit Range  to edit the sub-range.</p> <p>If a sub-range has more than one excluded section, you cannot choose to exclude only one section; if you choose to exclude one section, all sections will be excluded.</p> <ul style="list-style-type: none"> <li data-bbox="418 772 1383 947">  Edit Range. Opens the Edit Range dialog box, enabling you to edit the sub-ranges you want to include or exclude from the full range of the selected domain. This button is available only if you have previously added at least one sub-range of the domain to the Management Zone. For details on editing the existing ranges for management zones, see "New/Edit Range Dialog Box" on the next page. <li data-bbox="418 961 1383 1073">  Delete Range. Enables you to delete a sub-range from the Management Zone. This button is available only if you have previously added at least one sub-range of the domain to the Management Zone. <p>Note: Deleting a sub-range here deletes the sub-range from the Management Zone, but not from the domain itself.</p>

Settings Tab





This tab allows you to configure settings for the selected Management Zone. For details about global Management Zone settings, see ["Global Settings Dialog Box" on page 455.](#)

<p>Important information</p>	<p>These settings are the same as the settings that can be configured globally for all Management Zones, with the following limitations:</p> <ul style="list-style-type: none"> <li data-bbox="418 1528 1317 1591">The settings that you configure for a particular Management Zone affect that Management Zone only, and not all the Management Zones in the system. <li data-bbox="418 1606 1317 1669">The settings configured for a particular Management Zone override the global Management Zone settings for that Management Zone only.
-------------------------------------	---

UI Elements	Description
General Settings	<p>Enables you to change the current value of a selected setting.</p> <p>Note: The setting Maximum Probe Connections Per Second can be configured globally for all Management Zones only, as this setting affects the entire probe and not only a Management Zone.</p>
Application Signatures	<p>Enables you to select application signatures for the Management Zone.</p> <p>Note: The list of available application signatures is managed Global Settings dialog box. For details, see "How to Configure Global Management Zone Settings" on page 435.</p>
Ports	<p>Enables you add ports or edit a port's port number, or delete a port.</p> <p>Note: If the port should be detected using TCP/UDP port scanning, select Discover Port.</p>

New/Edit Range Dialog Box




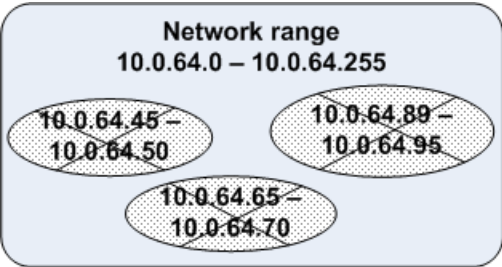
Enables you to set network ranges at domain level for management zones. The results are retrieved from the addresses in the range you define. You can also define IP addresses that must be excluded from a range.

To access	<ol style="list-style-type: none"> 1. Select Data Flow Management > Universal Discovery > Zone-Based Discovery tab, and then click New Management Zone  or select an existing Management Zone and click Edit . 2. In the Add/Edit Management Zone dialog box, go to the Details tab, select Define partial ranges on domains for Ranges Method. 3. In the <Define Domain Ranges area>, go to Domains > <Domain> in the Domains tree, and in the right pane click the New Range  or Edit Range  button.
Important information	It will not check whether the new range is also defined at probe level. Only valid IPs could trigger the related activities to perform discovery.
Relevant tasks	<ul style="list-style-type: none"> • "How to Create Management Zones" • "New/Edit Management Zone Dialog Box" • "Configure IP Ranges for Management Zones at Domain Level"

User interface elements are described below:

UI Element	Description
IPv4/6	Enables you to define the IP range in IPv4 or IPv6 format.
Definition Type	<ul style="list-style-type: none"> • IP Range. (IPv4 format only) Enables you to define an IP address range for the probe/cluster. You define a start IP address and an end IP address. • CIDR. Enables you to define an address range using the CIDR (Classless Inter-Domain Routing) notation, where each IP address has a network prefix that identifies either an aggregation of network gateways or an individual gateway. The length of the network prefix is also specified as part of the IP address and varies depending on the number of bits that are needed. <p>Available: When creating a new range only</p>
Range	<p>Enables you to select a range over which domain a probe or cluster should perform discovery.</p> <p>IPv4</p> <ul style="list-style-type: none"> • IP Range. Define a range of IPv4 addresses using the following rules: <ul style="list-style-type: none"> ◦ The IP address range must have the following format: start_ip_address – end_ip_address For example: 10.0.64.0 - 10.0.64.57 ◦ The first decimal value (octet) of the start IP address and the end IP address must be identical. For example, 10.1.2.3 - 10.4.5.6 ◦ The range can include an asterisk (*), representing any number in the range of 0-255. <ul style="list-style-type: none"> • If you use an asterisk, you do not need to enter a second IP address. For example, you can enter the range pattern 10.0.48.* to cover the range from 10.0.48.0 to 10.0.48.255. • Use an asterisk in the lower bound IP address of the IP range pattern only. If you use an asterisk in the lower bound IP address and also enter an upper bound IP address, the upper bound IP address is ignored. • You can use more than one asterisk (*) in an IP address as long as they are used consecutively. The asterisks cannot be situated between two numbers in the IP address, nor can they be substituted for the first digit in the number. For example, you can enter 10.0.*.* but not 10.*.64.*. • CIDR Notation. Define a range using the CIDR notation as follows: <ol style="list-style-type: none"> a. Enter the IP address in IPv4 format. b. In the drop-down, choose the number of bits (1-32) to determine the network prefix.

UI Element	Description
	<p>For example, if you enter 192.30.250.00/18, then 192.30.250.00 is the network address and 18 indicates that the first 18 bits are the network part of the address, leaving the last 14 bits for specific host addresses.</p> <p>IPv6</p> <p>IPv6 ranges are defined in CIDR notation only:</p> <ol style="list-style-type: none"> 1. Enter the IP address in IPv6 format. You can define IPv6 ranges using the full or compressed IPv6 notation <p>Example:</p> <ul style="list-style-type: none"> ○ Full IPv6 addresses: abcd:abcd:abcd:abcd:abcd:abcd:abcd:abcd ○ Compressed IPv6 address: <ul style="list-style-type: none"> ● A:B:C:D:1:2:3:4 is the compressed version of 000A:000B:000C:000D:0001:0002:0003:0004 ● abcd::abcd is the compressed version of abcd:0000:0000:0000:0000:0000:0000:abcd ● ::abcd is the compressed version of 0000:0000:0000:0000:0000:0000:0000:abcd <ol style="list-style-type: none"> 2. In the drop-down, choose the number of bits (1-128) to determine the network prefix. <p>For example, if you enter abcd:abcd:abcd:abcd:abcd:abcd:abcd:abcd/100, then abcd:abcd:abcd:abcd:abcd:abcd:abcd:abcd is the network address and 100 indicates that the first 100 bits are the network part of the address, leaving the last 28 bits for specific host addresses.</p> <p>Note: IPv6 ranges cannot include IPv4-mapped IPv6 addresses (0.0.0.0 - 255.255.255.255). If your IPv6 range includes IPv4-mapped IPv6 addresses, these addresses must be defined separately in IPv4 ranges.</p> <p>For example, the IPv6 range, 0:0:0:0:ffe:0:0/60, must be defined as a number of ranges as follows:</p> <ul style="list-style-type: none"> ● IPv6 range: 0:0:0:0:0:0:0:0 – 0:0:0:0:ffe:fff:fff:fff ● IPv4-mapped IPv6 range, 0:0:0:0:fff:0:0 - 0:0:0:0:fff:fff:fff:fff, must be defined in IPv4 format: 0.0.0.0 - 255.255.255.255, per network class ● IPv6 range: 0:0:0:1:0:0:0:0 – 0:0:0:f:fff:fff:fff:fff
<p>Description (Optional)</p>	<p>A description about the selected range.</p> <p>Note:</p> <ul style="list-style-type: none"> ● Maximum number of characters allowed: 150 ● No new lines or tabs may be inserted


UI Element	Description
Excluded IP Ranges	<p>Enables you to define a range of IP addresses to exclude from the full network range specified above.</p> <p>Note:</p> <ul style="list-style-type: none">• The rules for entering an excluded range are the same as for entering a range. For details, see Range (on page 451).• The excluded range must be defined in the same format (IPv4/IPv6) as the full network range.• Even when a network range is defined using CIDR notation, the excluded ranges can still only be defined in <start_ip_address> – <end_ip_address> format. <p>New Excluded IP Range . Enables you to define a range of IP addresses to exclude from the full range, and enter a description about the excluded range if desired.</p> <p>Delete Excluded IP Range . Deletes an excluded IP range.</p> <p>Edit Excluded IP Range . Enables you to edit a defined excluded IP range.</p> <p>Example:</p> <p>You can divide a network range into several sub-ranges.</p> <p>For example, if the range is 10.0.64.0 – 10.0.64.255</p> <p>and you define three excluded ranges:</p> <ul style="list-style-type: none">• 10.0.64.45 – 10.0.64.50• 10.0.64.65 – 10.0.64.70• 10.0.64.89 – 10.0.64.95 <div data-bbox="412 1381 911 1646"></div> <p>the Universal Discovery is performed over:</p> <ul style="list-style-type: none">• 10.0.64.0 – 10.0.64.44• 10.0.64.51 – 10.0.64.64• 10.0.64.71 – 10.0.64.88• 10.0.64.96 – 10.0.64.255

Find Management Zone Dialog Box

Enables you to locate Management Zones in the tree answering to specified search criteria.


To access	Select Universal Discovery > Zone-based Discovery > Management Zones pane, and click the Find Management Zone  button.
------------------	---

User interface elements are described below:

UI Element	Description
	Finds the next Management Zone in the tree meeting the search criteria.
Find Management Zone by	<p>Enables you to search for a Management Zone by name, or IPv4/IPv6 address.</p> <p>Depending on your selection, enter the relevant search criteria:</p> <ul style="list-style-type: none"> • Name. Enter the name of the Management Zone, or part of the name. • IP Address. Enter the IP address in the relevant format. <p>Note: When looking for an IP address for a specific routing domain, also specify the domain. If no domain is provided, all domains will be searched.</p>
Direction	Directs the search forwards or backwards through the Management Zone tree.




Management Zone Ranking Dialog Box

This dialog box enables you to set ranking levels for your Management Zones.

To access	<p>Select Data Flow Management > Universal Discovery > Zone-based Discovery tab > Management Zones root, and click the View/Edit Management Zone</p> <p>Ranking  button.</p>
Important information	<ul style="list-style-type: none"> • Changing ranks of Management Zones may cause discovery activities to rerun. • As noted, when defining ranges for your Management Zones, if you are aware of a discovery node having multiple IP addresses, we recommend that all of these IP addresses are included in the ranges of only one Management Zone. If IP addresses belonging to one discovery node span more than one Management Zone, and the Management Zones are ranked at different levels, unpredictable discovery results may occur. This is because the IP address that was selected to


	communicate with the discovery node is used to determine which Management Zone the Node belongs to, and that address may not always belong to the Management Zone with the highest rank.
Relevant tasks	<ul style="list-style-type: none"> • "How to Run Zone-based Discovery" on page 428 • "How to Rank Management Zones" on page 434
See also	"Management Zone Ranking" on page 421

User interface elements are described below:

UI Elements	Description
	<p>Rank Higher/Lower. Enables you to move the selected Management Zone to a higher or lower ranking level.</p> <p>Note: Management Zones with a ranking of level 1 are the highest ranking Management Zones.</p>
	Reset. Enables you to undo changes that you made to the ranks.
	Expand/Collapse All. Expands/Collapses the Ranks tree, displaying the Management Zones under each rank.
< Ranks tree >	Displays all the Management Zones under its ranking level.
< Management Zone Ranking Details pane >	<p>When you select a Management Zone in the Ranks tree, the right pane displays the following information:</p> <ul style="list-style-type: none"> • Management Zones Overlapping with <Management Zone>. Displays all of the Management Zones that contain ranges that overlap with the range of the selected Management Zone. • Ranges of <Management Zone>. Displays the ranges defined for the Management Zone selected in the Ranks tree. For more details, see "New/Edit Range Dialog Box" on page 131.








Global Settings Dialog Box




This dialog box enables you to set and view global settings for all Management Zones in your system.

To access	Select Data Flow Management > Universal Discovery > Zone-based Discovery tab > Management Zone Actions pane, and click View/Edit Global Settings  .
Relevant tasks	<ul style="list-style-type: none"> • "How to Configure Global Management Zone Settings" on page 435 • "How to Create Management Zones" on page 429

See also	<ul style="list-style-type: none"> • "New/Edit Management Zone Dialog Box" on page 446 • "Software Identification Rule Editor Dialog Box" on page 290
-----------------	---

User interface elements are described below:

UI Elements	Description
General Settings	<p>Enables you to manage general settings for all of the Management Zones.</p> <ul style="list-style-type: none"> • Categories pane. Displays the available setting categories. Select a category to display the relevant settings on the right. •  Properties. Opens the Properties window, and allows you to view the properties for a selected global setting and change it's value. <p style="margin-left: 20px;">Note: You can also open the Properties window by double-clicking on a global setting in the list.</p> •  Undo. Restores the previous value of the selected setting (only relevant if you changed the value of that setting). • Filter by column. Filters the list of global settings by selecting a category from the drop-down list and entering filter criteria in the text box. <p>Note: For details about each of the displayed settings, see the section describing the globalsettings.xml file in the <i>Universal CMDB Discovery and Integrations Content Guide</i>.</p>
Application Signatures	<p>Enables you to manage application signatures.</p> <ul style="list-style-type: none"> •  Add. Opens the Software Identification Rule Editor dialog box, enabling you to add an application signature to the list of available signatures. For details, see "Software Identification Rule Editor Dialog Box" on page 290. •  Edit. Opens the Software Identification Rule Editor dialog box, enabling you to edit a selected application signature. For details, see "Software Identification Rule Editor Dialog Box" on page 290. •  Export Application Signature to XML. Enables you to export the selected application signature to an xml file. •  Import Application Signature from XML Enables you to import an application signature from an xml file. •  Remove. Removes the selected application signature from the list of available signatures.
Ports	<p>Enables you to manage ports.</p>

UI Elements	Description
	<ul style="list-style-type: none"> •  Add Port. Opens the Add New Port dialog box, enabling you to add a new port. •  Edit Port. Enables you to modify port number of the selected port. •  Remove Port. Enables you to remove the selected port. <p>Note:</p> <ul style="list-style-type: none"> • Naming conventions for the port: <ul style="list-style-type: none"> ◦ The port name can contain the following characters: a-z, A-Z, 0-9, hyphen (-), underscore (_), and space () ◦ Max length: 255 characters • When adding or modifying a port, if the port should be detected using TCP/UDP port scanning, select Discover Port.

Zone-based Discovery View











This view enables you to manage Management Zones, run discovery activities in the Management Zones, and troubleshoot why expected CIs are missing after discovery.










To access	Select Data Flow Management > Universal Discovery > Zone-based Discovery tab.
Relevant tasks	"How to Run Zone-based Discovery" on page 428
See also	<ul style="list-style-type: none"> • "Universal Discovery Overview" on page 416 • "Management Zone Ranking" on page 421 • "New/Edit Management Zone Dialog Box" on page 446 • "Discovery Troubleshooter" on page 424 • "Discovery Troubleshooter Wizard" on page 441




User interface elements are described below:

Management Zones Tree Pane

The Management Zone tree displays all of the Management Zones defined in Universal Discovery and all of the discovery activities that have been defined in each Management Zone.

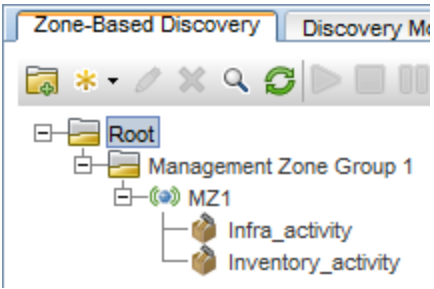
UI Element	Description
	<p>New Folder. Enables you to create a new Management Zone folder.</p>
	<ul style="list-style-type: none"> • New Management Zone. Enables you to create a Management Zone. For more information on creating Management Zones, see "New/Edit Management Zone Dialog Box" on page 446. • New Discovery Activity. Enabled when you select a Management Zone. Enables you to create discovery activities in the selected Management Zone. For more information on defining discovery activities, see the <i>HPE UCMDB Discovery and Integrations Content Guide - Discovery Activities</i>.
	<p>Edit. Enables you to edit the selected Management Zone or discovery activity.</p>
	<p>Delete. Deletes the selected Management Zone, discovery activity, or folder.</p> <p>Note: When you delete a Management Zone, all activities associated with it are also deleted.</p> <p>When you delete a folder, all Management Zones and subfolders in the folder are also deleted.</p>
	<p>Find Management Zone. Opens the Find Management Zone dialog box, enabling you to locate a Management Zone in the tree by name or by IP address. For details, see "Find Management Zone Dialog Box" on page 454.</p>
	<p>Reload Data. Refreshes the data in the Management Zones tree.</p>
	<p>Activate. Activates the selected Management Zone or discovery activity.</p> <p>Note: Activating a Management Zone activates all of its activities.</p>
	<p>Deactivate. Deactivates the selected Management Zone or discovery activity.</p> <p>Note: Deactivating a Management Zone deactivates all of its activities.</p>
	<p>Pause. Pauses the selected Management Zone or discovery activity.</p> <p>Note:</p> <ul style="list-style-type: none"> • Pausing a Management Zone also pauses all of the activated and running discovery activities in the Management Zone. • Pausing a Management Zone does not have any effect on discovery activities that are not activated.
	<p>Resume. Resumes the selected, paused Management Zone or discovery activity.</p> <p>Note:</p>

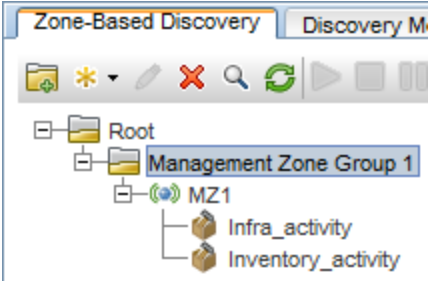
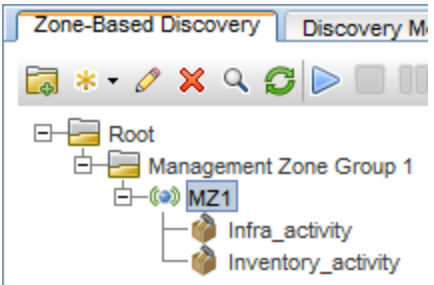
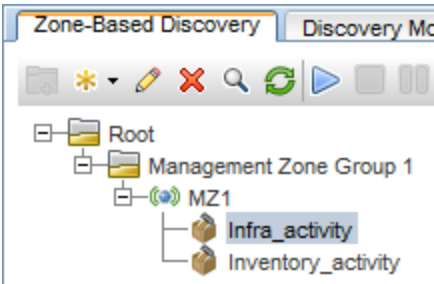
UI Element	Description
	<ul style="list-style-type: none"> Resuming a Management Zone also resumes all of the paused discovery activities in the Management Zone. Resuming a Management Zone does not have any effect on discovery activities that are not activated.
	<p>Rerun.</p> <ul style="list-style-type: none"> Management Zone root: Runs discovery again in all of the Management Zones. Management Zone: Runs discovery again in the selected Management Zone. Discovery activity: Runs the selected discovery activity again.
	<p>Troubleshoot Missing CIs. Opens the Discovery Troubleshooter wizard.</p> <p>If a CI is missing from the results of a Data Flow Probe and you expected to see it, the Discovery Troubleshooter wizard tries to find the missing CI.</p> <p>Note: This feature is enabled in a Management Zone only after the Infrastructure and Basic Software Configuration discovery activities have run. For more information on Discovery Troubleshooter, see "Discovery Troubleshooter" on page 424.</p>
	<p>Expand/Collapse All. Expands/Collapses the Management Zone tree. When expanded, all discovery activities that have run in the Management Zones are listed.</p>
<p><Management Zones tree icons></p>	<p>The Management Zones tree displays the following icons:</p> <ul style="list-style-type: none"> . Represents a Management Zone folder. . Represents a Management Zone. <ul style="list-style-type: none"> . Indicates that all of the activated activities in the Management Zone are running. . Indicates that all of the activated activities in the Management Zone are paused. . Indicates that some of the activated activities in the Management Zone are running and some are paused. . Represents a running/paused activity in a Management Zone.
<p><right-click menu></p>	<p>In addition to some of the functionality described above, right-clicking a folder enables you to do the following:</p> <ul style="list-style-type: none"> Rename Folder. Allows you to rename the selected management zone folder's name.

UI Element	Description
	<p>Right-clicking a management zone enables you to do the following:</p> <ul style="list-style-type: none">  Rename. Opens the Rename Management Zone dialog, which allows you to rename the selected management zone's name. This option is enabled when the selected management zone and all activities in the management zone are deactivated. <p>Note: This operation might last longer for management zones with larger number of discovery activities/jobs.</p> <p>Right-clicking a discovery activity enables you to do the following:</p> <ul style="list-style-type: none">  Clear Probe Results Cache. Clears the selected activity's results cache on the Probes. <p>Note: If an activity's results cache is cleared, all discovery results are sent again the next time the activity runs.</p> <ul style="list-style-type: none">  Rename. Opens the Rename Activity dialog, which allows you to rename the selected activity's name. This option is enabled when the selected activity is deactivated. <p>Note: This operation might last longer for activities with larger number of discovery jobs.</p>

Management Zone Details Pane

The right pane of the Zone-based Discovery view displays varying information, depending on what you select in the Management Zones tree on the left.


Selected in the tree	Displayed in right pane
<p>Management Zones tree root</p> 	<ul style="list-style-type: none"> • "Management Zone Actions Pane" on the next page • "Discovery Status Pane" on page 463
<p>A Management Zone folder</p>	<p>A list of all the Management Zones under the selected folder</p>






Selected in the tree	Displayed in right pane
	
<p>A Management Zone</p> 	<ul style="list-style-type: none"> • "Management Zone Details Pane" on the next page • "Discovery Status Pane" on page 463
<p>A discovery activity</p> 	<ul style="list-style-type: none"> • "Activity Details Pane" on page 464 • "Discovery Status Pane" on page 463

Management Zone Actions Pane

Displayed when you select the Management Zones root in the tree.


This pane provides a portal to performing actions that affect all Management Zones.

UI Element	Description
	<p>Create Management Zone. Opens the New Management Zone dialog box, enabling you to create a new Management Zone. For details, see "New/Edit Management Zone Dialog Box" on page 446.</p>

UI Element	Description
	View/Edit Management Zone Ranking. Opens the Management Zone Ranking dialog box, enabling you to manage the ranking levels of the Management Zones. For details, see "Management Zone Ranking Dialog Box" on page 454.
	<p>View/Edit Discovery Activity Template. Opens the Discovery Activity Template dialog box, where you can create or delete discovery activity templates. Discovery activity templates can be used to as a basis for custom discovery activities.</p> <ul style="list-style-type: none">  Create Discovery Activity Template. Open the Discovery Activity Template wizard, enabling you to define a template on which to base custom discovery activities. For more details, see "How to Create Discovery Activity Templates" on page 431.  Remove Discovery Activity Template. Enables you to remove a selected discovery activity template. <p>Note: You cannot remove a template if there are custom discovery activities that use the template.</p>
	<p>View/Edit Global Settings. Opens the Global Settings dialog box where you can view and edit global Management Zone settings. For details, see "Global Settings Dialog Box" on page 455.</p> <p>Note: An individual Management Zone's settings override the settings defined in the global settings. For details on configuring an individual Management Zone, see "New/Edit Management Zone Dialog Box" on page 446 (Settings tab).</p>

Management Zone Details Pane

Displayed when you select a Management Zone in the Management Zone tree.

Important information	To edit the details of the selected Management Zone, click the Edit  button in the Management Zones pane.
------------------------------	---

User interface elements are described below:

UI Element	Description
Description	The description of the Management Zone, defined when the Management Zone was created.
Ranges Method	The method for defining ranges for the Management Zone, as defined when creating the Management Zone:

UI Element	Description
	<ul style="list-style-type: none"> • Based on full Data Flow Probe ranges • Based on partial Data Flow Probe ranges <p>For more details, see "New/Edit Management Zone Dialog Box" on page 446.</p>
Ranges	<p>Displays the defined ranges for the selected Management Zone on the selected Data Flow Probe.</p> <p>Note:</p> <ul style="list-style-type: none"> • You cannot edit ranges in this pane. To edit ranges, see "New/Edit Range Dialog Box" on page 131. • If the ranges method is Based on partial Data Flow Probe ranges, the range can be displayed here either according to the IP range format or CIDR format, as explained in "New/Edit Range Dialog Box" on page 131.

Discovery Status Pane









Displays the progress and results of discovery in Management Zones. Displayed when you select the Management Zones root, a Management Zone, or a discovery activity in the Management Zones tree.




UI Element	Description
Progress Tab	<ul style="list-style-type: none"> • Displays the last status known by the UCMDB server for each job Trigger CI within the context selected for discovery. <p>The information displayed varies depending on the selected area of focus.</p> <ul style="list-style-type: none"> ◦ Management Zone root Displays the aggregated progress of the new trigger CIs across all of the activities in all of the Management Zones. ◦ Management Zone: Displays the aggregated progress of the new trigger CIs across all of the activities in the selected Management Zones. ◦ Discovery Activity: Displays the progress of the new trigger CIs across the discovery activity. <p>For more details, see "Discovery Progress Dialog Box" on page 670.</p> <ul style="list-style-type: none"> • The information is automatically refreshed every 30 seconds. • Use the information displayed in this pane to drill down to problematic trigger CIs, to uncover specific problems that Universal Discovery encountered during the discovery—for example, incorrect credentials. You can also add newly discovered CIs to the trigger CI list. • Hold the SHIFT and CTRL keys to select adjacent and non-adjacent CIs in a list.

UI Element	Description
Results Tab	<p>Displays the results from discovery activities that ran in the Management Zones, over filterable time periods. The results displayed depend on the area of focus.</p> <p>For more details, see "Discovery Results Tab/Pane" on page 678.</p>

Activity Details Pane

Displayed when you select a discovery activity in the Management Zones tree.

UI Element	Description
Overview Tab	<p>Displays the type and status of the discovery activity, and a summary of the activity as it was defined when it was created. To edit an activity, select the activity in the Management Zones tree, and click the Edit Activity  button.</p>
Activity Jobs Tab	<p>Displays the activity jobs available for the discovery activity.</p> <ul style="list-style-type: none"> • Activity Jobs Toolbar <ul style="list-style-type: none"> ◦  Go to Adapter. Redirects you to the adapter for the selected activity job. ◦  View Permission Details. Opens the Discovery Permissions dialog box, enabling you to view the permissions data for the selected activity job. ◦  View Discovered CITs in Map. Displays the selected adapter, together with its CIs and relationships, in the Discovered CITs Map window. Hold the cursor over a CIT to read a description in a tooltip. ◦  View Parameters. Opens the Activity Job Parameters dialog box, enabling you to view the parameters for the selected activity job. ◦  Edit Script. Displays a list of scripts related to the selected activity job. Select a script and edit it in the Script Editor. ◦  Edit Trigger Query. Displays the trigger query related to the selected activity job, enabling you to open and edit it in the Trigger Query Editor. ◦  Hide/Show Legend. Hides/displays the legend at the bottom of the pane. • Activity Jobs Grid. Displays the information about jobs available for the discovery activity. <ul style="list-style-type: none"> ◦ Activity Job Name. The name of the activity job. ◦ Discovered CITs. The CITs discovered by the activity job.

UI Element	Description
	<ul style="list-style-type: none">○ Protocols. The protocols used by the activity job.○ IPv6 Support. Indicates whether the activity job's adapter supports IPv6.○ Scheduling.<ul style="list-style-type: none">● Activity Schedule indicates that the activity job runs according to the activity's discovery schedule.● For an activity job that does not run according to the activity's discovery schedule, but rather according to its own discovery schedule, displays the job's schedule.● Indicator Icons<p>The following icons indicate the status of the jobs:</p><ul style="list-style-type: none">○  Enabled job. The job is enabled with permissions.○  Enabled job has no credentials. The job is enabled but it is missing credential information.○  Job not enabled. The job is not enabled.

Chapter 14: Module/Job-based Discovery

This chapter includes:

Discovering Running Software	466
Modules/Jobs-based Discovery Overview	467
Viewing Permissions While Running Jobs	467
Discovered CIs and Relationships In a Multi-Tenancy Environment	468
How to Verify Whether a Discovery Job Supports IPv6	470
How to Run Module/Job-based Discovery	470
How to Manually Activate Modules/Jobs/CIs	473
How to Discover Running Software – Scenario	473
How to Define the Owner Tenant For a Discovery Job	476
Module/Job-based Discovery User Interface	477

Discovering Running Software

You can discover software (for example, a specific Oracle database) running in your environment.

This section includes the following topics:

- ["Discovery Process" below](#)
- ["Running Software Default View" on the next page](#)

Discovery Process

The discovery process runs as follows:

- The Host Resources and Host Applications jobs are activated.
- Universal Discovery searches for processes on the machines in your environment.
- Universal Discovery saves the process data (including open port and command line information) to the Probe database.
- The jobs run on this data in the Probe database, build the new RunningSoftware CIs according to

the data in the database, and extract the key attributes from the process data. The jobs send the CIs to the UCMDB Server.

Running Software Default View

A default view displays the mapping of relationships between applications: **Modeling > Modeling Studio > Resources** pane > **Root > Application > Deployed Software**.

To configure Universal Discovery to discover running software, see ["How to Discover Running Software – Scenario" on page 473](#).

Modules/Jobs-based Discovery Overview

You can customize discovery by making changes to an out-of-the-box discovery job or building your own discovery jobs.

For details, see ["How to Run Module/Job-based Discovery" on page 470](#).

For details about the jobs and how they are organized in modules, see the *Universal CMDB Discovery and Integrations Content Guide*.

Viewing Permissions While Running Jobs

During a job run, you often need to know which credentials are being used to connect to a component in the system. You also often need to know the effect of a run on network performance, for example, whether the job should be run at night instead of during the day. View Permissions enables you to view the objects and parameters of a job's Jython script commands, as can be seen in the following image:

Permission	Operation	Usage Description	Objects and Parameters
shellprotocol	exec	Basic login	uname ver
shellprotocol	exec	CPU Info	AIX: lsattr grep "proc" AIX: prtconf grep "proc" FreeBSD: dmesg grep "cpu Multiprocessor" FreeBSD: dmesg grep -A 1 "CPU:" FreeBSD: sysctl hw.model hw.ncpu hw.clockrate HPUX: model Linux: cat /proc/cpuinfo SunOS: /usr/sbin/psrinfo -v SunOS: prtconf Windows: reg query HKEY_LOCAL_MACHINE\HARDWARE\DESCRIP...

Note: The information you define here is not dynamic, that is, if an adapter is changed, the information in this dialog box is not updated.

For details, see "[Discovery Permissions Window](#)" on page 495.

Example of Using the Discovery Permissions Window:

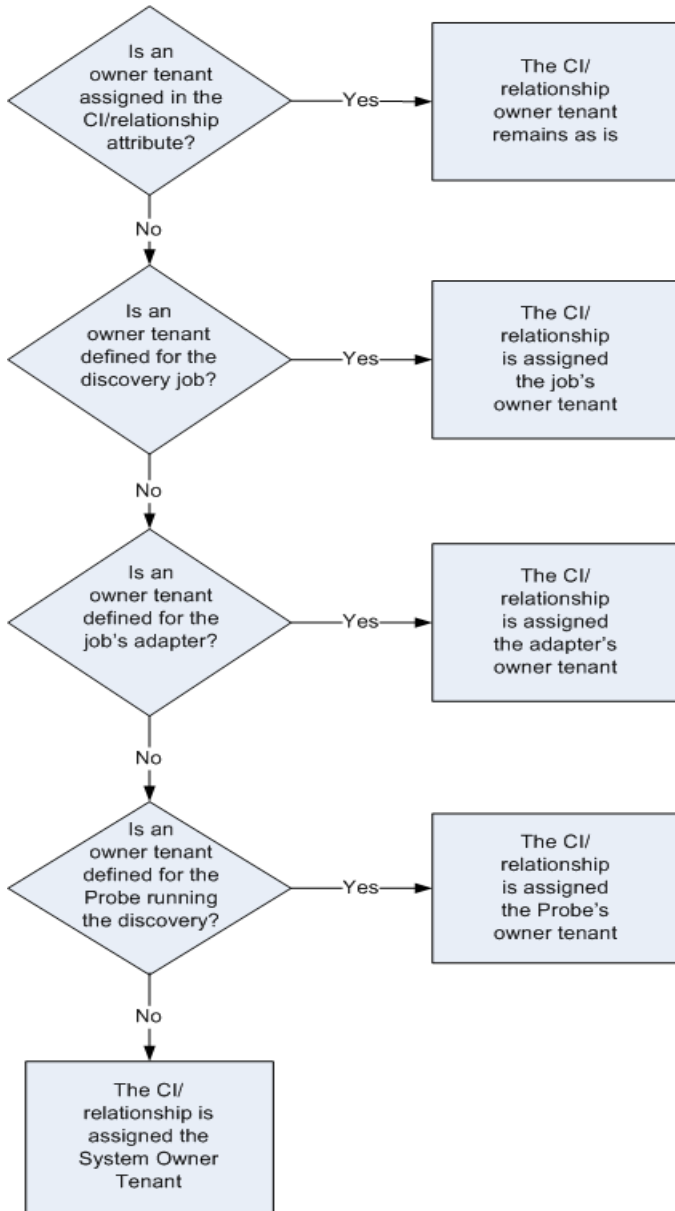
You are running the **Host Connection by Shell** job to discover a host running on a UNIX system. An error message in the Discovery Progress pane shows that Universal Discovery could not access a host through SSH because permission was denied. You display the Discovery Permissions window and see that the command to access the host requires a user with a certain level of permissions. You check the SSH Protocol window and discover that the user defined there does not have that level of permissions.

To resolve the problem, change the user in the SSH protocol or update the permissions for the existing user in the external system.

Discovered CIs and Relationships In a Multi-Tenancy Environment

When discovering data in a multi-tenancy environment, CIs and relationships that are not directly assigned an owner tenant when discovered, are assigned an owner tenant based on the owner tenant defined in the Data Flow Probe properties, discovery adapter parameters, or discovery job properties.

The following diagram illustrates the mechanism used for assigning owner tenant to discovered CIs/relationships:



- For details about assigning an owner tenant to a Data Flow Probe, see ["How to Define Owner Tenants on Data Flow Probes"](#) on page 66.
- For details about assigning an owner tenant to an discovery adapter, see ["How to Define the Owner Tenant Adapter Parameter"](#) on page 228.
- For details about assigning an owner tenant to a discovery job, see ["How to Define the Owner Tenant For a Discovery Job"](#) on page 476.

How to Verify Whether a Discovery Job Supports IPv6

This task describes how you can verify whether or not a particular discovery job or integration supports IPv6. If the adapter used by the job supports IPv6, then the job supports IPv6.

1. Go to **Data Flow Management > Discovery Modules/Jobs**, and select the job.
2. In the Details tab, **IPv6 Support** displays whether or not the job supports IPv6.

Note: The adapter's **Support IPv6** setting controls whether the IPv6 triggers are dispatched to the jobs or not. While this setting can be changed, you must never make such a change for any of the out-of-the-box adapters. If the job does not have the IPv6 support yet, enabling IPv6 support for its adapter will prevent the job from working correctly.

To see a full list of adapters that come packaged out-of-the-box with UCMDDB Content Packs that do support IPv6, see the section describing IPv6 support in the *Universal CMDB Discovery and Integrations Content Guide*.

To change the IPv6 support for a user-defined adapter only:

1. In **Adapter Management**, select the adapter.
2. On the **Adapter Configuration** tab, under **Trigger Dispatch Options**, select (or clear) **Supports IPv6**.

How to Run Module/Job-based Discovery

This task describes how to begin mapping your system and its components. You would use this workflow to customize the components of a module.

Note: For details about running Zone-based discovery, see "[How to Run Zone-based Discovery](#)" on page 428.

This task includes the following steps:

- ["Prerequisites" below](#)
- ["Set up the Data Flow Probes" below](#)
- ["Select and activate the relevant discovery jobs" below](#)
- ["Monitor the discovery process" on the next page](#)
- ["View discovery results" on the next page](#)

1. Prerequisites

- a. Verify that the Data Flow Probe is installed on a Windows machine.

Note: The Data Flow Probe installed on a Linux platform is intended for the CMS Sync integration only, and not for discovery.

- b. Verify that the relevant packages are deployed.

If you need to deploy discovery packages, see [How to Deploy a Package in the *Universal CMDB Administration Guide*](#).

2. Set up the Data Flow Probes

- o **Determine the network range**

Determine the network range of the network to be discovered. For details, see ["New/Edit Range Dialog Box" on page 131](#).

Note: Adapters try to connect to every IP address in a range. Therefore, if a range is wide, network performance may be affected.

- o **Set the relevant credentials**

To enable the Data Flow Probes to connect to servers or applications using specific protocols, you must set the relevant credentials (for example, UD, NTCMD, SNMP, TTY, or WMI). For details on protocol parameters, see the [Universal CMDB Discovery and Integrations Content Guide](#).

Note: The Data Flow Probe tries to connect to a node by using each credential in turn. Universal Discovery then saves the successful credential. The next time the Data Flow Probe connects to this node, it first tries to connect using the successful credential.


3. Select and activate the relevant discovery jobs

Once you have defined the network range and set credentials, you can run discovery on specific jobs. For details on running specific jobs, see *Universal CMDB Discovery and Integrations Content Guide*.

Tip:

- You can view a full description of a selected job in the **Properties tab > Description pane**.
- You can search for all jobs that discover a particular connection type.

For example, to search for all jobs that discover SNMP connections:

In the **Universal Discovery > Discovery Modules/Jobs tab**, click the **Find Job**  button. In the Find Jobs dialog box, enter **SNMP** in the **Name** box and click **Find All**. For details, see ["Find Jobs Dialog Box" on page 499](#).

4. Monitor the discovery process

You can monitor CIs being discovered in the discovery job's Discovery Progress pane, or from the Data Flow Probe Status Window. For details, see:

- ["Discovery Progress Dialog Box" on page 670](#)
- ["Data Flow Probe Status Window" on page 149](#)

You can also create queries to retrieve information about CIs and CITs from the CMDB. For details, see *How to Define a TQL Query in the Universal CMDB Modeling Guide*. If necessary you can trigger queries to manually discover objects. For details, see ["Trigger Queries Pane" on page 493](#).

To view the results of the query, build a subset of the overall IT universe model, a **view**, containing only those CIs in the CMDB that relate to a specific discovery. For details, see *Pattern View Editor in the Universal CMDB Modeling Guide*.

5. View discovery results


You can display overall results for a discovery job or you can filter the results by time range, by Data Flow Probe, or by cluster. Each time you log in to UCMDB and access the Universal Discovery window, the results are updated so that the data displayed is the latest for the selected module or job.

For details on viewing discovery results, see ["Discovery Results Tab/Pane" on page 678](#).



How to Manually Activate Modules/Jobs/CIs

You can manually activate modules/jobs/CIs in the Discovery Modules/Jobs tab.

To manually activate a module/job:

In the Discovery Modules pane, select the module/job, and click **Activate** .

To manually activate a CI:

1. Select the job with the CI you want to activate manually.
2. Disable the Data Flow Probes for the job: In the job's **Properties** tab > **Trigger Queries** pane, select the query, and in the **Probe Limit** column, click the  button and ensure that no Probes are selected.
3. Manually activate CIs: In the **Details** tab, in the **Discovery Progress** pane, click the **Add CI**  button and manually add CIs.

The job runs using only the redispached CIs. For details, see "[Discovery Modules/Jobs – Discovery Modules Pane](#)" on page 482.

How to Discover Running Software – Scenario

This scenario explains how to set up the discovery of Oracle databases so that there is no need to enter a specific set of credentials to discover each database instance. Universal Discovery runs an **extract** command that retrieves the database name attribute.

In this scenario, we assume that the following syntax is used in the Oracle command lines:

```
c:\ora10\bin\oracle.exe UCMDB
```

This task includes the following steps:





- "[Prerequisites](#)" on the next page
- "[Create a Command Line Rule](#)" on the next page

- ["Define the value of an attribute" on the next page](#)
- ["Activate the Job" on page 476](#)

1. Prerequisites

Display the Attribute Assignment Editor dialog box:


- Go to **Data Flow Management > Universal Discovery**.
- In the Discovery Modules/Jobs tab, in the **Discovery Modules** tree, select **Host and Resources > Basic Applications**.
- Select any one of the Host Application jobs, and in the **Properties** tab, select **Global Configuration Files**.

Tip: If you cannot see the Global Configuration Files pane, click the Up arrow [] below the Trigger Queries pane.
- Select **applicationSignature.xml**, and click **Edit**  to open the Software Library dialog box. For details, see ["Software Library Dialog Box" on page 292](#).
- Select the signature to be edited and click **Edit** .
- In the Software Identification Rule Editor dialog box that opens, next to **Additional Attributes**, click  to open the Attributes Assignment Editor dialog box.

2. Create a Command Line Rule

The command line rule is text that identifies the process to be discovered, for example, `oracle.exe c:\ora10\bin\oracle.exe UCMDB`. You can substitute the text entry with a regular expression, so that discovery is more flexible. For example, you can set up a rule that discovers all Oracle databases, whatever their name.

Subsequently, Universal Discovery uses the information in the command lines discovered by the regular expression to populate a CI's name attribute with the database name.

- To create a Command Line rule that includes a regular expression, in the Attributes Assignment Editor dialog box, click the **Add**  button in the Parsing Rules pane. For details, see ["Attributes Assignment Editor Dialog Box" on page 267](#).
- In the Parse Rule Editor dialog box, build the rule:
 - Enter a unique name in the **Rule ID** field: **r1**.
 - In the **Process Attribute** field, select **Command Line**.

- In the **Regular Expression** field, enter the following regular expression:


.+|s+(|w+)\$

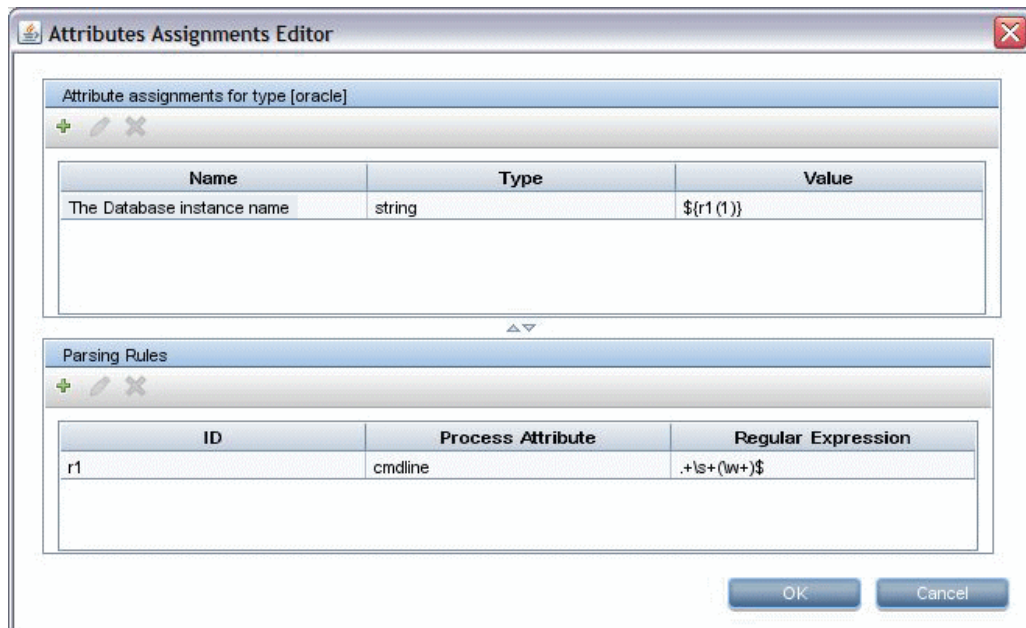
This expression searches for any character (.), followed by a space or spaces (|s+), followed by a word or words (|w+) that appear at the end of the line (\$). You can use the following characters: a-z, A-Z, or 0-9. The following command line fulfills this expression:

c:\ora10\bin\oracle.exe UCMDB

3. Define the value of an attribute

In this step, you define which attribute is used by Universal Discovery to discover the Oracle databases, and the value it should take.

- a. In the Attributes Assignment Editor dialog box, in the Attribute Assignments pane, click **Add**  to select the attribute.
- b. In the Attribute Editor dialog box that opens:
 - Choose the attribute that holds the database name, from the list of Oracle CIT attributes—in this case **The Database instance name**.
 - Enter a value, using the following syntax: **\${<rule ID name>(<group number>)}**, in this case, **\${r1(1)}**.



This dialog box is configured as follows: Universal Discovery enters the value of the first group (**(\w+)**) in the command line regular expression (**(\${r1(1)})**) in the name attribute of the Oracle database CI.

That is, during discovery, Universal Discovery searches through the process files for command lines with a word or words at the end of the line. For example, the following command line matches this regular expression:

```
c:\ora10\bin\oracle.exe UCMDB
```

4. Activate the Job

For details, see ["How to Manually Activate Modules/Jobs/CIs" on page 473](#) and ["Discovery Modules/Jobs – Discovery Modules Pane" on page 482](#).

How to Define the Owner Tenant For a Discovery Job

If you want a discovery job to assign an owner tenant to discovered CIs and relationships other than the owner tenant defined in its adapter's parameters, you can define an override value in the job's properties.

This task describes how to define an override for the owner tenant in the job properties.

Note: This section is relevant for multi-tenancy environments only.

1. Prerequisite

- The owner tenant that you want to define in the discovery job's properties must already be defined in UCMDB. For details on creating owner tenants in UCMDB, see *New Tenant/Edit Tenant Dialog Box* in the *Universal CMDB Administration Guide*.
- An owner tenant parameter must be defined in the adapter that the discovery job uses. For details, see ["How to Define the Owner Tenant Adapter Parameter" on page 228](#).

2. In the Universal Discovery window, click the **Discovery Module/Jobs** tab.

3. Select the discovery job.

4. In the **Properties** tab, in the **Overrides** area, select check box next to the **defaultOwner**

parameter, and enter the name of the owner tenant that is to override the value in the adapter parameter.

5. Click **OK** to save your changes.

Module/Job-based Discovery User Interface

This section includes:

Create New Discovery Job Dialog Box	477
Discovery Modules/Jobs Window	481
Discovery Permissions Window	495
Discovery Scheduler Dialog Box	496
Find Jobs Dialog Box	499
Time Templates Dialog Box	500
Trigger Query Editor Window	501





Create New Discovery Job Dialog Box

Enables you to create a job.

To access	Select Data Flow Management > Universal Discovery > Discovery Modules/Jobs tab > Discovery Modules pane, right-click a module, and select New > Job .
Relevant tasks	<ul style="list-style-type: none">• "How to Run Module/Job-based Discovery" on page 470• "How to Manually Activate Modules/Jobs/CIs" on page 473
See also	<ul style="list-style-type: none">• "Universal Discovery Overview" on page 416• "Modules/Jobs-based Discovery Overview" on page 467

Discovery Job Details Pane

User interface elements are described below:

UI Element (A–Z)	Description
	Opens the Help document related to the selected job's adapter. To update or modify this document, see "Adapter Definition Tab" on page 253 .
	Click to go to the adapter in the Resources pane.
	You can choose to view a map of the CIs and relationships that are discovered by the adapter, instead of a list. Click the button to open the Discovered CITs Map window. The selected adapter is shown together with its CIs and relationships. Hold the cursor over a CIT to read a description in a tooltip.
	Click to view permissions that are defined for specific adapters. For details, see "Discovery Permissions Window" on page 495 . For details on editing these permissions, see "Permission Editor Dialog Box" on page 284 .
Adapter	The adapter used by the job to discover the CIs.
Discovered CIs	The CIs that are discovered by this job.
Input CI Type	The CIT that triggers the CIs for this job.
IPv6 Support	Indicates whether the job's adapter supports IPv6.
Job Name	The name and description of the job and the package in which it is located. <div style="border-left: 2px solid black; padding-left: 10px;"> <p>Note: Naming conventions for jobs:</p> <ul style="list-style-type: none"> • Job names can contain the following characters: a-z, A-Z, 0-9, hyphen (-), underscore (_), space () • Job names must not start with a digit or an underscore (_) </div>
Required Protocols	The protocols needed by the activated job to access the system components.

Parameters Pane

Enables you to override adapter behavior.

To view a description, hold the pointer over the parameter.

To access	Select a job in the Discovery Modules pane in the Universal Discovery window.
Important Information	You can override a default adapter parameter for a specific job, without affecting the default value.



User interface elements are described below:




UI Element (A–Z)	Description									
Name	The name given to the adapter.									
Override	<p>Select to override the parameter value in the adapter.</p> <p>When this check box is selected, you can override the default value. For example, to change the protocolType parameter, select the Override check box and change MicrosoftSQLServer to the new value. Click OK in the Properties tab to save the change:</p> <table border="1" data-bbox="371 699 1198 873"> <thead> <tr> <th colspan="3">Parameters</th> </tr> <tr> <th>Override</th> <th>Name</th> <th>Value</th> </tr> </thead> <tbody> <tr> <td><input checked="" type="checkbox"/></td> <td>protocolType</td> <td>MicrosoftSQLServer</td> </tr> </tbody> </table> <p>For details on editing parameters in the Adapter Parameters pane, see "Adapter Definition Tab" on page 253.</p>	Parameters			Override	Name	Value	<input checked="" type="checkbox"/>	protocolType	MicrosoftSQLServer
Parameters										
Override	Name	Value								
<input checked="" type="checkbox"/>	protocolType	MicrosoftSQLServer								
Value	The value defined in the adapter.									

Trigger Queries Pane

Enables you to define one or more queries to be used as triggers to activate the selected job.


User interface elements are described below:

UI Element (A–Z)	Description
	<p>Add Query. Opens the Choose Discovery Query dialog box, enabling you to add one or more non-default TQL queries to be used as triggers to activate the selected job.</p> <p>The Choose Discovery Query dialog box lists available queries for the job. Select a query to displayed it in the Query Preview pane. Hold the cursor over an TQL element to view details.</p>
	<p>Remove Query. Removes the selected query.</p> <p>Note:</p> <ul style="list-style-type: none"> No message is displayed. To restore the query, click the Cancel button.

UI Element (A–Z)	Description
	<ul style="list-style-type: none"> If a query is removed for an active job, Discovery no longer receives new CIs coming from that query. Existing Trigger CIs that originally came from the query are not removed.
	Opens the Trigger Query Editor . For details, see " Trigger Query Editor Window " on page 501 . Available: In the job's Properties tab only.
	Opens the Modeling Studio. Available: In the job's Properties tab only.
Probe Limit	The Probes/clusters used for the query. Click the  button to open the Edit Probe Limitation for Query Output dialog box where can select the Probes/clusters on which the trigger query should run.
Query Name	The name of the Trigger query that activates the job.

Global Configuration Files Pane


User interface elements are described below:

UI Element (A–Z)	Description
	Edit. Opens the selected configuration file in an appropriate editor. For example, the file msServerTypes.xml opens the Script Editor.

Discovery Scheduler Pane

Enables you to set up a schedule for this job.

User interface elements are described below:

UI Element (A–Z)	Description
	Click to add times to the Allow Discovery to run at list. The Time Templates dialog box opens. To add a time template to the list, in the Time Templates dialog box, click the Add

UI Element (A–Z)	Description
	button to open the Edit Time Template dialog box. For details, see "Time Templates Dialog Box" on page 500 .
Allow Discovery to run at	Choose a template that includes the days and times when the job should run.
Edit scheduler	Click to open the Discovery Scheduler . For details, see "Discovery Scheduler Dialog Box" on page 496 .
Invoke on new triggered CIs immediately	Enables the job to run as soon as the Trigger CI reaches the Probe. When this option is not selected, the job runs according to the schedule defined in the Schedule Manager . Note: If this option is not selected and a job is running, new triggered CIs are not run by the job. Although new triggered CIs are not run, they are counted into the status bar. This means the status bar does not reach 100% completed, even though the job successfully completed, and the user has to wait until the next run of the job for the status bar to reach 100% completed.

Discovery Modules/Jobs Window

Enables you to view and manage modules and jobs, to activate jobs, and to follow job progress.

To access	Select Data Flow Management > Universal Discovery > Discovery Modules/Jobs tab.
Important information	<ul style="list-style-type: none"> This tab is suitable for advanced users of Universal Discovery only. Each change you make in the Universal Discovery window is delivered to and stored in the CMDB. From there, the changes are sent to the Probe. You can verify that changes have been sent to the Probe by opening the wrapperProbe.log file located in C:\hp\UCMDB\DataFlowProbe\runtime\logs\ and searching for the following lines: <pre>processing document domainScopeDocument.xml Processing document domainScopeDocument.xml is done.</pre>
Relevant tasks	<ul style="list-style-type: none"> "How to Run Module/Job-based Discovery" on page 470 "How to Manually Activate Modules/Jobs/CIs" on page 473

See also	<ul style="list-style-type: none"> • "Universal Discovery Overview" on page 416 • "Modules/Jobs-based Discovery Overview" on page 467
-----------------	---

User interface elements are described below:



UI Element (A–Z)	Description
Dependency Map tab	Displays a visual representation of the real-time progress of the process. For details, see "Discovery Module/Jobs – Dependency Map Tab" on page 489 .
Details tab	Enables you to manage a module's CIs and view CI statistics. For details, see "Discovery Module/Jobs – Details Tab" on page 486 .
Discovery Modules pane	Each module includes jobs. You activate a module or job to discover a specific group of CIs. For details, see "Discovery Modules/Jobs – Discovery Modules Pane" below .
Properties tab	Enables you to view and administer the properties of modules and jobs. For details, see "Discovery Modules/Jobs – Properties Tab" on page 490 .








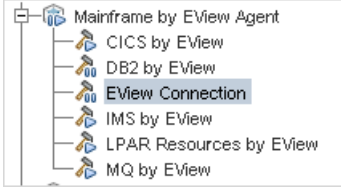

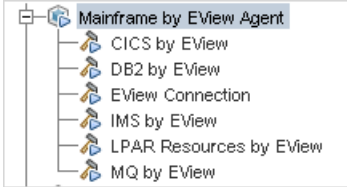



Discovery Modules/Jobs – Discovery Modules Pane


Enables you to view and manually manage modules and jobs. Each module includes the jobs necessary to discover specific CIs.

To access	Select Data Flow Management > Universal Discovery > Discovery Modules/Jobs tab.
Relevant tasks	<ul style="list-style-type: none"> • "How to Run Module/Job-based Discovery" on page 470 • "How to Manually Activate Modules/Jobs/CIs" on page 473
See also	<ul style="list-style-type: none"> • "Universal Discovery Overview" on page 416 • "Modules/Jobs-based Discovery Overview" on page 467






User interface elements are described below:







UI Element (A–Z)	Description
	Create New Job/Module. Enables you to create a discovery job or module for discovery jobs.
	Delete Selected Item. Removes the selected item from the modules/jobs tree.




UI Element (A–Z)	Description
	Find Job. Click to open the Find Jobs dialog box. For example, to search for all jobs that discover SNMP connections, in the Find Jobs dialog box, enter SNMP in the Name box and click Find All . For details, see " Find Jobs Dialog Box " on page 499.
	Refresh All. Updates the modules.
	Activate Selected Discovery Jobs. You can run one job or several jobs in a module, and one or several modules. Select the jobs or modules and click Activate .
	Deactivate Selected Discovery Jobs. Select the jobs or modules to be stopped and click Deactivate .
	Represents the module root. To create a module, right-click to enter the name of the module you are creating. Note: A name is case sensitive. Names beginning with an upper case letter appear in the Discovery Modules list before names beginning with a lower case letter.
	Represents a module. <ul style="list-style-type: none">  . Indicates that some of a module's jobs are activated.   . Indicates that all of a module's jobs are activated. 
	Represents a job. <ul style="list-style-type: none">  . Indicates that the job is active.  . Indicates that the job is paused. To view an adapter description, hold the pointer over the icon.

UI Element (A–Z)	Description
	Jobs contain configuration information derived from adapters and other resources and are the entities controlled by users, for example, when activating or deactivating a module. For details on the right-click menu, see "Right-Click Menu" below .
	An exclamation mark signifies that one or more of the jobs is experiencing a problem that could affect the discovery process, for example, a protocol connection failure. To view the reason for the problem, click the (show errors) link in the Discovery Progress pane. For details, see "Discovery Module/Jobs – Details Tab" on page 486 . Note: If a problem is resolved by clicking the Refresh All button, the Problem Indicator disappears.

Right-Click Menu

UI Element (A–Z)	Description
 Activate	Module: Runs the jobs in the selected module. Job: Runs the selected jobs The Discovery Module discovers CITs and relationships of the types that are described in each job, and places them in the CMDB. For example, the Class C IPs by ICMP job discovers the Dependency , IpAddress , and Membership CITs and relationships.
 Clear Probe Results Cache	Clears the results cache on the Probes. Note: If the results cache is cleared, all discovery results are sent again the next time the jobs run.
 Content Help	Opens the Help document related to the selected job's adapter. To update or modify this document, see "Adapter Definition Tab" on page 253 . To see the full <i>Universal CMDB Discovery and Integrations Content Guide</i> , select Help > Discovery and Integrations Content Help .
 Create New > Job	Opens the Create New Discovery Job dialog box, enabling you to create a job. For details, see "Create New Discovery Job Dialog Box" on page 477 .
 Create New > Module	Enables you to define a new name for the module root. Note: Naming conventions for modules: <ul style="list-style-type: none"> • Module names can contain the following characters: a-z, A-Z, 0-9,

UI Element (A–Z)	Description
	<p>hyphen (-), underscore (_), space (), and forward slash (/)</p> <ul style="list-style-type: none"> • Module names must not start with a digit • Module names must be limited to a length of 50 characters
 Deactivate	<p>Module: Stops the running jobs in the selected module.</p> <p>Job: Stops the selected running jobs.</p> <p>Note: To stop all the running jobs simultaneously, right-click the Discovery Modules root folder and click Deactivate all jobs.</p>
 Delete	<p>Enables you to delete the selected module.</p> <p>Caution: Only administrators with an expert knowledge of the Universal Discovery process should delete modules.</p>
 Delete job	<p>Enables you to delete the selected job.</p>
 Edit Scheduling	<p>Opens the Discovery Scheduler to define a schedule for the selected job.</p>
Edit Script	<p>Enables you to select and edit one of the selected job's scripts.</p>
 Go to adapter	<p>Opens the details of the selected adapter in the Adapter Management module, enabling you to view and edit its definition.</p>
Move to	<p>Enables you to move the selected module folder or job to a different folder.</p>
 Pause	<p>Click to pause an active job.</p> <p>To pause all active jobs simultaneously, right-click the Discovery Modules root folder and click Pause jobs.</p> <p>Note:</p> <ul style="list-style-type: none"> • When you pause an active job: <ul style="list-style-type: none"> ◦ triggers that are currently running continue to run until they are finished ◦ all the execution information is retained, including errors • Jobs are paused based on their defined job execution policies. For details, see "Job Execution Policies" on page 36.
Rename	<p>Enables you to enter a new display name for the selected module.</p> <p>Available: When you right-click a module</p>
Rename Job	<p>Opens the Rename Job dialog box, enabling you to enter a new display name for the job.</p>

UI Element (A–Z)	Description
	<p>Note: You cannot rename active jobs.</p> <p>Available: When you right-click a job</p>
 Rerun Discovery	Reruns the selected job using the selected Trigger CIs.
 Resume	<p>Enables you to resume a paused job.</p> <p>To resume all paused jobs simultaneously, right-click the Discovery Modules root folder and click Resume jobs.</p>
 Save as...	Enables you to clone the selected job.

Discovery Module/Jobs – Details Tab

Enables you to view and administer modules and jobs, to follow the progress of the DFM process, and to manage errors during discovery.





To access	Select Universal Discovery > Discovery Modules/Jobs tab > Discovery Modules pane > a module/job > Details tab.
Important Information	<p>Depending which level you select in the Discovery Modules pane on the left, different information is displayed in the Details tab.</p> <p>If you select:</p> <ul style="list-style-type: none"> • The Discovery Module root or a module, the following panes display information and statistics about all active jobs and errors discovered during a run: <ul style="list-style-type: none"> ◦ "Progress Pane" ◦ "Results Pane" • A job, the following is displayed: <ul style="list-style-type: none"> ◦ "Discovery Job Details Pane" ◦ "Progress Pane" ◦ "Results Pane" • Several jobs or modules, the following is displayed: <ul style="list-style-type: none"> ◦ "Selected Items Pane"
Relevant tasks	<ul style="list-style-type: none"> • "How to Run Module/Job-based Discovery" on page 470 • "How to Manually Activate Modules/Jobs/CIs" on page 473

See also	<ul style="list-style-type: none"> • "Universal Discovery Overview" on page 416 • "Modules/Jobs-based Discovery Overview" on page 467 • "Error Messages Overview" in the <i>Universal CMDB Developer Reference Guide</i>
-----------------	---

Discovery Job Details Pane

Important information	Displayed when a job is selected in the Discovery Modules pane on the left.
------------------------------	---

User interface elements are described below:

UI Element (A–Z)	Description
	<p>Opens the Help document related to the selected job's adapter.</p> <p>To update or modify this document, see "Adapter Definition Tab" on page 253.</p>
	Click to go to the adapter in the Resources pane.
	<p>You can choose to view a map of the CIs and relationships that are discovered by the adapter, instead of a list. Click the button to open the Discovered CITs Map window. The selected adapter is shown together with its CIs and relationships. Hold the cursor over a CIT to read a description in a tooltip.</p>
	<p>Click to view permissions that are defined for specific adapters. For details, see "Discovery Permissions Window" on page 495.</p> <p>For details on editing these permissions, see "Permission Editor Dialog Box" on page 284.</p>
Adapter	The adapter used by the job to discover the CIs.
Discovered CIs	The CIs that are discovered by this job.
Input CI Type	The CIT that triggers the CIs for this job.
IPv6 Support	Indicates whether the job's adapter supports IPv6.
Job Name	<p>The name and description of the job and the package in which it is located.</p> <p>Note: Naming conventions for jobs:</p> <ul style="list-style-type: none"> • Job names can contain the following characters: a-z, A-Z, 0-9, hyphen (-), underscore (_), space () • Job names must not start with a digit or an underscore (_)

UI Element (A–Z)	Description
Required Protocols	The protocols needed by the activated job to access the system components.

Results Pane

Displays the discovery results from discovery job runs. For details, see ["Discovery Results Tab/Pane" on page 678](#).

Progress Pane

Displays the discovery progress. For details, see ["Discovery Progress Dialog Box" on page 670](#).

Selected Items Pane

User interface elements are described below (unlabeled elements are shown in angle brackets):

UI Element (A–Z)	Description
<right-click menu>	Edit Scheduling. Click to open the Discovery Scheduler to define a schedule for a specific job. For details, see "Discovery Scheduler Pane" on page 494 .
Invoke immediately	<ul style="list-style-type: none"> A check mark signifies that the DFM job runs as soon as the triggered CI reaches the Probe. In this case, the Invoke on new triggered CIs immediately check box is selected in the Properties tab. If this column does not contain a check mark, the job runs according to the schedule defined in the Schedule Manager.
Job name	The name of the job.
Schedule info	The scheduling information of the job as defined in the Discovery Scheduler .
Trigger Queries	The name of the query that activated the job. For details, see "Trigger Queries Pane" on page 493 .

Discovery Module/Jobs – Dependency Map Tab

Displays a visual representation of the real-time progress of the discovery process. The map displays CIs that were triggered by a job, and CIs that were discovered as a result of the activated job.

To access	Select Universal Discovery > Discovery Modules/Jobs tab > Discovery Modules pane > a module/job> Dependency Map tab.
Important Information	<p>Depending which node you select in the Discovery Modules pane, different information is displayed in the Dependency Map tab.</p> <p>If you select:</p> <ul style="list-style-type: none"> ○ The Discovery Modules root, and select the Show only active Discovery jobs check box, the Dependency Map displays only active jobs and their interdependencies. ○ The Discovery Modules root, and clear the Show only active Discovery jobs check box, the Dependency Map displays all discovery jobs and their interdependencies. ○ A module, a topology map is displayed showing the module's active and inactive jobs. ○ A job, the topology map highlights the job in the module's map.
Relevant tasks	<ul style="list-style-type: none"> ○ "How to Run Module/Job-based Discovery" on page 470 ○ "How to Manually Activate Modules/Jobs/CIs" on page 473
See also	<ul style="list-style-type: none"> ○ "Universal Discovery Overview" on page 416 ○ "Modules/Jobs-based Discovery Overview" on page 467 ○ "Discovered/Created/Last Updated CIs Dialog Box" on page 668

User interface elements are described below (unlabeled elements are shown in angle brackets):

UI Element (A-Z)	Description
<right-click menu>	<p>Use the right-click menu to view details for a job, CI, or link, for example, the number of CI instances (of a specific type) in the CMDB or the number of CI instances created by a specific job.</p> <p>Depending on which object is selected, the following menu options are displayed:</p> <ul style="list-style-type: none"> • When a job is selected: <ul style="list-style-type: none"> ○ Show discovered CIs. Click to view the CIs discovered by the job. To filter the query, select a CIT from the menu.

UI Element (A-Z)	Description
	<p>Show trigger CIs. Click to view the CIs that triggered the job.</p> <ul style="list-style-type: none"> When a CI is selected: <p>Show all CIT instances. Click to view all CIs of this CI type.</p> <ul style="list-style-type: none"> When a link from a CI to a job is selected: <p>Show trigger CIs for job. Click to view CIs (of the selected type) that triggered the job.</p> <ul style="list-style-type: none"> When a link from a job to a CI is selected: <p>Show discovered instances. Click to view CIs (of the selected type) that were discovered by the job.</p>
<Toolbar>	For a description of the icons, see "Toolbar Options" in the <i>Universal CMDB Modeling Guide</i> .
<Tooltip>	Hold the pointer over a CI or job to display a description.
Show only active Discovery jobs	<p>When the Discovery Modules root is selected in the Discovery Modules pane, this check box is displayed.</p> <p>Select to display all active jobs (from any module).</p>

Discovery Modules/Jobs – Properties Tab

Enables you to view and administer the properties of modules and jobs.




To access	Select Universal Discovery > Discovery Modules/Jobs tab > Discovery Modules pane > a module/job > Properties tab.
Important Information	<p>Depending which level you select in the Discovery Modules pane, different information is displayed in the Properties tab.</p> <p>If you select:</p> <ul style="list-style-type: none"> The Discovery Modules root, all active jobs are displayed with scheduling information. Click any of the columns to sort the list by that column. Right-click a job to edit its scheduling. For details, see "Discovery Scheduler Dialog Box" on page 496. A Discovery module, the Description and Module Jobs panes are displayed. To edit a description, make changes in the Description pane and click OK. See also "Module Jobs Pane" on the next page. A job, the Parameters, Trigger Queries, Global Configuration Files, and

	Discovery Scheduler panes are displayed. For details, see below.
Relevant tasks	<ul style="list-style-type: none"> • "How to Run Module/Job-based Discovery" on page 470 • "How to Manually Activate Modules/Jobs/CIs" on page 473
See also	<ul style="list-style-type: none"> • "Universal Discovery Overview" on page 416 • "Modules/Jobs-based Discovery Overview" on page 467

Module Jobs Pane

Enables you to view the active jobs for the selected module.

User interface elements are described below:

UI Element (A–Z)	Description
	Add Discovery Job to Module. Opens the Choose Discovery Jobs dialog box where you can select jobs from more than one zip file. (Hold the SHIFT or CTRL keys to select several jobs.)
	Remove Selected Discovery Job from Module. Select the job and click the button. (No message is displayed. To restore the job, click the Cancel button.)
	Show discovered CITs as a map. You can choose to view a map of the CIs and links that are discovered by the adapter, instead of a list. Click the button to open the Discovered CITs Map window. The selected adapter is shown together with its CIs and relationships. Hold the cursor over a CIT to read a description in a tooltip.
<Column heading>	<ul style="list-style-type: none"> • Click a column heading to change the order of the CITs from ascending to descending order, or vice versa. • Click a column heading and drag the column to a different location in the table columns. • Right-click a column heading to customize the table. Choose from the following options: <ul style="list-style-type: none"> ◦ Hide Column. Select to hide a specific column. ◦ Show All Columns. Displayed when a column is hidden. ◦ Select Columns. Select to display or hide columns and to change the order of the columns in the table. Opens the Columns dialog box. ◦ Auto-resize Column. Select to change a column width to fit the contents. For details, see Select Columns Dialog Box in the <i>Universal CMDB Modeling Guide</i>.
<List of	All jobs included in the module. (Displayed when a specific module is selected in the

UI Element (A–Z)	Description
jobs>	Discovery Modules pane.) Right-click a row to open the Discovery Scheduler for the selected job. For details, see " Discovery Scheduler Dialog Box " on page 496.
Invoke Immediately	<ul style="list-style-type: none"> • A check mark signifies that the Discovery job runs as soon as the triggered CI reaches the Probe. In this case, the Invoke on new triggered CIs immediately check box is selected in the Properties tab. • If this column does not contain a check mark, the job runs according to the schedule defined in the Schedule Manager.
Job Name	The name of the job and the package in which the job is included. (Displayed when a job is selected in the Discovery Modules pane.)
Schedule Information	The scheduling information of the job as defined in the Discovery Scheduler .
Trigger Queries	The name of the query that activated the job.

Parameters Pane

Enables you to override adapter behavior.

To view a description, hold the pointer over the parameter.

To access	Select a job in the Discovery Modules pane in the Universal Discovery window.
Important Information	You can override a default adapter parameter for a specific job, without affecting the default value.

User interface elements are described below:




UI Element (A–Z)	Description
Name	The name given to the adapter.
Override	Select to override the parameter value in the adapter. When this check box is selected, you can override the default value. For example, to change the protocolType parameter, select the Override check box and change



UI Element (A–Z)	Description									
	<p>MicrosoftSQLServer to the new value. Click OK in the Properties tab to save the change:</p> <table border="1"> <thead> <tr> <th colspan="3">Parameters</th> </tr> <tr> <th>Override</th> <th>Name</th> <th>Value</th> </tr> </thead> <tbody> <tr> <td><input checked="" type="checkbox"/></td> <td>protocolType</td> <td>MicrosoftSQLServer</td> </tr> </tbody> </table> <p>For details on editing parameters in the Adapter Parameters pane, see "Adapter Definition Tab" on page 253.</p>	Parameters			Override	Name	Value	<input checked="" type="checkbox"/>	protocolType	MicrosoftSQLServer
Parameters										
Override	Name	Value								
<input checked="" type="checkbox"/>	protocolType	MicrosoftSQLServer								
Value	The value defined in the adapter.									

Trigger Queries Pane

Enables you to define one or more queries to be used as triggers to activate the selected job.

User interface elements are described below:


UI Element (A–Z)	Description
	<p>Add Query. Opens the Choose Discovery Query dialog box, enabling you to add one or more non-default TQL queries to be used as triggers to activate the selected job.</p> <p>The Choose Discovery Query dialog box lists available queries for the job. Select a query to displayed it in the Query Preview pane. Hold the cursor over an TQL element to view details.</p>
	<p>Remove Query. Removes the selected query.</p> <p>Note:</p> <ul style="list-style-type: none"> No message is displayed. To restore the query, click the Cancel button. If a query is removed for an active job, Discovery no longer receives new CIs coming from that query. Existing Trigger CIs that originally came from the query are not removed.
	<p>Opens the Trigger Query Editor. For details, see "Trigger Query Editor Window" on page 501.</p> <p>Available: In the job's Properties tab only.</p>

UI Element (A–Z)	Description
	Opens the Modeling Studio. Available: In the job's Properties tab only.
Probe Limit	The Probes/clusters used for the query. Click the  button to open the Edit Probe Limitation for Query Output dialog box where can select the Probes/clusters on which the trigger query should run.
Query Name	The name of the Trigger query that activates the job.

Global Configuration Files Pane

Lists the global configuration files defined for the adapter used by the selected job.


User interface elements are described below:

UI Element (A–Z)	Description
	Edit. Opens the selected configuration file in an appropriate editor. For example, the file msServerTypes.xml opens the Script Editor.

Discovery Scheduler Pane

Enables you to view information about the schedule set up for the selected job.

User interface elements are described below:

UI Element (A–Z)	Description
	Click to add times to the Allow Discovery to run at list. The Time Templates dialog box opens. To add a time template to the list, in the Time Templates dialog box, click the Add button to open the Edit Time Template dialog box. For details, see " Time Templates Dialog Box " on page 500.
Allow Discovery to run at	Choose a template that includes the days and times when the job should run.


UI Element (A–Z)	Description
Edit scheduler	Click to open the Discovery Scheduler . For details, see " Discovery Scheduler Dialog Box " on the next page.
Invoke on new triggered CIs immediately	<p>Enables the job to run as soon as the Trigger CI reaches the Probe.</p> <p>When this option is not selected, the job runs according to the schedule defined in the Schedule Manager.</p> <p>Note: If this option is not selected and a job is running, new triggered CIs are not run by the job.</p> <p>Although new triggered CIs are not run, they are counted into the status bar. This means the status bar does not reach 100% completed, even though the job successfully completed, and the user has to wait until the next run of the job for the status bar to reach 100% completed.</p>

Discovery Permissions Window

Enables you to view permissions data for jobs.

To access	Select Data Flow Management > Universal Discovery > Discovery Module/Jobs tab > a job > Details tab > Discovery Job Details pane , and click the View Permissions button.
See also	<ul style="list-style-type: none"> • "Viewing Permissions While Running Jobs" on page 467 • "Adapter Definition Tab" on page 253 • "Permission Editor Dialog Box" on page 284
Relevant tasks	<ul style="list-style-type: none"> • "How to Run Module/Job-based Discovery" on page 470 • "How to Manually Activate Modules/Jobs/CIs" on page 473
See also	<ul style="list-style-type: none"> • "Universal Discovery Overview" on page 416 • "Modules/Jobs-based Discovery Overview" on page 467 • "Viewing Permissions While Running Jobs" on page 467 • "Adapter Definition Tab" on page 253 • "Permission Editor Dialog Box" on page 284

User interface elements are described below:

UI Element (A-Z)	Description
	Export a permission object in Excel, PDF, RTF, CSV, or XML format. For details, see "Browse Views Mode" in the <i>Universal CMDB Modeling Guide</i> .
Objects and Parameters	The commands that appear in the relevant Jython scripts.
Operation	The action that is being run.
Permission	The name of the protocol as defined for the job.
Usage Description	A description of how the protocol is used.






Discovery Scheduler Dialog Box





Enables you to define a schedule for a specific job, for example, every day Data Flow Management starts running an IP ping sweep on Class C networks at 6:00 AM.

To access	<p>Use one of the following:</p> <ul style="list-style-type: none"> • Right-click a job and select Edit scheduling. • Select Universal Discovery > Discovery Modules/Jobs tab > a job > Properties tab > Discovery Scheduler pane, and click the Edit Scheduler button.
Important Information	<ul style="list-style-type: none"> • The Discovery Scheduler defines the frequency of the discovery (daily, monthly) whereas the time template defines when the job should run (during the day, at night, at weekends only). You can run the same schedule with different time templates. For example, you can define a schedule that runs every day and you can define a time template that runs at night from 01:00 AM to 05:00 AM. A job defined in this way runs every day from 01:00 AM to 05:00 AM. You can define a second time template to run at a different time, and you also can use this time template with the same schedule. • If you change a schedule for a job, DFM next runs the job according to the following calculation: The current date and time plus the selected interval. For example, if you choose Once, the Invocation Time is in one hour. <p>For details on creating a time template, see "Time Templates Dialog Box" on page 500.</p>
Relevant tasks	<ul style="list-style-type: none"> • "How to Run Module/Job-based Discovery" on page 470 • "How to Manually Activate Modules/Jobs/CIs" on page 473
See also	<ul style="list-style-type: none"> • "Universal Discovery Overview" on page 416

- ["Modules/Jobs-based Discovery Overview" on page 467](#)

User interface elements are described below (unlabeled elements are shown in angle brackets):


UI Element (A–Z)	Description
	<p>(Appears when you select Cron). Click to validate the Cron expression you entered.</p> <p>For descriptions and samples of Cron expressions, see "Cron Expressions" in the <i>Universal CMDB Modeling Guide</i>.</p>
Cron Expression	<p>(Appears when you select Cron). Enter a Cron expression in the proper format. For a description of the fields used in Cron expressions and examples of how to use them, see Cron Expressions in the <i>Universal CMDB Modeling Guide</i>.</p>
<Days of month>	<p>(Displayed when you select Monthly.) Click the  button to choose the days of the month on which the action must run. The Select Days dialog box opens. Choose the required days by selecting the check boxes. You can select multiple days.</p> <ul style="list-style-type: none"> •  Select All. Select all the days. •  Clear Selection. Clear all the selected days. •  Invert Selection. Switch the selection.
<Days of the week> (Sunday - Saturday)	<p>(Appears when you select Weekly.) Select the day or days on which the action should run.</p>
<Schedule options>	<ul style="list-style-type: none"> • Once. Define the task to run only once. • Interval. Defines the interval between successive runs. • Daily. Run a task on a daily basis. • Weekly. Run a task on a weekly basis. • Monthly. Run a task on a monthly basis. • Cron. Enter a Cron expression in the correct format.
<Months of the year> (January - December)	<p>(Displayed when you select Monthly.) Select the month or months in which the action must run.</p>
End by	<p>(Does not appear when you select Once). Select the date and time when the action should stop running by selecting the End by check box, opening the calendar, selecting the date and time, and clicking OK.</p> <p>Note: This step is optional. If you do not need to specify an ending date, leave the End by check box cleared.</p>

UI Element (A–Z)	Description
Invocation hour	<p>(Appears when you select Daily, Weekly, or Monthly.) Select the time to activate the action. Click the  button to open the Select Hours dialog box. Choose the required time by selecting the check boxes. You can select multiple times.</p> <ul style="list-style-type: none"> •  Select All. Select all the times. •  Clear Selection. Clear all the selected times. •  Invert Selection. Switch the selection. <p>Note: You can also enter the time manually in the Invocation hour box. Separate times by a comma and enter AM or PM after the hour. The manually entered action times are not restricted to the hour and half hour only: you can assign any hour and minute combination. Use the following format: HH:MM AM, for example, 8:15 AM, 11:59 PM.</p>
Invocation Time	<p>(Appears when you select Once.) Choose the date and time the action should begin running by opening the calendar and choosing a date and time, or accept the default.</p>
Repeat every	<p>(Appears when you select Interval.) Select how often the action runs.</p> <p>Type a value for the interval between successive runs and choose the required unit of time (minutes, hours, or days).</p> <p>Note: After each change, the next time that the job runs is the current time plus the interval, that is, the job does not start immediately.</p>
Start at	<p>(Does not appear when you select Once.) Choose the date and time when the action must begin running by selecting the Start at check box, opening the calendar, selecting the date and time, and clicking OK.</p> <p>Note:</p> <ul style="list-style-type: none"> • When selecting the start time, the time zone in the start time is set according to the client machine's location, although it may not match the value selected in Time Zone. • This step is optional. If you do not want to specify a beginning time, leave the Start at check box unselected.
Time zone	<p>Select the time zone according to which the Probe must schedule jobs.</p>


UI Element (A–Z)	Description
	<p>The default is <<Data Flow Probe Time Zone>>: the Probe uses its own system-defined time zone. This enables scheduling to take place at different times in different geographical locations.</p> <p>For all Probes to start working at the same time, select a specific time zone. (This assumes that the Probes' system date/time and time zone are correctly configured.)</p>

Find Jobs Dialog Box

Enables you to search for jobs answering to specific criteria. The results of the search are displayed in the Selected Items pane in the Details tab.


To access	Click the Find Job  button in the Discovery Modules pane.
Relevant tasks	<ul style="list-style-type: none"> • "How to View Job Information on the Data Flow Probe" on page 147 • "How to Find Discovery Errors" on page 661 • "How to Run Module/Job-based Discovery" on page 470 • "How to Manually Activate Modules/Jobs/CIs" on page 473
See also	<ul style="list-style-type: none"> • "Universal Discovery Overview" on page 416 • "Modules/Jobs-based Discovery Overview" on page 467

User interface elements are described below:




UI Element (A–Z)	Description
Direction	Searches forwards or backwards through the modules.
Find All	All jobs meeting the search criteria are highlighted.
Find Discovery job by	<p>Choose between:</p> <ul style="list-style-type: none"> • Name. Enter the name of the job or part of it. • Input type. CIs that triggered the job. Click the  button to open the CI type list. Locate the CI type that you are searching for. • Output type. CIs that are discovered as a result of the activated job.
Find Next	The next job meeting the search criteria is highlighted.

Time Templates Dialog Box

Enables you to define a daily or weekly schedule to run selected jobs.

To access	Select Universal Discovery > Discovery Modules/Jobs tab > a job > Properties tab > Discovery Scheduler pane, and click the Time Template  button.
Relevant tasks	<ul style="list-style-type: none"> • "How to Run Module/Job-based Discovery" on page 470 • "How to Manually Activate Modules/Jobs/CIs" on page 473
See also	<ul style="list-style-type: none"> • "Universal Discovery Overview" on page 416 • "Modules/Jobs-based Discovery Overview" on page 467 • "Discovery Scheduler Dialog Box" on page 496

User interface elements are described below:

UI Element (A–Z)	Description
	<p>Add new job execution template. Opens the Edit Time Template dialog box, enabling you to add a time template:</p> <ul style="list-style-type: none"> • Time Template. A unique name for the time template. <p>Note: The name of the time template must be unique.</p> • Every day between. Enables you to define a daily schedule for the job execution. You can define any hour and minute combination. • Week Time. Enables you to define a weekly schedule for the job execution. Select this option to select a time in the Time Definition grid. To select adjacent cells in the grid, click and drag the mouse over the grid. To clear a time, click the selected cell in the grid a second time.
	<p>Remove job execution template. Removes the selected time template.</p>
	<p>Edit job execution template. Select a time template and click to edit it. Opens the Edit Time Template dialog box.</p>

Trigger Query Editor Window

Enables you to edit a TQL query that has been defined to trigger jobs.

To access	Select Data Flow Management > Universal Discovery > Discovery Modules/Jobs tab > Properties tab > Trigger Queries pane > a TQL query, and click the Open the Query Editor button.
Important Information	A Trigger query associated with a job is a subset of the Input query, and defines which specific CIs should be the Trigger CIs for a job. That is, if an Input query queries for IPs running SNMP, a Trigger query queries for IPs running SNMP in the range 195.0.0.0-195.0.0.10.
Relevant tasks	<ul style="list-style-type: none"> • "How to Run Module/Job-based Discovery" on page 470 • "How to Manually Activate Modules/Jobs/CIs" on page 473
See also	<ul style="list-style-type: none"> • "Universal Discovery Overview" on page 416 • "Modules/Jobs-based Discovery Overview" on page 467 • "Trigger CIs and Trigger Queries" on page 27

User interface elements are described below (unlabeled elements are shown in angle brackets):

UI Element (A–Z)	Description
<Panels>	<ul style="list-style-type: none"> • "CI Type Selector Pane" below • "Editing Pane" on the next page • "Information Pane" on the next page
Query Name	The name of the Trigger query that activates the job.

CI Type Selector Pane

Displays a hierarchical tree structure of the CI Types found in the CMDB. For more details, see CI Type Manager User Interface in the *Universal CMDB Modeling Guide*.

Note: The number of instances of each CIT in the CMDB is displayed to the right of each CIT.

Important Information	To create or modify a TQL query, click and drag nodes to the Editing pane and define the relationship between them. Your changes are saved to the CMDB. For details, see How to Add Query Nodes and Relationships to a TQL Query in the <i>Universal</i>
------------------------------	--

	<i>CMDB Modeling Guide.</i>
Relevant tasks	<ul style="list-style-type: none"> • How to Define a TQL Query in the <i>Universal CMDB Modeling Guide</i> • How to Create a Pattern View in the <i>Universal CMDB Modeling Guide</i>

Editing Pane

Enables you to edit the node selected in the **Trigger Queries** pane.

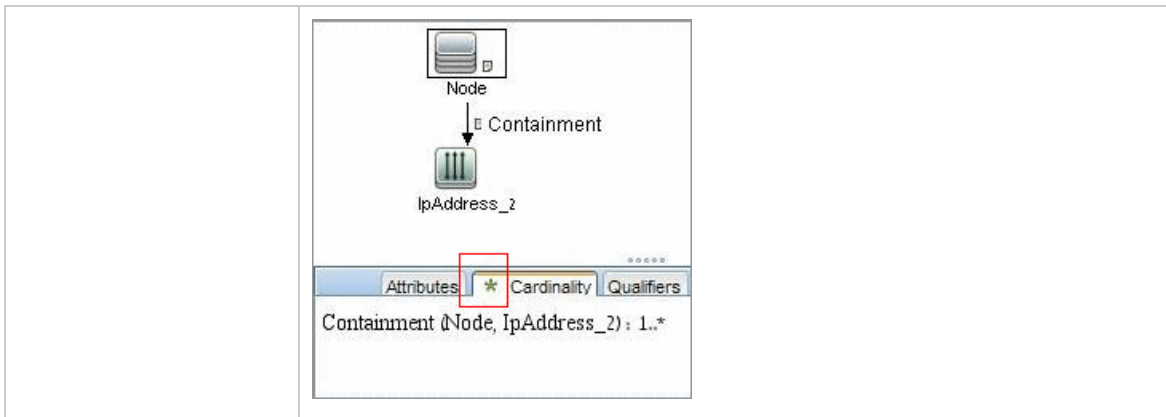
User interface elements are described below (unlabeled elements are shown in angle brackets>):

UI Element (A–Z)	Description
<node>	Click to display information about the node in the information pane.
<right-click menu>	To view a list of icons, see Shortcut Menu Options in the <i>Universal CMDB Modeling Guide</i> .
<Toolbar>	To view a list of icons, see Toolbar Options in the <i>Universal CMDB Modeling Guide</i> .

Information Pane

Displays the properties, conditions, and cardinality for the selected node and relationship.

<p>Important Information</p>	<p>Hold the pointer over a node to view information:</p> <pre> graph TD Node_2[Node_2] -- Composition --> WMI[WMI] Node_2 -- Containment_2 --> IpAddress[IpAddress] Node_2 -- Composition_2 --> Shell[Shell] WMI --> IpAddress Shell --> IpAddress </pre> <p>Information pane content:</p> <pre> Element Name: WMI CI Type: WMI Visible: false Cardinality: Composition (Node_2, WMI) : 1..* </pre> <p>A small green indicator is displayed next to the tabs that include information:</p>
-------------------------------------	---



User interface elements are described below:

UI Element (A-Z)	Description
Attributes	Displays the attribute conditions defined for the node or the relationship. For details, see Attribute Tab in the <i>Universal CMDB Modeling Guide</i> .
Cardinality	Cardinality defines how many nodes you expect to have at the other end of a relationship. For example, in a relationship between host and IP, if the cardinality is 1:3, the query retrieves only those hosts that are connected to between one and three IPs. For details, see Cardinality Tab in the <i>Universal CMDB Modeling Guide</i> .
Details	<ul style="list-style-type: none"> • CI Type. The CIT of the selected node/relationship. • Visible. A tick signifies that the selected node or relationship is visible in the topology map. When the node/relationship is not visible, a box <input type="checkbox"/> is displayed to the right of the selected node/relationship in the Editing pane: <div data-bbox="441 1289 808 1587" data-label="Diagram"> </div> • Include subtypes. Display both the selected CI and its descendants in the topology map.
Edit button	To view information, select a node or relationship in the Editing pane, select the tab in the Information pane, and click the Edit button. For details on the Node Condition dialog box, see Query Node/Relationship Properties Dialog Box in the <i>Universal CMDB Modeling Guide</i> .

UI Element (A-Z)	Description
Qualifiers	Displays the qualifier conditions defined for the node or the relationship. For details, see Qualifier Tab in the <i>Universal CMDB Modeling Guide</i> .
Selected Identities	Displays the element instances that are used to define what should be included in the query results. For details, see Identity Tab in the <i>Universal CMDB Modeling Guide</i> .

Chapter 15: Inventory Discovery

This chapter includes:

Inventory Discovery Overview	507
Inventory Discovery Scanners	509
Inventory Discovery Deployment Overview	512
Scan Files	516
Processing Scan Files	519
Scan File Processing Power	520
XML Enricher	521
XML Enricher Log Files	525
Application Teaching	527
Using Rules to Teach Applications	527
Enriched Scan File Structure	530
Hardware and Software Recognition	532
App Store Applications	534
Custom Hardware or Asset Mapping	534
Inventory Tools	534
BDNA Normalize Integration	536
Discovery Options for Client IP Ranges	538
How to Run Inventory Discovery	538
How to Run Inventory Discovery Manually	539
How to View Discovery Status of an Inventory CI in JMX	541
How to View Agent Deployment Log for an Inventory CI in JMX	544
How to Edit Pre-/Post-Scan Scripts	544
How to Set Up Asset Fields for Data Collection	547
How to Set Up Asset Fields for Data Collection - Example	558
How to Set up the Scanner to Handle Delta Scan Files in Manual Deployment Mode	561
How to Configure XML Enricher to Suit the Probe Deployment Mode	564
How to Configure the Maximum Number of Threads to Process Scan Files	567

How to Check XML Enricher Health Using JMX	568
How to Limit the XML Enricher Port to Allow Local Connection Only	568
How to Reprocess Scan Files	569
How to Import SAIs to the Data Flow Probe	569
How to Import Normalization Rules to the Data Flow Probe	570
How to Configure and Optimize Inventory Discovery	571
How to Configure Analysis Asset Fields	572
How to Map Scan File Attributes to UCMDB	572
Mapping Hardware or Asset Fields to UCMDB - Use-Case Scenarios	574
How to Set Extract Options	577
Configure Filtering in UCMDB	579
How to Enable Discovery of App-V Applications	580
How to Rename Scanner Executable Files	581
How to Integrate BDNA Normalize with Universal Discovery	582
How to Discover Client IP Ranges Without SNMP	584
How to Discover Windows Device Drivers using the Inventory Discovery by Scanner Job	584
Scanner Command Line Parameters Overview	585
Scanner Command Line Parameters	586
Scanner Information Type Parameters	593
Scanner File Locations	595
Web Server Configuration for Saving Scan Files via HTTP	596
XML Enricher Directory Structure	598
Enriched XSF File Structure	600
Inventory Discovery User Interface	600

Inventory Discovery Overview

Inventory Discovery helps your organization drive standardization and compliance initiatives, manage risk, perform IT asset audits, and implement chargeback policies.

Inventory Discovery, which also includes Infrastructure discovery, determines which devices are in your network and gathers information about each of them. It also serves as the foundation for the other modules of discovery. For example, Universal Discovery can gather information about what software is used and how often it is used. Universal Discovery can also build relationships between licensing and licensed applications that are installed. These relationships are useful when reconciling your organization's license obligations.

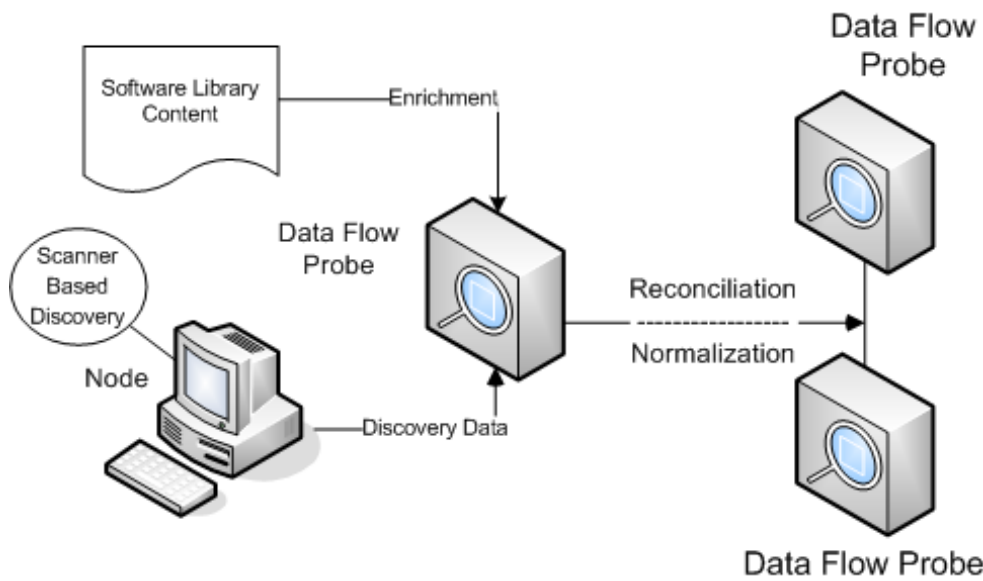
Inventory discovery is typically managed and run based on Management Zones using wizard-driven activities. These activities automate management of discovery jobs, and component deployment and upgrades. Additionally, these activities can be configured with specialized settings for each Management Zone. For example, UNIX servers in the Data Center may have different requirements for discovery than laptops in the Finance group. Alternatively, inventory discovery can be deployed and run manually using any third-party software packages.

Inventory Discovery begins by deploying software components to discovered devices in the Management Zone - Universal Discovery Agents and Scanners. Deployment methods can be automatic using activities. Alternatively, these components can be deployed manually using third-party tools.

The Universal Discovery Agent (UD Agent) provides secure communication between the device and the Data Flow Probe, and manages and runs the Scanner. The Scanner searches the device for detailed hardware, configuration, and software license information, and then stores the raw discovery data in a scan file. When the UD Agent is not installed, Scanners are managed using activities or, alternatively, managed manually using standard shell protocols.

Next, the discovery data is enriched with content from the Software Library. This enrichment process helps Universal Discovery recognize applications and identify hardware. Finally, enriched data is reconciled and normalized to reduce redundancies and errors, and then stored in UCMDB CIs.

The conceptual diagram below illustrates a basic inventory discovery system:



For details about deployment methods, see ["Inventory Discovery Deployment Overview" on page 512](#).

For details about the Universal Discovery Agent, see ["Universal Discovery Agent Overview" on page 163](#).

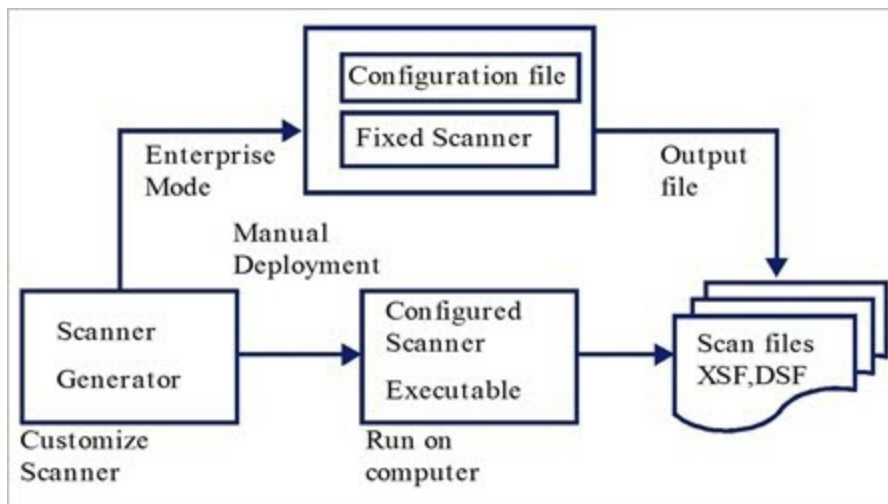
For details about setting up the Inventory Discovery activity, see the *HPE UCMDB Discovery and Integrations Content Guide - Discovery Activities*.

Inventory Discovery Scanners

After defining requirements, the next step in an IT asset inventory is to collect data. The data is collected by **Scanners**.

You configure and generate scanners using the **Scanner Generator**. Scanners are configured according to the specifications determined in the planning stage of the inventory.

The Scanner Generator is used to both configure and define the level of information to be collected. One or more scanner executable programs with the desired configuration are then generated and subsequently run across a computer population.



The Scanner Generator also provides a set of options for controlling the behavior of the scanner as it scans each computer, under both normal and exceptional conditions (such as when an error occurs).

Scanner Modes

The scanner is run across the computer population to collect inventory data in one of the following ways:

- **Enterprise Mode** (default). Automatically collects an inventory using the Universal Discovery's scheduling and launching capabilities.
- **Manual Deployment Mode**. Scans are launched manually. For example, scans are schedule and launched from login scripts or on non-networked machines.

Components of a Scanner

A scanner consists of the following files:

The scanner executable file	<p>This file is an executable file. It contains the constant parts of the scanner:</p> <ul style="list-style-type: none"> • strings • data files • the scanner executable code
The scanner configuration file	<p>The configuration file is a compressed XML file containing the settings for the scanner you are currently configuring.</p> <p>When the scanners are used in Enterprise Mode, they read the configuration from a separate configuration file. This is a binary file with a .cxz extension. The typical size of the configuration file is about 3K. As the size of the configuration file is significantly smaller than the size of the complete scanner, a separate scanner configuration is useful for repetitive inventory collection when the configuration of the scanner has been altered. In this case, only a small configuration file is delivered to the user's computer to run with the original scanner instead of delivering the entire new scanner.</p>

Note: When used in **Manual Deployment Mode**, the Scanner Generator generates self-contained scanner executables that consist of a combination of the scanner executable and configuration file.

What Information Does the Scanner Collect?

Scanners can collect several types of information and can be configured to collect any or all of them. The details recorded for each computer within each main category depend on the options and settings selected when the scanner is generated and the configuration of the computer.

Scanners can collect the following information:

Information	Description
Hardware and Configuration Information	<p>Hardware information is detected automatically. The scanners collect and store from 100 to 900 hardware items for a computer, depending on the type and manageability options available on the computer.</p> <p>The Scanner Generator allows a subset of the hardware collection to be disabled. Normally this is not required, but it may be desirable to decrease the scan file size or scan time.</p> <p>The hardware details that can be defined and recorded by the scanner include the following:</p>

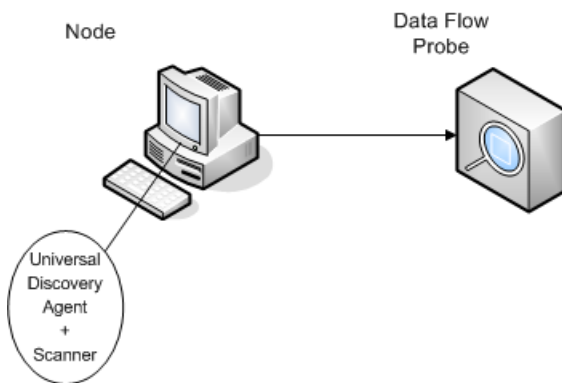
Information	Description
	<ul style="list-style-type: none"> • The processor type and BIOS details. • The memory size and configuration details. • The computer bus type and details of the attached cards. • The hard disk drive specifications (including the total size and free space). • The network type and ID (if applicable). This hardware item cannot be disabled in Enterprise Mode. • Comprehensive detection of network settings, including detection of multiple network adapters, TCP/IP settings, gateways, DNS servers, subnet masks, DHCP status. • The monitor and video display adapter details. • The type of keyboard and mouse driver installed and details of the I/O ports. • The Operating System version and other details. • The expansion (or adapter) cards detected. • The hardware data information from System Management BIOS (SMBIOS). • Running software processes.
Software Information	<p>Software information is scanned automatically, and consists of detailed information about the files and directories on the drives scanned. The information collected about files can be defined (including the file types and the level of information collected). It is possible to define the drives that are to be scanned based on either the media or format of the drive, or to use the targeted scanning option to scan just a set of directories. Specific files can be collected (that is, stored in the scan file) for further analysis or for error recovery purposes. It is also possible to configure the level of file detail stored in the scan file and filters can be set up that specify directories or files to be included or excluded from being stored.</p>
User or Asset Information	<p>User or asset information consists of configurable fields that can be collected automatically. It usually includes the asset number which is used to uniquely identify each computer. Asset data fields are automatically populated from the data extracted from text files, the Windows registry/WMI and environment variables.</p>
Software Utilization	<p>Universal Discovery can gather information about the software that is being used on the machines in your network. This is referred to as Software Utilization. The information collected can be used to optimize software license cost, for example by eliminating unused or under-utilized software installations.</p> <p>From a software recognition perspective, any files that are Unknown and are shown to have a high Utilization should be marked for teaching.</p> <p>Software utilization data shows the number of days that an application was used (as a percentage) over a period of time. This period of time is known as the Utilization Period.</p>

Information	Description
	As a guideline the Utilization Periods are as follows: <ul style="list-style-type: none">• Month (31 days)• Quarter (90 days)• Year (365 days)

Inventory Discovery Deployment Overview

There are several different types of deployment scenarios for Inventory Discovery. These diagrams illustrate the basic flow of scan files from each major component of Universal Discovery.

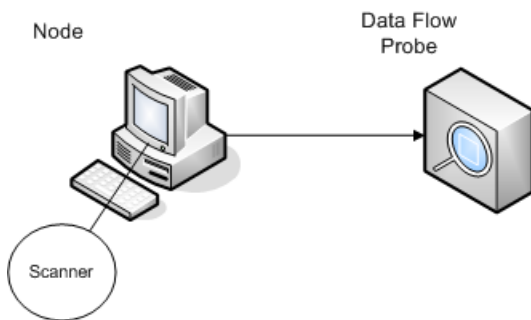
Scenario 1: Complete, Fully-Automated (Recommended)



- **Scenario:** You want a complete inventory discovery solution that takes full advantage of automated activities that schedule and run jobs. Universal Discovery Agents are deployed that are used as shell clients for communication with nodes, and as managers of Scanners for discovery.
- **Type of discovery:** Agent-based inventory discovery.
- **Deployment Methods:**
 - The Infrastructure Activity is used to trigger deployment of the Universal Discovery Agents to discovery nodes. Alternatively, deployment can be performed manually using third party tools. Scanners are copied to nodes by Universal Discovery Agents.
 - The Inventory Discovery Activity is used to trigger deployment of the Scanner.
- **Discovery Methods:**

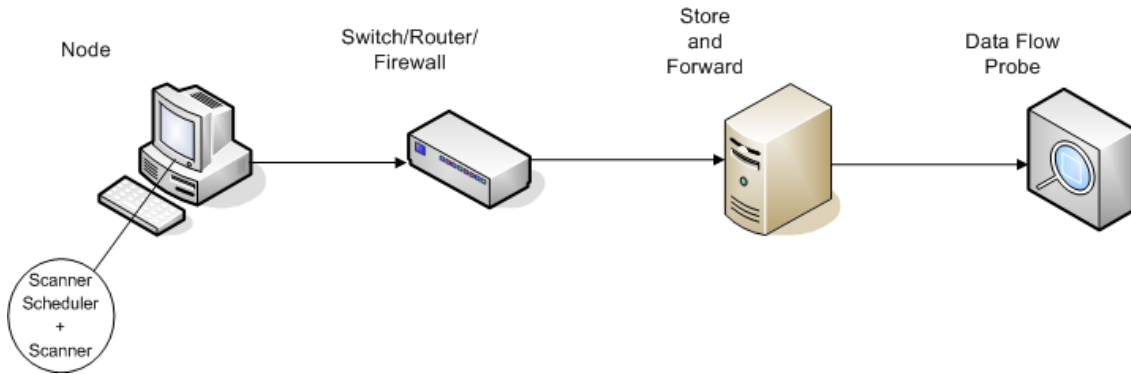
- The Infrastructure Activity is used to manage the Universal Discovery Agent lifecycle.
- The Inventory Discovery Activity is used to schedule, manage, and run scanner-based inventory discovery.
- **Links to Tasks:**
 - ["How to Run Zone-based Discovery" on page 428](#)
 - ["How to Install the Universal Discovery Agent Manually" on page 174](#)

Scenario 2: Scanner Testing



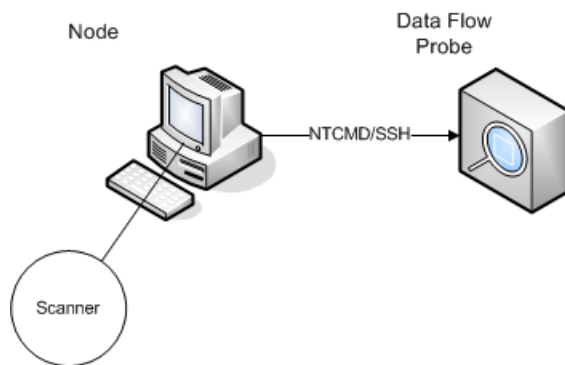
- **Scenario:** You want to test the functionality of the Scanner, or to analyze scan file data or file structure.
Alternatively, you are looking for a manually-initiated discovery process only.
- **Type of Discovery:** Agentless inventory discovery
- **Deployment Methods:** Generate a Scanner using the Scanner Generator Wizard, then copy the Scanner file to the node using any remote access technology.
- **Discovery Methods:** Remote access technologies are used to connect to the discovery node and execute the Scanner. Scanners can also be executed interactively at the console of the discovery node. Scan files are uploaded to the Data Flow Probe via FTP or HTTP, or they can be manually copied directly to the Data Flow Probe using any remote access technology.
- **Links to Tasks:**
 - ["Inventory Discovery Scanners" on page 509](#)
 - ["How to Install the Universal Discovery Agent Manually" on page 174](#)

Scenario 3: Routed, Complex



- **Scenario:** You have a complex environment that requires a routed solution for scan files to reach the Data Flow Probe. You also change Scanner versions or configuration files frequently and need an automated solution to deploy them.
- **Type of Discovery:** Agentless inventory discovery
- **Deployment Methods:**
 - Scanners are manually deployed to the discovery node.
 - Scanner Scheduler and Store and Forward are installed using any remote access technology.
- **Discovery Methods:** Scanner Scheduler schedules and runs inventory discovery.
- **Links to Tasks:**
 - ["How to Deploy the Scanner Scheduler" on page 202](#)
 - ["How to Install the Store and Forward Server" on page 210](#)
 - ["How to Run Inventory Discovery Manually" on page 539](#)

Scenario 4: Partially-Automated



- **Scenario:** You want a partially-automated solution for inventory discovery, but do not require any shell communication to the node.
- **Type of Discovery:** Agentless inventory discovery
- **Deployment Methods:** The Inventory Discovery Activity is used to deploy the Scanner.
- **Discovery Methods:** The Inventory Discovery Activity is used to trigger inventory discovery. The Data Flow Probe uses NTCMD or SSH to communicate with the discovery node.
- **Links to Tasks:**
 - ["How to Run Zone-based Discovery" on page 428](#)
 - ["How to Run Inventory Discovery Manually" on page 539](#)

Scan Files

Information that is collected from each computer is written to a scan file and is stored in the following file formats:

- **Compressed XML (XSF)**

All information scanned on the computer is stored to the file. The file is compressed using gzip. The files can be uncompressed using gzip, WinZip, or any other program that supports gzip decompression.

- **Delta Scan File (DSF)**

Instead of sending a full scan file to a probe after every scan, the scanners can calculate the difference (the *delta*) between the last full scan and the current one and transfer just this in Delta Scan File format (DSF). This format can dramatically reduce network bandwidth.

Delta Scan files cannot be viewed or used in the Inventory Tools (Analysis Workbench, SAI Editor, and Viewer).

Scan File Structure

A scan file contains a sequence of elements, each of which have various attributes. Root elements are:

- **<hardwaredata>**
- **<applicationdata>**
- **<users>**
- **<applicationusage>**
- **<filedata>**
- **<storedfiles>**
- **<configurationdata>**

The following is an example of several sections of a scan file:

```
<?xml version="1.0" encoding = "UTF-8" ?>  
<inventory codepage="1251" locale="English (United States)" fsfmajorver="7"  
fsfminorver="6" enricherver="10.00.000.555">
```

```
<hardwaredata>
  <hwAssetData type="shell">
    <hwAssetDescription type="attrib">tbrown - Xeon,
    2800MHz, 3712Mb</hwAssetDescription>
    <hwAssetTag type="attrib">000590 </hwAssetTag>
  </hwAssetData>
  <hwMemoryData type="shell">
    <hwMemTotalMB type="attrib">3712</hwMemTotalMB>
    <hwSwapFiles type="shell">
      <hwSwapFiles_value type="shell_value">
        <hwMemSwapFileName type="attrib">C:\pagefile.sys</hwMemSwapFileName>
        <hwMemSwapFileSize type="attrib">1534</hwMemSwapFileSize>
      </hwSwapFiles_value>
    </hwSwapFiles>
    <hwDOSMemoryData type="shell">
      <hwMemConventional type="attrib">640</hwMemConventional>
    </hwDOSMemoryData>
    <hwCMOSMemory type="shell">
      <hwMemExtended type="attrib">3799944</hwMemExtended>
      <hwMemCMOSTotal type="attrib">3800584</hwMemCMOSTotal>
      <hwMemCMOSConventional type="attrib">640</hwMemCMOSConventional>
    </hwCMOSMemory>
  </hwMemoryData>
</hardwaredata>

<applicationdata>
<recogconfig>
  <sai name="C:\hp\UCMDB\DataFlowProbe\runtime\probeManager\
    discoverySaiResources\saiRuntime\User.zsai"
    desc="User SAI File" date="04/06/2011" type="User"/>
  <sai name="C:\hp\UCMDB\DataFlowProbe\runtime\probeManager\
    discoverySaiResources\saiRuntime\Master.zsai"
    desc="" date="07/05/2011" type="Master"/>
</recogconfig>
<application version="6.4.09"
release="6.4"
name="Windows Media Player"
publisher="Microsoft"
language="English"
os="Windows 2000"
type="Ambient music or advertising messaging software"
typeid="143033"
maindir="C:\Program Files\Windows Media Player"
lastUsed="2011-08-26 00:00:00"
versionid="9978"
releaseid="582"
licencedby="11907"
licencedbyrelease="84"/>
<application version="6.0 sp1"
```

```
release="6.0"
name="Internet Explorer"
desc="Microsoft Internet Explorer"
publisher="Microsoft"
language="English"
os="Windows 98/NT/2K/ME/XP"
type="Internet browser software"
typeid="122252"
maindir="C:\Program Files\Internet Explorer"
lastUsed="2011-05-07 00:00:00"
versionid="12790" releaseid="131"/>
</applicationdata>

<filedata>
  <dir name="C:\\" date="2011-07-03 03:23:04" contains="-1">
    <file name="AUTOEXEC.BAT" size="0" modified="2011-04-03 13:51:04" attr="a"/>
    <file name="BOOT.INI" size="288" modified="2011-04-03 15:14:38" attr="rsa"/>
    <file name="sd_settings.ini" size="462" msdos="SD_SET~1.INI" modified="2011-06-
14 09:08:44" attr="a">
      <verinfo name="DOS 8.3 Name" value="SD_SET~1.INI"/>
    </file>
  </dir>
</filedata>

<storedfiles>
  <storedfile type="storedfile" name="SYSTEM.INI" size="217" istext="1"
istruncated="0" dir="C:\WINNT\SYSTEM.INI">
    <contents encoding="text">; for 16-bit app support
    [386Enh]
    woafont=dosapp.fon
    EGA80WOA.FON=EGA80WOA.FON
    EGA40WOA.FON=EGA40WOA.FON
    CGA80WOA.FON=CGA80WOA.FON
    CGA40WOA.FON=CGA40WOA.FON
    [drivers]
    wave=mmdrv.dll
    timer=timer.driv
    [mci]
  </contents>
</storedfile>
</storedfiles>
</inventory>
```

Processing Scan Files

Processing Normal Scan Files

At the end of the enrichment process, a new enriched scan file is created; the enriched core file is converted to UCMDB CI and relationship data, and reported to UCMDB. If delta scanning was enabled in the parameters for the Scanner used to produce the scan file, the incoming scan file is stored in the **Original** directory for future use by the delta scan processing. If delta scanning was disabled, the incoming scan file is deleted.

Tip:

- If an error occurs, the original scan file is moved to a failure directory and is not deleted.
- If an enriched scan file for the same computer already exists, the old file is overwritten.

Reprocessing Normal Scan Files

Scan files can be reprocessed after they are enriched. For example, you may want to run this operation when you update the Software Application Index (SAI) file. For example, after you use Express Teaching to teach applications, you may want to reprocess scan files. Scan files for selected nodes are moved from the **Processed** folder to the **Incoming** folder. Then, the scan file is processed using the updated SAI file.

To reprocess normal scan files, see ["How to Reprocess Scan Files" on page 569](#).

Processing Delta Scan Files

The delta scan file is used in conjunction with the previous version of the scan file located in the **Original** directory to reconstruct the new full version of the scan file. This full version is then moved into the **Incoming** directory, where it gets processed in the same way as other normal scan files.

At the end of the process, the reconstructed scan file is moved to the **Original** directory, ready for the next time a delta scan is found for this particular scan file instance.

For details handling delta scan files (Manual Deployment mode only), see ["How to Set up the Scanner to Handle Delta Scan Files in Manual Deployment Mode" on page 561](#).

Note: If the enriched scan file contains the **hwOSUserProfiles** attribute that has about 300,000 values, the Data Flow Probe maximum memory size should be increased by one gigabyte (GB).

For details on how to increase the Data Flow Probe maximum memory size , see ["How to Update the Data Flow Probe Memory Size" on page 65.](#)

Scan File Processing Power

When the scan files flow into the **incoming** directory of the XML Enricher faster than the XML Enricher is able to process them, a build-up of scan files occurs in the **incoming** directory. To allocate more processing power for enriching scan files, Universal Discovery can be configured to allocate more resources to accommodate this load.

Configuring Threads

In general, higher numbers of threads that are allocated to the XML Enricher service results in higher amounts of CPU and memory that the XML Enricher process consumes. As a result, the processing of scan files runs faster and faster. However, too many threads may slow down the processing if there is not enough CPU or memory resources available. In this case, disk performance becomes a constraining factor.

It is recommended to experiment with this setting using gradual changes and then analyze the results in the **incoming** directory of the XML Enricher.

To configure the maximum number of processing threads in the XML Enricher service, see ["How to Configure the Maximum Number of Threads to Process Scan Files" on page 567.](#)

Configuring Memory Mode or Database Mode

You can configure the mode in which the XML Enricher service runs when processing scan files. Select the mode that best suits your system or business needs as follows.

Mode	Memory Usage	Hard Disk Usage
Memory	High	Low
Database	Low	High

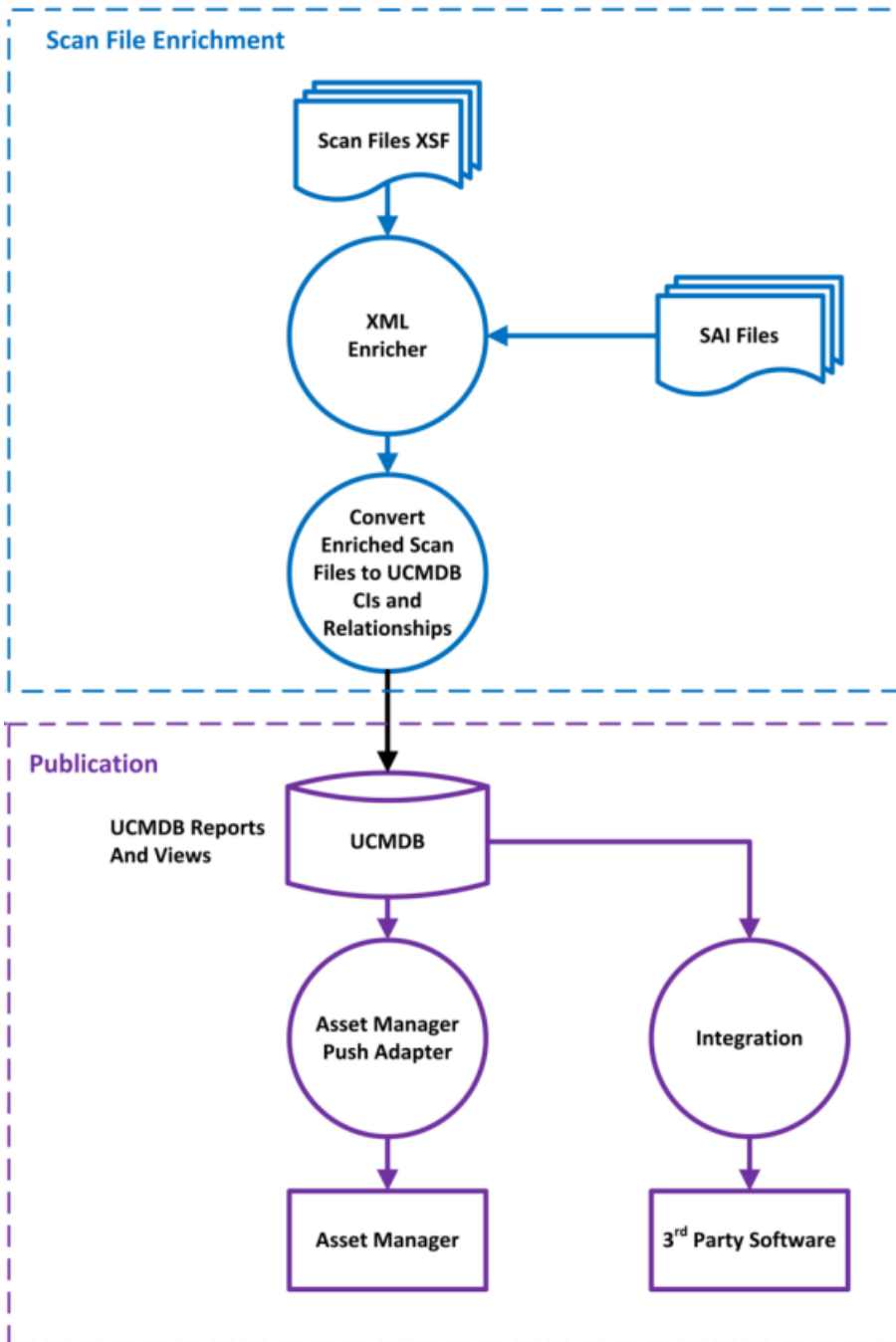
To configure this mode, see ["How to Configure XML Enricher to Suit the Probe Deployment Mode" on page 564.](#)

XML Enricher

The XML Enricher is a process that runs in the background and automatically adds application data to scan files. This process is called **scan file enrichment**. It works as follows:

1. The XML Enricher looks for new scan files (xsf or dsf format) in the **Incoming** directory.
2. If a file is found, it processes the file using **SAI** (Software Application Index) application recognition.
3. Information about recognized applications is added to the file data and separate **<applicationdata>**, **<applicationusage>**, and **<users>** sections are added to the XML file.
4. Two types of enriched scan files are created:
 - In the **Processed** directory complete enriched files are stored. They contain the complete scan file information enriched with the application recognition and software utilization data. The Inventory tools (the Viewer, the Analysis Workbench, and the SAI Editor) can make use of the files in the Processed directory for analysis and application teaching. To prevent locking of the scan files in the Processed directory, and to reduce the load on the computer running the Data Flow Probe, it is recommended to copy these files to the Universal Discovery Administrator's desktop where Inventory Tools are installed.
 - In the **ProcessedCore** directory, the core enriched files are created. These files do not contain the information about stored files. Additionally, the files do not contain information about file and directory data. Therefore, they are much smaller than the fully enriched files. The core enriched files are used internally by the InventoryDiscovery adapter to process the scan file information and convert it to the UCMDb CI and relationship data.

The XML Enricher can also be used to re-enrich scan files that were enriched previously. This can be useful after applying a significant update to the SAIs.



For information about setting up the XML Enricher to optimize performance, see ["How to Configure the Maximum Number of Threads to Process Scan Files"](#) on page 567 and ["How to Configure XML Enricher to Suit the Probe Deployment Mode"](#) on page 564.

For information about setting up software recognition options, see ["XML Enricher: Software Recognition Configuration Dialog Box"](#) on page 650.

Software Application Index (SAI) Files

The Software Application Index (.zsai) files contain a database of software applications. The XML Enricher uses these files to perform application recognition.

Note: These files are supplied in Content Packs by Micro Focus and are not editable. However, if you want to edit or delete SAI files, you can create a new user SAI named **Filter.zsai**. For details about this file, see ["Filter.zsai File" below](#).

Master.zsai	Contains English versions of software and language-neutral versions of Windows software.
French.zsai	Contains French versions of Windows software.
German.zsai	Contains German versions of Windows software.
Unix.zsai	Contains English and language-neutral versions of UNIX software.
BaseUnixOS.zsai	Contains language-neutral installed package rules for base UNIX operating system software.
Mac.zsai	Contains language-neutral versions of Apple Mac software.
Legacy.zsai	Contains older versions of UNIX and Windows applications for all languages.

Filter.zsai File

This section includes:

Overview	523
Filtering Mechanism	524
How to Create and Update Filter.zsai Using the SAI Editor	524
How to Deploy Filter.zsai to UCMDB	524

Overview

Master SAIs supplied with Content Packs or Inventory Discovery Knowledge Packs are read-only.

If there are problems with the software application recognition or you want to name some applications in the following ways:

- Edit or Delete the Master SAI content
- Disable some Master SAI content
- Make the content of the user SAI take priority over what is available in the master library

You can create a new user SAI named **Filter.zsai** that contains either excluded publishers or applications. This file provides the configuration for the master SAI filtering.

Filtering Mechanism

Filtering is configured on according to publisher or application basis only:

- If a publisher is present in **Filter.zsai** and there is no application under it, all content for this publisher will be filtered out from the master SAIs.
- If a publisher is present in **Filter.zsai** and the publisher has one or more applications under it, only these applications from that publisher will be filtered out from all master SAIs.
- Only Master SAIs are filtered out. User SAIs remain unchanged.



How to Create and Update Filter.zsai Using the SAI Editor

To create and update the **Filter.zsai** file using the SAI Editor, do the following:

1. Open the SAI Editor, and go to **File > New User SAI** to create a new user SAI.
2. In the Create a User SAI dialog box, name it **Filter.zsai**, and assign an unused SAI ID.
3. Click **OK**.
4. Drag and drop the unwanted content from a particular master SAI into the **Filter.zsai**.

How to Deploy Filter.zsai to UCMDB

To Deploy the **Filter.zsai** file to UCMDB, do the following:

1. Go to **Data Flow Management > Software Library**.
2. In the SAI Files pane, click  and select **Import SAI File** to deploy **Filter.zsai**. For more information about these options, see "[SAI Files Pane](#)" on page 682.
3. In the SAI Files pane, click .

4. In the Software Recognition Configuration dialog box that opens, click the **SAI Recognition** tab, and then select **Filter.zsai**.

For more information, see ["XML Enricher: Software Recognition Configuration Dialog Box" on page 650](#).

5. Click **OK**.

6. Results

After **Filter.zsai** gets deployed to the Data Flow Probe, the new filtering logic applies and produces master SAIs with unwanted content filtered out. The XML Enricher will be restarted to re-read the new SAI set.

The Data Flow Probe is updated with the SAI files. To verify this, check the files at **<DataFlowProbe_Home>\runtime\probeManager\discoverySaiResources\saiRuntime**.

In this directory, two file folders **base** and **filtered** are generated to back up the related SAI files:

- **base**. Contains the original master SAI files without being filtered out.
- **filtered**. Contains the master SAIs that are filtered out.

XML Enricher Log Files

Master Log

A running log that contains all activity that occurred in the XML Enricher service. By default, it is named **XMLEnricherService.log** and contained in the following location: **C:\hp\UCMDB\DataFlowProbe\runtime\log**

The format for a line in the log file is:

<date> <time> <thread> <level> <description>

Parameter	Description
<date>	Format: YYYY-MM-DD
<time>	Format: HH:MM:SS:MSS where:

Parameter	Description
	<ul style="list-style-type: none"> • HH. Hours • MM. Minutes • SS. Seconds • MSS. Milliseconds
<thread>	<p>The name of the processing thread where the log event occurred.</p> <ul style="list-style-type: none"> • Main. The main thread . • Pool 1- Thread <ThreadNumber> <p>where <ThreadNumber> represents the thread where the log event occurred.</p> <p>Note: The maximum amount of threads can be configured. For more information, see "How to Configure the Maximum Number of Threads to Process Scan Files" on page 567.</p>
<level>	<p>One of the following:</p> <ul style="list-style-type: none"> • Info. Information-related entry. • Error. An error occurred. Stack information is provided. • Debug. A debugging event.
<description>	Provides details about the logging event.

Scan File Error Logs

Error information about scan files that have not been successfully enriched are created in two locations. For information about the file structure of XML Enricher service, see ["XML Enricher Directory Structure" on page 598.](#)

Note: The data contained in the text file and the XML file is the same.

- **Text File.** A text file is created in one of the following subdirectories in the **Failed** subdirectory:
 - Error
 - Delta
 - Corrupt

The naming convention of this text file is as follows:

<ScanFileName> .xsf.log

where **<ScanFileName>** is the name of the scan file.

Application Teaching

Application Teaching is a process to improve application recognition.

The following are ways to perform application teaching:

- **Rules.** For more information, see ["Using Rules to Teach Applications" below](#).
- **Express Teaching.** For more information, see ["Express Teaching Overview" on page 691](#).

Using Rules to Teach Applications

Overview

Rules are used to teach applications in order to improve application recognition.

After a discovery job, the XML Enricher attempts to match data that is contained in a scan file to rules. Rules are contained in SAI files and are created by Micro Focus and by users.

Universal Discovery offers two main ways to teach applications:

- **Application Rules.** Choose the Package Rules or Version Data Rules option.
- **File Rules.** Specify files to use to recognize applications.

Ensure that the application or the release or version of the application is not already taught by Micro Focus. All rules taught by Micro Focus are contained in the Master SAI files in the Software Library. To see if your app or version is contained in the SAI library, see the release notes for the latest Content Pack.

Tip:

- As an alternative to teaching applications yourself, you can contact Micro Focus Support and submit a request for Micro Focus to add rules for your application to the next release of the Content Pack. For more information, contact Micro Focus Support.
- For the fastest and most convenient method, especially when teaching applications that are packaged in a standard format, choose **Application Rules > Package Rules** option.

For both ways, you identify files that Universal Discovery uses to recognize applications or release or versions of applications. While each are similar, there are differences in the number of supported platforms, and the effort levels required to configure the rules.

The SAI Editor and Viewer is used when configuring rules for both methods. To install these tools, see Inventory Tools in the *Universal CMDB Data Flow Management Guide*.

Note: Micro Focus provides some package rules and version data rules out-of-box, and actively maintains them in the Content Pack updates.

In general terms for each way, teach an application as follows:

1. Install the application
2. Run the scanner (additional configuration options required for Package Rules) and analyze the scan file using Inventory Tools
3. Configure the rule by entering the package name (Package Rule) or by specifying individual files (File Rule)
4. Teach different releases and versions for the same application by typing a regular expression (Package Rule), or by specifying additional individual files for that release or version (File Rule)
5. (Optional) Use Viewer to view the rule to ensure the rule information was saved.

Application Rules

Package Rules

(Most platforms/Operating Systems)

This method leverages package information, specifically the name of the package, to recognize applications.

Not all applications are packaged using standard formats. If the application is not using standard or support packages, for example, an .exe file, consider using File based rules.

Using this method is best for simple scenarios. The effort required to configure a rule is comparatively low because you create one simple rule for all releases and versions of an application and then UD automatically recognizes all releases and versions.

For more information on supported package types, see Supported Package Types in the *Universal CMDB Inventory Tools User Guide*.

Version Data

(Windows only)

Essentially, this option operates the same as Package Rules, but the regular expressions that are used to recognize releases and version information use the information contained in the executable files of the file system. This option is recommended when consistent publisher and version information is reported in the version data inside its executable files.

File

(Most platforms/Operating Systems)

To use this method effectively, you must be knowledgeable about the file contents of each package that you want to teach.

If there are many versions of an application, you must install each version of the application. Additionally, you must identify files that help UD recognize each version of the application. Alternatively, consider using the Package Rules method.

You teach individual files for different releases and versions of the same application. Then, you assign categories to each of those files that helps Universal Discovery identify the relationship of the file to the application.

Rules Matrix

The following table summarizes basic attributes of the ways to teach applications:

Type/Attribute	Platform	Effort Level	Target Use
Package	Many	Low	Standard Packaged Apps
Version	Windows	Low	Windows Executables
File	All	High	Executables

How to Use Rules to Teach Applications

Application Rules

Package Rules

For an example, see Example of a Recognition Rule Using Installed Package Information in the *Universal CMDB Inventory Tools User Guide*.

Version Data Rules

See Version Data Based Recognition Rules in the *Universal CMDB Inventory Tools User Guide*.

For an example, see Example of a Recognition Rule Using Version Data in the *Universal CMDB Inventory Tools User Guide*.

File

See Teaching Applications to the User SAI in the *Universal CMDB Inventory Tools User Guide*.

Note: The *Universal CMDB Inventory Tools User Guide* is installed together with the installation of the Inventory Tools.

Enriched Scan File Structure

The XML Enricher reads scan files and outputs enriched XML scan files containing all of the original data as well as data identified in the application recognition step.

Each file is stored as a <file> element. When a file is identified as belonging to an application, two attributes are added to the element:

- **versionid**
- **flag**

For example,

```
<file name="winword.exe" size="12345" versionid="1111" flag="M"/>
```

represents a file named **winword.exe** identified as belonging to the application with a version ID of 1111. The type of the file is "M", which means Main file. The possible values for the type field are:

flag	"type" tag in enriched XML file
Main	M
Associated	Y
3rd Party	3
Device Driver	A
Unknown	N

The **versionid** attribute refers to the unique ID associated with every version in the SAI library. In an enriched XML scan file, the **<applicationdata>** section contains a list of applications identified on the machine along with the version IDs.

For example:

```
<applicationdata>
<application version="6.0 sp1"
  release="6.0"
  name="Internet Explorer"
  desc="Microsoft Internet Explorer"
  publisher="Microsoft"
  language="English"
  os="Windows 98/NT/2K/ME/XP"
  type="Internet browser software"
  typeid="122252"
  maindir="C:\Program Files\Internet Explorer"
  lastUsed="2004-05-05 00:00:00"
  versionid="12790"
  releaseid="131"
/>

<application version="6.0 sp1"
  release="6.0" name="Outlook Express"
  publisher="Microsoft"
  language="English"
  os="Windows 98/NT/2K/ME/XP"
  type="Desktop communications software"
  typeid="105020"
  maindir="C:\Program Files\Outlook Express"
  lastUsed="2004-05-05 00:00:00"
  versionid="12792"
  releaseid="372"
  licencedby="12790"
```

```
        licencedbyrelease="131"  
      />  
</applicationdata>
```

The example above could be found for a machine with just two applications on it: Microsoft Internet Explorer and Microsoft Outlook Express. The **licencedby** attribute indicates that Microsoft Outlook Express is licensed by Microsoft Internet Explorer. In other words, while both are licensable applications, this machine requires one license for Microsoft Internet Explorer; with this license, no separate Outlook Express license is required.

Hardware and Software Recognition

Recognition is the process of identifying certain properties and attributes of a hardware device or a software application by leveraging content that is supplied by Content Packs and by publisher data.

Hardware Recognition

- **Discovery Rules.** A database containing information on hardware that is available for sale by a wide range of manufacturers. The Discovery Rules Engine determines the device's operating system, application, device family, and model. Then, Discovery Rules assigns a device type to your device model.

This database is updated monthly and is included in Content Packs. For more information, see the [ITOM Marketplace](https://marketplace.microfocus.com/itom/content/ud-content-packs) website (<https://marketplace.microfocus.com/itom/content/ud-content-packs>).

To find more information about viewing Discovery Rules that are installed on your system, see "[How to View Discovery Rules in JMX](#)" on page 307.

Software Recognition

- **Software Identification Tags.** Universal Discovery supports the ISO/IEC 19770-2 standard. A software identification tag is an XML file that contains identification information about a software product. The tag is installed on a discovery node together with the software product, and it uniquely identifies the software. When tags are captured by Scanners during discovery, the data can be leveraged for improved software asset management and compliance.

The tag may be created as part of the installation process, or added later for software already installed without tags.

Software identification tag files must have the **.swidtag** file extension in order to be recognized by Inventory Discovery tools. You can create installed package rules that can match the information found in the software ID tags.

For more information, about viewing software identification tags, see ["Inventory Tools" on the next page](#).

- **Software Application Index (SAI)**. SAI files provided with the Content Pack contain information to identify applications on a discovery node. The library also contains license relationship information that allows Universal Discovery to identify how individual software products are related to a software product suite.

SAI files can be exported from the **Administration > Package Manager**, then select **SAI**. For more information, see How to Export a Package in the *Universal CMDB Administration Guide*.

In addition to the standard libraries, Universal Discovery includes several tools that allow you to create your own library extensions in the form of one or more User SAI files that can be applied to the automatic Application Recognition process. For more information, see the section that describes the SAI Editor in ["Inventory Tools" on the next page](#). For more information about teaching applications to improve the Application Recognition process, see ["Application Teaching" on page 527](#).

The SAI contains information about applications in multiple languages for multiple platforms. SAI files are available as follows:

Windows	The following languages are available: <ul style="list-style-type: none">○ English○ French○ German
UNIX	SAI files are available for the following variant systems: <ul style="list-style-type: none">○ BaseUnix○ HP-UX○ AIX○ Solaris
Mac	Mac OS X

App Store Applications

"App" Store applications refer to applications that are downloaded or distributed from an online digital distribution platform store.

Information about App Store applications that is collected during Inventory Discovery is sent to UCMDB and contained in the **Installation Source** attribute of the **Installed Software CI**.

For more information on viewing CIs, see "CI Selector" in the *Universal CMDB Modeling Guide*.

Custom Hardware or Asset Mapping

Universal Discovery provides the capability to create custom mappings between captured data contained in scan files and attribute of a CI in UCMDB.

By default, Universal Discovery maps a large subset of scan file data to UCMDB CIs and relationships, however, not all data is mapped.

Note: If you create post-scan scripts to capture customized data, you need to create mappings for this data. For more information on post-scan scripts, see ["Pre-Scan and Post-Scan Scripts" on page 251](#).

To create custom mappings of hardware or asset-related data, see ["How to Map Scan File Attributes to UCMDB" on page 572](#).

Inventory Tools

The Inventory Tools enable you to view and analyze scan file data.

Note: These tools are installed using the Data Flow Probe Installer program. They are installed together with the Data Flow Probe. However, it is recommended to install them on a separate computer to prevent performance degradation on the Data Flow Probe, and also to prevent data corruption of the SAI files. For more information on installing Inventory Tools, see the section that describes installing Data Flow Probes in the interactive *Universal CMDB Deployment Guide*.

To install them separately, run the Data Flow Probe Installer program and select the **Inventory Tools** type installation. For details about supported platforms, see the *Universal CMDB Support Matrix* document.

To start the tools (on Windows), click **Start > All Programs > UCMDB > Inventory Tools**.

When the Inventory Tools are installed on your Windows computer, you can view the help documentation for the tools by clicking the **Help** menu option of the Inventory Tool. Users of all platforms that have Adobe Reader installed on the computer can also view the help documentation by clicking **Start > All Programs > UCMDB > Inventory Tools**.

Software Application Index (SAI) Editor

View Software Application Index (SAI) file data, and perform additional tasks as follows:

- View and edit a collection of SAI files
- Create new User SAIs
- Move and copy items between SAIs (you can only edit User SAIs), and delete items
- Export the contents of an SAI to XML format
- Display license relationships
- Add and edit existing license relationships

Viewer

Displays software, hardware and asset information that is collected for an individual computer as follows:

- Details of all software scanned, presented in an explorer style view
- User entered asset information
- Detailed and summarized hardware and configuration information
- The contents of key files collected during Inventory Discovery, such as system configuration files
- Details of all logical drives
- Details of all recognized applications and their utilization statistics
- Detailed comparison of two scan files

Analysis Workbench

Perform analysis tasks using three types of information as follows:

- Software files that are recognized as belonging to a particular application
- Unidentified software and files that may belong to unrecognized applications
- Hardware and asset data

Analysis Workbench uses the Software Application Index (SAI) that contains application and version descriptions to identify the files found during Inventory Discovery. Scan results are checked against the SAI to identify and recognize software. Any unrecognized files can be marked for further investigation, and when identified, their details can be added to the SAI file so they will be correctly identified in the future. For more information on Application Teaching, see ["Application Teaching" on page 527](#).

BDNA Normalize Integration

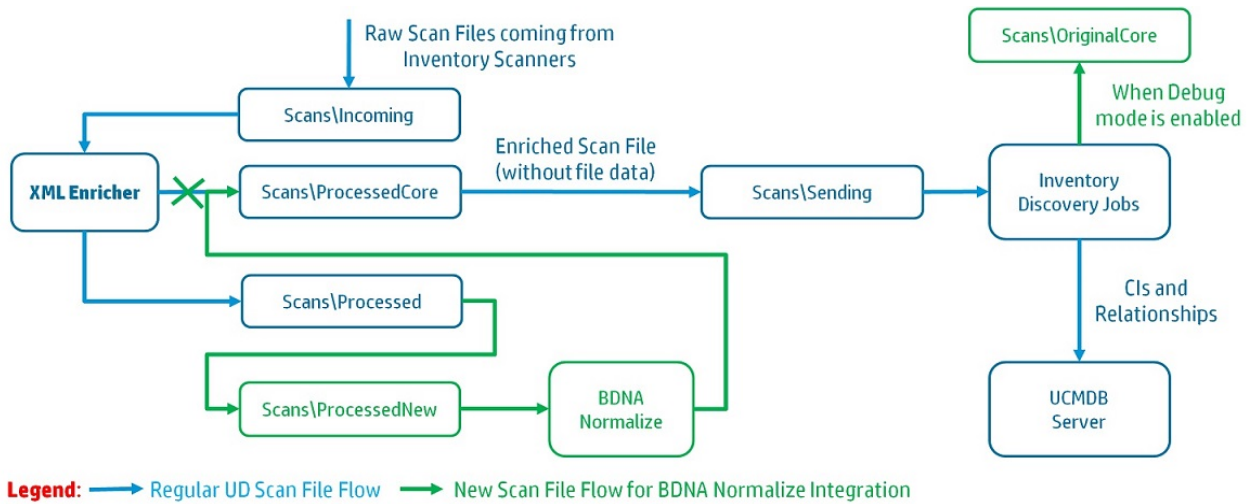
BDNA Normalize is a software product that is capable of normalizing raw inventory data against the normalized catalog called BDNA Technopedia. Universal Discovery can integrate with BDNA Normalize, so that the normalized installed software produced by the scanner-based inventory discovery is normalized using the BDNA Technopedia data instead of Universal Discovery SAI.

When BDNA integration is enabled, the following changes occur during the BDNA installation and configuration:

- Folders are created in `<DataFlowProbeInstallDir>\runtime\xmlenricher\Scans` as follows:
 - **ProcessedNew**. BDNA Normalize monitors this folder for scan files.
 - **OriginalCore**. Contains the scan files enriched by BDNA Normalize.

Note: These folders are created when the configurations are performed on the Data Flow Probe and not when BDNA Normalize is installed. However, OriginalCore folder is created only when you enable the Debug mode. For more information on enabling the Debug mode, see ["Debug Mode" on the next page](#).

- The scan file workflow is changed as follows:



- The following attributes were added to the Installed Software CI type in the Universal Discovery class model to hold BDNA Normalize specific data:

Attribute Name	Display Name	Description
component	Component	Contains the name of the installed software component as described in the BDNA Technopedia catalog. (e.g: Client, Server, Agent,...)
service_pack	Service Pack	Contains the name of the service pack of the installed software product as described in the BDNA Technopedia catalog.
edition	Edition	Contains the edition of the installed software product as described in the BDNA Technopedia catalog.
recognized_by	RecognizedBy	Indicates the source of the normalized installed software data. When the value is "SAI", the installed software is normalized using Universal Discovery SAI. When the value is "BDNA", the installed software is normalized using BDNA Normalize.

Debug Mode

The Debug mode preserves the scan files enriched by BDNA Normalize in the `<DataFlowProbeInstallDir>\runtime\xmlenricher\Scans\OriginalCore` directory, so that troubleshooting of the BDNA Normalize operation can be done. When the debug mode is disabled, a copy of the BDNA Normalize enriched scan file is not kept and once it is processed, it is deleted by the inventory discovery jobs.

Software Utilization

The Software Utilization Data collected by Universal Discovery for applications recognized via its SAI library is available and is normalized to the BDNA Technopedia format. The Software Utilization Data is not available for applications that are not recognized by Universal Discovery (via SAI), but can be recognized by BDNA Normalize.

Discovery Options for Client IP Ranges

Universal Discovery offers options to use or not use SNMP when discovering client type IP ranges. The option that you choose depends on your organization's policies.

Discovery Option	Advantages	Disadvantages
Without SNMP	<ul style="list-style-type: none">• Switch/router IP addresses are not used.• Switch/router passwords are not used.	IP addresses in UCMDB are not up-to-date.
With SNMP	IP addresses in UCMDB are up-to-date.	<ul style="list-style-type: none">• Switch/routers IP ranges are used.• Switch/routers passwords are used.

How to Run Inventory Discovery

This high level task describes how to run Inventory Discovery in your environment.

This task includes the following steps:

1. ["Prerequisites " on the next page](#)
2. ["Run inventory discovery" on the next page](#)
3. ["Results" on the next page](#)

1. Prerequisites

- Ensure that UCMDB is running.
- Ensure that the Data Flow Probe server is running.
- (For Zone-based discovery only) Ensure that you have discovered the infrastructure in your management zones. To do this, see ["How to Run Zone-based Discovery" on page 428](#).

2. Run inventory discovery

Select one of the following methods to run inventory discovery:

- (Recommended) **Zone-based**. Use a Discovery Activity to run in specific Management Zones. For more information, see "Inventory Discovery Activity" in the *HPE UCMDB Discovery and Integrations Content Guide - Discovery Activities*.
- **Manual**. Use any third party software packages to run inventory discovery. For more information, see ["How to Run Inventory Discovery Manually" below](#).

3. Results

To verify the discovery ran successfully, select the Management Zone in the Management Zones tree. In the **Discovery Status** pane, click the **Results** tab.

Note: If you are not using Management Zones, click the Inventory Discovery job.

For user interface details, see ["Discovery Results Tab/Pane" on page 678](#).

How to Run Inventory Discovery Manually

This task describes how to run inventory discovery manually.

This task includes the following steps:

- ["Prerequisites" on the next page](#)
- ["Configure the scanners" on the next page](#)
- ["Distribute the scanners" on the next page](#)
- ["Run the scanners" on the next page](#)

- ["Save the scan files to the Data Flow Probe" below](#)
- ["Run inventory discovery job" on the next page](#)
- ["Results" on the next page](#)

1. Prerequisites

- Ensure that a Data Flow Probe server is running.
- Ensure that UCMDB is running.

2. Configure the scanners

Generate a scanner using the **Scanner Generator Wizard**. For more information, see ["Scanner Generator Wizard" on page 605](#).

Note: Ensure you select Manual Mode in the **Scanner Generator Wizard**.

3. Distribute the scanners

Connect to discovery nodes using any remote access technology to copy the scanner executable file to the discovery node.

4. Run the scanners

Methods to run scanners are as follows:

- **Attended**

Click the executable file. To see a list of default file names, see ["Scanners tab" on page 647](#).

- **Unattended**

Connect to the discovery nodes using any remote access technology, third party solution, or scripting solution and then run the scanner executable file. To see a list of default file names, see ["Scanners tab" on page 647](#). You can pass command line parameters to the discovery node shell to override any configurations that were used in the Scanner Generator. For more information about scanner command line options, see ["Scanner Command Line Parameters Overview" on page 585](#).

5. Save the scan files to the Data Flow Probe

Methods to save the scan file to the Data Flow Probe are as follows:

- Use an integrated solution that schedules scan times and automatically routes scan files. For example, Store and Forward together with Scanner Scheduler. For more information, see ["Store and Forward Overview" on page 210](#) and ["Scanner Scheduler Overview" on page 202](#).
- Manually copy the scan file from a discovery node to the Data Flow Probe using any remote file transfer technology. For more information, see ["XML Enricher Directory Structure" on page 598](#) and ["Scanner Options Page" on page 635](#).

6. Run inventory discovery job

Run the **Inventory Discovery by Manual Scanner Deployment** job. For more information, see ["How to Manually Activate Modules/Jobs/CIs" on page 473](#).

7. Results

To verify the discovery ran successfully, select the Management Zone in the Management Zones tree. In the **Discovery Status** pane, click the **Results** tab.

Note: If you are not using Management Zones, click the Inventory Discovery job.


For user interface details, see ["Discovery Results Tab/Pane" on page 678](#).

How to View Discovery Status of an Inventory CI in JMX


As an inventory discovery administrator, you can invoke the **getDiscoveryStateForInventoryCI** method to check the discovery status of an inventory CI, so that you can verify the health and live state of that device.

To do so,

1. Log in to the UCMDB JMX console. (Launch the Web browser and enter the following address: **https://<server_name>:8443/jmx-console**. You may have to log in with a user name and password.)
2. Locate **UCMDB:service=Discovery Manager** and click the link to open the Operations page.
3. Locate the **getDiscoveryStateForInventoryCI** operation.

4. Enter your Customer ID. **(Default: 1)**
5. For the **cild** field, enter the global ID for the inventory CI for which you want to check the discovery status.
 - a. In UCMDB UI, go to **Modeling > IT Universe Manager**.
 - b. In the CI Selector pane, go to the **Search CIs** tab, click the **Start the Search**  icon for the **CI Name** field.
 - c. From the returned results, select a discovered node.
 - d. Go to the **Properties** tab in the right pane, scroll down to locate the **Global Id** property.
 - e. Right-click the value for the **Global Id** property, select **Copy Property Name and Value**.
 - f. Paste the value into the **cild** field in the JMX console and remove the property name.
6. Click **Invoke**.

The result displays, which looks similar to the following:



[JMX Search](#) [JMX List](#) [Operations Index](#) [Back to MBean](#) [Reinvoke MBean](#) (Current Server is a writer: SGDLITVM0420)

Mbean: UCMDB:service=Discovery Manager. Method: getDiscoveryStateForInventoryCI

Discovery State

First Discovery	Tue May 12 11:14:18 IST 2015
Last Seen	Tue May 12 11:12:59 IST 2015
Last Discovery Result	Success

Agent State

N/A

Scanner State

N/A

The result page contains discovery information in three sections:

o **Discovery State**

Field	Description
First Discovery	Time when the CI was discovered for the first time.
Last Seen	Time when this CI was last discovered successfully by a job. When there are no active jobs to discover this CI, or all jobs failed in discovering this CI, the value is N/A .
Last Discovery Result	Last discovery result. Available statuses include: <ul style="list-style-type: none"> • Pending. There are one or more active discovery jobs that are running. This CI is not yet discovered. • Success. The CI was successfully discovered. • Fail. Discovery of this CI failed with one or more errors. • Warning. Discovery of this CI completed with one or more warning messages. • N/A. No active jobs and trigger CIs are available for discovering this CI.

o **Agent State**

N/A if no agent is available.

When agent is used, this section displays agent related information. The same information can also be found in the Properties tab of the CI.

o **Scanner State**

N/A if no scanner is available.

When scanner is used, this section displays scanner related information. The same information can also be found in the Properties tab of the CI.


Note:

- If the trigger CI is a Probe Gateway CI, then the job discovery status and the **Last Seen** value for the specific CI will not display.
- When a discovery job is deactivated, its last discovery record is not available even if the job had successfully discovered the CI when it was active.
- The Last Seen value or the Last Discovery Result occasionally get reflected a bit late after the job is finished in the Universal Discovery UI.

How to View Agent Deployment Log for an Inventory CI in JMX

As an inventory discovery administrator, you can invoke the **getAgentDeploymentLogForInventoryCI** method to check the agent deployment log for an inventory CI. You work with the JMX console.

This task includes the following steps:

1. Log in to the UCMDB JMX console. (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. Locate **UCMDB:service=Discovery Manager** and click the link to open the Operations page.
3. Locate the **getAgentDeploymentLogForInventoryCI** operation.
4. In the **Value** field for **customerID**, enter your customer ID. (**Default: 1**)
5. For the **ciId** field, enter the global ID for the inventory CI for which you want to check the discovery status.
 - a. In UCMDB UI, go to **Modeling > IT Universe Manager**.
 - b. In the CI Selector pane, go to the **Search CIs** tab, click the **Start the Search**  icon for the **CI Name** field.
 - c. From the returned results, select a discovered node.
 - d. Go to the **Properties** tab in the right pane, scroll down to locate the **Global Id** property.
 - e. Right-click the value for the **Global Id** property, select **Copy Property Name and Value**.
 - f. Paste the value into the **ciId** field in the JMX console and remove the property name.
6. Click **Invoke**.

The result displays.

How to Edit Pre-/Post-Scan Scripts

This task describes how to edit pre- and post-scan scripts in your Management Zones.

This task includes the following steps:

- ["Prerequisites" below](#)
- ["Navigate to the script editor" below](#)
- ["Edit the script" below](#)
- ["\(optional\) Import resource files" on the next page](#)
- ["Deploy the scripts" on the next page](#)
- ["Results" on the next page](#)


1. Prerequisites

- A Data Flow Probe is installed.
- A Management Zone is defined.

2. Navigate to the script editor

You can access the Pre/Post Scan Script Editor in the following ways:

- In the Management Zone:
 - i. Set up and activate the **Inventory Discovery Activity**.
 - ii. On the Preferences Page, click to select **Scanner based Inventory Discovery** and then click **Edit script**. The Pre/Post Scan Script Editor opens.
- From the Adapter Management module:

Inventory Discovery > Adapters, click **Inventory Discovery by Scanner**, expand the Global Configuration Files pane, click the **PrePostScanScriptingConfiguration** file, and click **Edit** .


3. Edit the script

- a. Click the platform for which you want to edit a script. Depending on the platform, you might also need to select a version.

Tip: Click **All UNIX** to create a script that is used as a backup script in case a script for any of the other UNIX variant scripts fails to run.

- b. Click **pre scan script** or **post scan script**. The script editing window opens.
- c. Write your script using shell commands that are appropriate for the platform or shell that is running on the discovery node.

4. (optional) Import resource files

To include files that your script requires, import them by clicking the **Resources** node in the left pane and then click . The Import Files dialog box is displayed. Select the files you want to include in the script package.

Note:

- When files are transferred to the remote machine, they will not be marked as executables—even if they are executables. Ensure you mark them as executables in the pre/post scripts before running them.
- Resources files are never removed automatically. If you want to remove them after your scripts run, ensure your scripts perform clean-up operations as needed.

5. Deploy the scripts

To deploy and run the scripts, click to select **Run Pre/Post Scripts** on the Preferences Page of the **Inventory Discovery Activity**.

6. Results



To verify the script is deployed successfully, verify the script file is stored in the same directory as the scanner executable. For more information on the location of the scanner executable, see the section describing scanner file locations in "[Scanner File Locations](#)" on page 595.

How to Set Up Asset Fields for Data Collection

This task describes how to set up the asset data fields to be collected by the Scanner Generator.

For an example on how to set up a Combination type asset field, see ["How to Set Up Asset Fields for Data Collection - Example" on page 558](#).

Note: It is strongly recommended that **Description** and **Asset Tag** fields are included in your list of asset fields.

1. In the Scanner Generator wizard, go to the **Asset Data** page > **Asset Data** tab.
2. Click **Create New Field** . The Choose Field dialog box opens, showing all standard fields not currently in use by the scanner. For a full list of asset fields, see ["Asset Fields" on the next page](#).
3. Select a field and click **OK**.
4. Configure the asset field:
 - a. On the Asset Data tab, select the field you just added, and click **Edit Field** .
 - b. Configure the asset field as described in ["Asset Field Configuration Dialog Box" on page 632](#).
 - i. Define a caption for field and determine the maximum length.
 - ii. Select the type of field.
 - iii. Next to the **Parameter** box, click **Change** to define parameters for the field. For details about the parameter options, see ["Asset Field Parameters" on page 550](#).
5. Consider the order of the asset fields as they appear in the Asset Fields list, and correct their order where necessary.

Important: A field cannot depend on a field that is placed below it in the Asset Fields list. That is, if you have set up any derived or automatic fields that require data from fields below them in the list, you must move them to a position in the list that is above these fields.



To correct the order of the fields, select and drag a row to the desired location in the list.

Asset Fields

The Scanner Generator provides several predefined standard field types that indicate to which hardware field the asset field is mapped.

- The following table lists the special standard asset fields:

Note: It is strongly recommended to include these fields in your list of asset fields.

Field	Description
 Description	<p>Can be configured to contain a brief description of the machine being scanned.</p> <p>Default: Combination type. It combines information from several hardware and asset fields.</p> <p>When loading data from scans into the analysis tools (Analysis Workbench and Viewer), the contents of the Description field are displayed for each scan file to help identify it.</p>
 Asset Tag	<p>Contains a unique identifier for the machine being scanned. It is normally populated from a sequence of hardware fields such as MAC Address, Serial Number or Asset tag.</p> <p>The asset number entered in this field is used to name the off-site scan file.</p>

- The following table lists other standard field types that indicate to which hardware field an asset field is mapped:

Field	Description	Hardware Field in Scan File
Asset Tag	The Asset Tag field contains a unique identifier for the machine.	hwAssetTag
Automatic Asset Fields	<p>These asset data fields can be automatically populated from data extracted from text files, the Windows registry/WMI or environment variables.</p> <p>You can configure up to 56 automatic fields, which can then be used in the calculation of derived or calculated fields.</p>	hwAssetAutomatic1..56
Bar Code	For machines with bar codes on them, use this field to allow the bar code to be entered or stored	hwAssetBarCode

Field	Description	Hardware Field in Scan File
Building	Identified the building containing the machine	hwAssetBuilding
Business Unit	Name of business unit	hwAssetBusinessUnit
Cellphone Number	Cell/Mobile phone number of user.	hwAssetCellphoneNumber
Cost Center	Cost center description or code	hwAssetCostCenter
Department	Department description or code	hwAssetDepartment
Device Type	Device type of the machine (Server, Notebook, Tower and so on)	hwAssetDeviceType
Division	Division description or code	hwAssetDivision
Employee ID	Employee ID as used in the organization.	hwAssetEmployeeID
First Name	First name of user	hwAssetUserFirstName
Floor	The floor on which the machine is located	hwAssetFloor
Full Name	Full name of user	hwAssetFullName
Job Title	Job title of user	hwAssetUserJobTitle
Last Name	Last name of user	hwAssetUserLastName
Machine Make	Make or Manufacturer of the machine	hwAssetMachineMake
Machine Model	Model of the machine. This data can be populated from SMBIOS using a Sequence Field on machines supporting SMBIOS.	hwAssetMachineModel
Office Location	Location of the office - normally a combination of country and city	hwAssetOfficeLocation
Printer Asset Tag	Asset tag of a local printer attached to the machine, if any	hwAssetPrinterAssetTag
Printer Description	Description of a local printer attached to the machine, if any	hwAssetPrinterDescription
Room	Description, name or number of the room containing the machine	hwAssetRoom

Field	Description	Hardware Field in Scan File
Section	Section description or code	hwAssetSection
Telephone Extension	Internal telephone extension	hwAssetTelephoneExtension
Telephone Number	Full direct telephone number of user	hwAssetTelephoneNumber
User Field	User-defined fields. You can configure up to 30 User fields.	hwAssetUserField1..30

Asset Field Parameters

Calculated Fields

Calculated fields can be automatically populated from data extracted from text files, the Windows registry, environment variables and so on.

- ["Environment Variable Extract Fields" below](#)
- ["Registry Extract Fields" on the next page](#)
- ["Text File Extract Fields" on page 552](#)
- ["WMI Extract Fields" on page 553](#)

Environment Variable Extract Fields

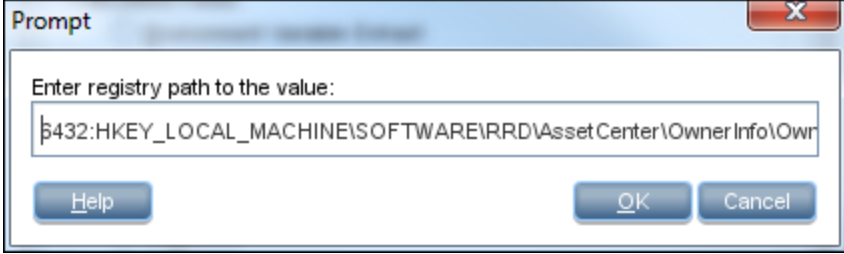
This field is set up to read the value contained in an operating system's environment string. For example, you may have the Host Name or SMS ID stored in an environment variable and want this to be automatically picked up by the scanner.

Parameter	Description
Enter the name of an environment variable	Examples of environment variables: TEMP and PATH.

Registry Extract Fields

This type of field searches the Windows registry for the defined key and makes an automatic entry of the key value. This extract field is applicable to Windows only.

Parameter	Description
<p>Enter registry path to the value</p>	<p>The full path to the registry value you want to have in this field in the form RegistryKey\Value.</p> <p>Example:</p> <p>To find out whether the Screen Saver is active on the system, you can use the following registry extract field:</p> <pre>HKEY_CURRENT_USER\Control Panel\Desktop\ScreenSaveActive</pre> <p>The registry does not allow the backslash ("\") character in the RegistryKey. However, it can be used in Value. If the backslash character is contained in the Value name, it must be escaped. For example, if Value is "a\b", it must be specified as follows:</p> <pre>HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\VSS\VssAccessControl\NT Authority\NetworkService</pre> <p>In Windows, the paths to various registry values can be found by viewing the content in the Registry Editor. For more information about the Registry Editor refer to the Windows documentation.</p> <p>In 64-bit versions of Windows, portions of the registry entries are stored separately for 32-bit applications and 64-bit applications and mapped into separate logical registry views using the registry redirector and registry reflection. This is because the 64-bit version of an application may use different registry keys and values than the 32-bit version. There are also shared registry keys that are not redirected or reflected.</p> <p>Because the Universal Discovery Windows scanner is a 32-bit application, by default, the scanner only reads the 32-bit portion of the registry. To access the 64-bit registry portion in 64-bit versions of Windows, the scanner supports the following prefixes:</p> <p>Note: The prefix includes the colon (:).</p> <ul style="list-style-type: none"> • 32: Forces only the 32-bit registry value to be read. • 64: Forces only the 64-bit registry value to be read. In 32-bit versions of Windows, the registry extract field with this prefix will always be empty. • 3264: Reads the 32-bit registry value, and, if it is empty, reads the 64-bit registry value. • 6432: Reads the 64-bit registry value, and, if it is empty, reads the 32-bit registry value. <p>If no prefix is given, the scanner reads the 32-bit registry value only.</p>

Parameter	Description
	<p>The actual registry value path should follow the prefix, as shown in the following example:</p> 

Text File Extract Fields

This field searches a named text file for a defined character string and makes an automatic entry of the characters between the search string and the end of the line.

This field type is normally used for the **Asset Number** field. This is used to extract the asset number from the file **Asset.bat** on the line containing the text: **SET ASSETNO=**

Parameter	Description
File Name	<p>The name of the file (and the file path) that the information is to be extracted from.</p> <p>Note:</p> <ul style="list-style-type: none"> • Entries in this field are case-sensitive. This is applicable to UNIX and Mac OS X only. • You can use an environment variable to specify the file name. The environment variable name must be in upper case for this to happen. If it is not, the string is interpreted as a literal. <p>For example, if the path is %WINDIR%\SMS.INI, then the final path (assuming WinDir=C:\WINNT) will be C:\WINNT\SMS.INI.</p> <p>But if the path is %WinDir%\SMS.INI, then no substitution will take place and the file extract will fail. This is done to ensure that it is possible to extract files from a directory or a file that has one or more % signs in the name.</p> <p>Another example of using an environment variable is as follows:</p> <p>You can type: %HOME%/.bashrc , or %SYSTEMDIR%\win.ini. In this case, %HOME% will be replaced with the value of the HOME environment variable.</p> <p>This is applicable to all platforms, and UNIX notation of the form \$NAME is not supported.</p>



Parameter	Description
Search	<p>Determines what information is to be extracted.</p> <ul style="list-style-type: none"> • A search string expression can be created in two ways depending on the file contents: • If you type * (an asterisk) for the search string, the scanner takes the complete first line of the file. <p>The scanner can find a line beginning with a particular anchor in a text file, and extract the rest of the line following the anchor. For example, if the line of the file has the following structure VariableName=Value, and Value needs to be extracted, set the search string to be VariableName=</p> <p>Note:</p> <ul style="list-style-type: none"> • The search string is case insensitive. • In the file being extracted from, if a comment is on the same line as the search string, then the comment is also returned. To prevent this happening, ensure that any comments in the file are placed on separate lines from the search string. This is particularly relevant to UNIX users.

WMI Extract Fields

Windows Management Instrumentation (WMI) is a component of the Microsoft Windows operating system that provides management information.

Some data on Windows operating systems is only available via the WMI interface. This type of field allows the scanner to be configured to extract and store specific pieces of WMI data. The Windows scanner populates this field on computers where WMI is enabled.

Parameter	Description
Query	<p>Windows Management Instrumentation Query Language (WQL) is a subset of SQL that is used to make data queries inside WMI.</p> <p>WQL Query. The following example of a WQL query collects the name and the frequency properties of the installed processor:</p> <p>For example, <code>select Name,CurrentClockSpeed from Win32_Processor</code></p> <p>For more information about WMI and WQL refer to the Microsoft MSDN website.</p> <ul style="list-style-type: none"> • WQL Query. The WQL query used to make data queries in WMI. <p>For example, <code>select Name,CurrentClockSpeed from Win32_Processor</code></p> <p>The above query collects the name and the frequency properties of the installed</p>

Parameter	Description
	<p>processor.</p> <ul style="list-style-type: none"> • Object Path. Should usually be: <code>root\cimv2</code> This is the default path for CIM v2 data provided by WMI. • Timeout. Specifies how long (in seconds) to wait until the query returns a single instance of the queried data. If no data is returned within this period, the query returns nothing and the value of the field is blank. <p>Note: You can use <code>-1</code> to wait indefinitely for the query to return data. However, this is not recommended since it may cause the query to hang.</p>
Options	<ul style="list-style-type: none"> • Collect the first instance/Collect all instances. Determines whether to collect information from the first instance only, or from all instances. For example, if there are several processors in a computer you can choose to collect the information about the very first processor or about all processors. If instances are requested, their values are separated with the string specified in the Separate Instance With field. When multiple properties are specified, the values returned by the query will be separated with the string specified in the Separate Property Values With field. • Separate Instance With. When Collect all instances is selected, the values collected from each instance are separated with the string specified here. • Separate Property Values With. When multiple properties are specified, the values returned by the query are separated with the string specified here.
Output Properties	<p>Enables you to add a property whose value is required in the asset field. The WQL query returns an instance of the WMI class which can have many properties. The required properties need to be specified manually.</p> <p>For example: <code>select * from Win32_Processor</code></p> <p>This returns all properties for processor, but if Name is required, it should be specified in the Output Properties box.</p> <ul style="list-style-type: none"> •  . Enables you to add an output property. •  . Enables you to remove the selected output property.

Derived Fields

Derived fields have dependencies on the data of other types of fields. That is, the data they contain is derived from other fields.

- ["Sequence Fields" below](#)
- ["Combination Fields" on the next page](#)
- ["OS/Scan Fields" on page 557](#)

Sequence Fields

The Sequence field enables you to define a sequence of up to ten asset or hardware fields. Each of these fields returns a value depending on the machine or environment running. The value returned as the result of the sequence field is the first of these fields containing a non-blank value.

Parameter	Description
Field Sequence	<p>The sequence of the field.</p> <p>Expand the tree on the right and drag a field to the File Name list on the left.</p>
Ignore Strings	<p>Used to specify a set of values that are known to be incorrect, fake, or unwanted. These values should be ignored.</p> <p>For example, when specifying a MAC address as one of the hardware fields in a sequence, you can designate the known fake MAC addresses in the Ignore Strings so that they can be filtered out.</p> <p>A blank field can be defined based on either of the following two criteria:</p> <ul style="list-style-type: none">• The string matches an ignore string.• The length of the field is shorter than the number specified in the Shorter Than field.• Matching. A string or a set of strings. <p>For example, you can define a set of ignore strings as Unknown;unknown;Not Tested.</p> <p>Note: The string is case-sensitive; strings must be separated by semicolons (;).</p> <p>If the content of the sequence field matches (is equal to) any of the strings specified here, the field is considered to be blank. For example, if the string Not Found is defined here, then a field that has the value 'Not Found' is considered to be blank.</p> <p>You can type a string in the form: *STRING*. Here the asterisks (*) are ignored and any string that contains the texts between the two asterisks will also be ignored.</p> <ul style="list-style-type: none">• Shorter Than. Specifies the minimum length of the string to be considered as non-blank. <p>If a field value's length is shorter than the specified number, then the field is ignored</p>

Parameter	Description
	<p>and considered blank.</p> <p>Default: Minimum: 1; Maximum: 255</p> <p>Note: An empty value's length is 0; an empty field is always ignored.</p>



Combination Fields

These fields can combine up to five asset or hardware fields into a single field. This is particularly useful for the **Description** field.

The combination field is made up by string substitution.

For a detailed example on setting up a Combination type asset field, see ["How to Set Up Asset Fields for Data Collection - Example" on page 558](#).

Parameter	Description												
Master substitution string	<p>The template substitution string that makes up the combination field.</p> <p>This string replaces the percent values (for example, %1) with the appropriate hardware or asset item.</p> <p>Syntax: Use the percentage symbol followed by a number.</p> <p>Note: You can also specify some text before or after the percent notation which will be a constant part of the value of the field.</p> <p>Examples</p> <ul style="list-style-type: none"> • '%1 (%2)' • If the master substitution string %1 %2MHz %3Mb is defined for the Description field in the asset entry form, where the following index definitions apply: <table border="1"> <thead> <tr> <th>Index</th> <th>Field/Description</th> <th>Display</th> </tr> </thead> <tbody> <tr> <td>%1</td> <td>CPU Data\CPU\CPU Type</td> <td>CPU Type</td> </tr> <tr> <td>%2</td> <td>CPU\CPU Speed (MHz)</td> <td>CPU SpeedMHz</td> </tr> <tr> <td>%3</td> <td>Memory Data\Total memory (Mb)</td> <td>Total MemoryMb</td> </tr> </tbody> </table> <p>then Description field may look as follows:</p> <p>Core i7 2666MHz 3958Mb</p>	Index	Field/Description	Display	%1	CPU Data\CPU\CPU Type	CPU Type	%2	CPU\CPU Speed (MHz)	CPU SpeedMHz	%3	Memory Data\Total memory (Mb)	Total MemoryMb
Index	Field/Description	Display											
%1	CPU Data\CPU\CPU Type	CPU Type											
%2	CPU\CPU Speed (MHz)	CPU SpeedMHz											
%3	Memory Data\Total memory (Mb)	Total MemoryMb											

Parameter	Description
Definitions	<p>Displays the fields selected from the Fields tree (on the right) to be used in the substitution string.</p> <p>The list can contain up to five index entries (represented as %1, %2, %3, %4 and %5).</p>
<Right-click menu>	<ul style="list-style-type: none"> To insert a field into the Definitions pane, right-click the field in the Fields tree and click Add . To remove a field from the Definitions pane, right-click the field and click Delete .

OS/Scan Fields

These fields allow the definition of multiple types of data sources to provide an automatic entry depending on the scanner used and the operating system being scanned.

This type of asset field is useful in situations when you want to scan multiple operating systems but want to collect the same piece of information for each from different sources.

For example, the data can be extracted from the registry on Windows or from a file on UNIX and Mac OS X.

Parameter	Description
Field Index	<ul style="list-style-type: none"> The operating system affected by this definition. Drop-down list: Links the operating system to the line numbers of the relevant field in the Fields referred to list.
Fields Referred to	Fields selected from the Fields tree (on the right) to be included in this definition. Can be any existing asset field or any hardware/configuration field (except hardware fields where multiple values may be collected, such as CPU type or IP address).
Fields tree	Displays the available fields.

Order of the Fields in the Form

You must consider the order of the fields in the form, and move them round accordingly. The rule is:

A field cannot depend on a field that is placed below it in the form.

That is, if you have set up any derived or automatic fields that require data from fields below them in the form, you must move them to a position in the form that is above these fields.

To correct the order of the field in the form:

1. Reorder the fields by clicking on a row and dragging the selected line to its new location in the form.
2. When you click **Next** in the **Asset Data** page, a confirmation message may be displayed.
3. Click **Yes** to have the Scanner Generator automatically reorder the fields.
4. Click **No** to reorder the fields manually.


How to Set Up Asset Fields for Data Collection - Example

This example describes how to set up a **Combination** type asset field.

Combination fields can combine up to five asset or hardware fields into a single field. This is particularly useful for the **Description** field.

In this example, the field combines the first and last names of an employee, and the department he works for, into one field, with the following format

```
<First name> <Last Name> - <Department>
```

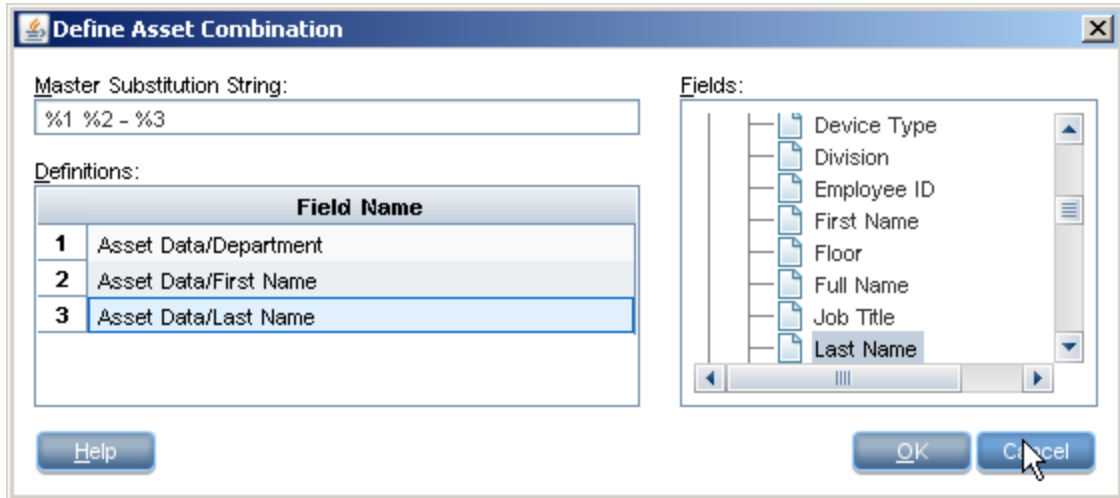
1. In the Scanner Generator wizard, go to the **Asset Data** page > **Asset Data** tab.
2. Select **Description**, and click **Edit Field** .
3. Configure the asset field as described in "[Asset Field Configuration Dialog Box](#)" on page 632.
 - a. In the **Caption** field, type **Employee**.
 - b. Select a field data type: Under **Derived Fields**, select **Combination Field**.
 - c. Next to the **Parameter** box, click **Change** to define parameters for the combination field.
4. Build the master substitution string to yield the desired format. In the **Master Substitution String** field, enter

```
%1 %2 - %3
```

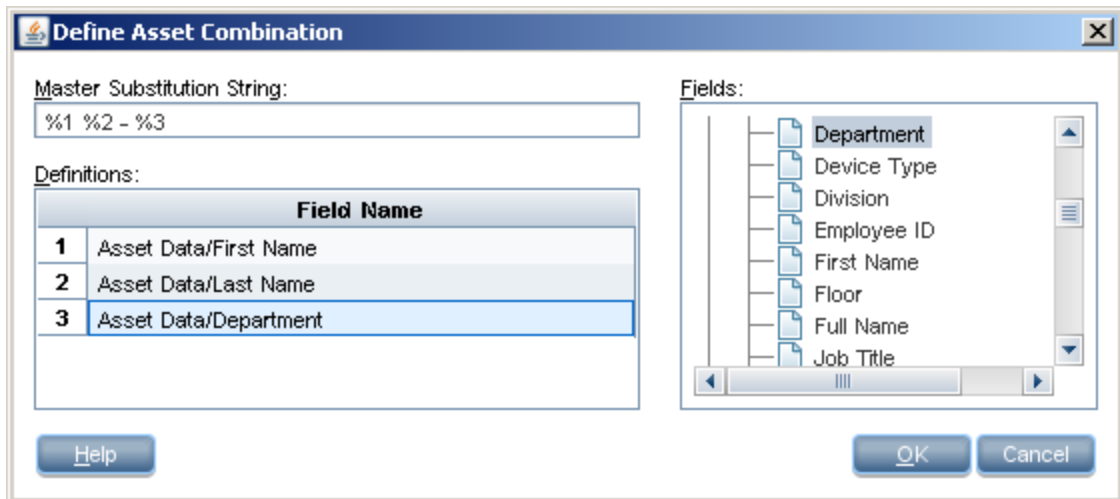
5. Select the asset fields that you want to appear in the resulting field.

In the **Fields** tree:

- a. Under **Asset Data**, double-click **Department**.
- b. Under **Asset Data**, double-click **First Name**.
- c. Under **Asset Data**, double-click **Last Name**.



6. To display **Department** after the name, in the **Definitions** grid, drag **Department** down to the third place in the list.



The numbers in the **Definitions** grid correspond to the numbers in the **Master Substitution String** field. So:

- %1 will be replaced with First Name (#1 in the grid)
- %2 will be replaced with Last Name (#2 in the grid)
- %3 will be replaced with Department (#3 in the grid)

Result

If the first name is **John**, the last name is **Doe**, and the department he works in is **Research and Development**, the resulting combination field string will be:

John Doe - Research and Development

How to Set up the Scanner to Handle Delta Scan Files in Manual Deployment Mode

When conducting an inventory in Manual Deployment mode, for the delta scan file processing in the XML Enricher to work correctly, ensure you do the following:

1. Configure the Scanner to save scan file results locally and enable delta scanning

On the **Scanner Generator > Scanner Options > Saving** tab page, select the **Save results locally** option and the **Enable Delta Scanning** option. For more information, see ["Scanner Options Page" on page 635](#).

2. Configure the Scanner to save scan results to the Incoming directory.

- On the **Scanner Generator > Scanner Options > Saving** tab page, select the **Save result to network (off-site)** option. For more information, see ["Scanner Options Page" on page 635](#).
- Depending on whether HTTP or HTTPS is used for off-site scan file saving, the **save file** path should be as follows:
 - HTTP: **http://localhost:1977/incoming**
 - HTTPS: **https://localhost:8453/incoming**

where:

- **1977** is the default Probe Manager JMX port. If the Probe Manager JMX was configured to use a different port, 1977 in the URL above needs to be replaced with the corresponding probe manager port.
- **8453** is the default HTTPS port. If a different port is used (as described earlier), 8453 in the URL above needs to be replaced with the corresponding HTTPS port.
- **DataFlowProbeHost** is the host name or the IP address (IPv4/IPv6) of the Data Flow Probe machine.
- By default, the Data Flow Probe shares the Incoming and Original directories via HTTP.

- The Data Flow Probe can be configured to share these directories via HTTPS instead.

The following entries in the **DataFlowProbe.properties** file (located in **C:\hp\UCMDB\DataFlowProbe\conf**) control the HTTPS behavior. The settings are defined, by default, as follows:

- **jettyHttpsEnabled** = true
- **jettyHttpsPort** = 8453

To disable HTTPS, set **jettyHttpsEnabled** = false.

To configure HTTPS port by modifying the **jettyHttpsPort** setting.

- When the Data Flow Probe is installed, user credentials are provided for uploading scan files to the Data Flow Probe. These credentials are stored in the **DataFlowProbe.properties** file on the Data Flow Probe.

To change the user name:

In the **DataFlowProbe.properties** file locate **com.hp.ucmdb.discovery.Probe.JMX.UploadAuth.User** and replace the value with the new user name.

To change the password:

- A. Access the Data Flow Probe JMX console. On the probe machine, launch a Web browser and enter the following address: **https://localhost:8453**.

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

Note: If you have not created a user, use the default user name **sysadmin** and the password to log in.

- B. Search for **type=mainProbe**, and click the link.
- C. Click **getEncryptedKeyPassword**, enter a new password, and click **Invoke**.
- D. Copy the generated value to the Clipboard.
- E. In the **DataFlowProbe.properties** file locate **com.hp.ucmdb.discovery.Probe.JMX.UploadAuth.Pwd** and paste the new encrypted password over the old value.

Note: You can also use the command line option **-p:<path>** with the Scanner to override the selection made in the Scanner Generator.

3. Configure the path to the Original directory.
 - On the **Scanner Generator > Scanner Options > Saving** tab page, set the **Path to Original**

Off-Site Scan Files option. For more information, see "[Scanner Options Page](#)" on page 635.

Depending on whether HTTP or HTTPS is used for off-site scan file saving, the path should be as follows:

- HTTP: **http://DataFlowProbeHost:1977/original**
- HTTPS: **https://DataFlowProbeHost:8453/original**

The special user, **UploadScanFile**, with the corresponding password should be configured for the original directory.

Note:

- You can also use the Scanner **-r:<path>** command line option to specify the location of this directory.
- In addition to the default HTTP/HTTPS options, you can configure manual deployment Scanners to store the off-site scan files using the following:
 - **File Share.** This is usually only suitable for Windows platforms. The **Incoming** and **Original** directories of the XML Enricher can be shared via Windows shares. For example: **Incoming\$** and **Original\$**, then the off-site scan file path and the original scan path in the Scanner Generator can be configured as the following UNC paths: **\\DataFlowProbeHost\\Incoming\$** and **\\DataFlowProbeHost\\Original\$**. Make sure that these shares/NTFS permissions on these directories allow appropriate access to all users, under the user's account through which the manual deployment Scanners are to be executed.
 - **FTP/FTPS.** The Incoming and Original directories of the XML Enricher can be shared via FTP/FTPS protocols. The Data Flow Probe does not include an FTP/FTPS server, but either a standard Windows FTP server supplied with IIS can be installed or enabled, or a suitable 3rd-party server can be installed for this purpose.

The FTP/FTPS URLs must be configured for off-site scan saving. For example: **ftp://DataFlowProbeHost/incoming** and **ftp://DataFlowProbeHost/original**.

How to Configure XML Enricher to Suit the Probe Deployment Mode

When the Data Flow Probe is installed, the XML Enricher is configured, by default, for the Standard Deployment mode.

Note: The XML Enricher's Windows service is configured with the Manual start up and the probe starts the XML Enricher service on demand when necessary. So you should not change the startup mode of the XML Enricher service.

If another Probe deployment is used, the XML Enricher settings must be manually adjusted to fit the deployment mode of the Probe.

Note:

- The XML Enricher configurations described below have been tested against the Data Flow Probe deployment modes.

However, other configurations may potentially be supported, provided that enough resources (memory and CPU) are available for the XML Enricher.

For details about the Data Flow Probe deployment modes, see the *Universal CMDB Support Matrix* document.

- This task relevant for Data Flow Probes meant for discovery (on Windows machines) only.

This task includes the following steps:

- ["Configure the XML Enricher parameters" below](#)
- ["Restart the XML Enricher" on page 566](#)
- ["Results " on page 566](#)

1. Configure the XML Enricher parameters

Configure the XML Enricher parameters to suit the Data Flow Probe deployment mode:

- a. Set the XML Enricher mode and maximum amount of memory allocated by the Java Virtual Machine for the XML Enricher service, per the Data Flow Probe's deployment mode:

- i. On the Data Flow Probe machine, locate the **WrapperEnricher.conf** file in the following folder:

c:\hp\UCMDB\DataFlowProbe\bin\xmlenricher

- ii. Open the file in any text editor.
- iii. In the **Java Additional Parameters** section, locate the following parameter, and set the value per the Data Flow Probe deployment mode:

Parameter	Description								
DsaiDataProvider	The XML Enricher mode.								
	<table border="1"> <thead> <tr> <th>Probe Deployment</th> <th>Mode</th> </tr> </thead> <tbody> <tr> <td>Small</td> <td>Database</td> </tr> <tr> <td>Standard</td> <td>Memory</td> </tr> <tr> <td>Enterprise</td> <td>Memory</td> </tr> </tbody> </table>	Probe Deployment	Mode	Small	Database	Standard	Memory	Enterprise	Memory
	Probe Deployment	Mode							
	Small	Database							
Standard	Memory								
Enterprise	Memory								

- iv. In the **Maximum Java Heap Size (in MB)** section, locate the following parameter, and set the value per the Data Flow Probe deployment mode:

Parameter	Description								
MaxMemory	The maximum amount of memory that the Java Virtual Machine allocates for the XML Enricher service.								
	<table border="1"> <thead> <tr> <th>Probe Deployment</th> <th>Maximum Memory</th> </tr> </thead> <tbody> <tr> <td>Small</td> <td>3584</td> </tr> <tr> <td>Standard</td> <td>5120</td> </tr> <tr> <td>Enterprise</td> <td>8192</td> </tr> </tbody> </table>	Probe Deployment	Maximum Memory	Small	3584	Standard	5120	Enterprise	8192
	Probe Deployment	Maximum Memory							
	Small	3584							
Standard	5120								
Enterprise	8192								

- b. Configure the maximum number of processing threads to allocate to processing scan files in the XML Enricher service for all management zones:

- i. On the Data Flow Probe machine, locate the **enricher.properties** file in the following folder:

c:\hp\UCMDB\DataFlowProbe\conf

- ii. Locate the following parameter, and set the value per the Data Flow Probe deployment mode:

Parameter	Description	
max_enricher_thread_number	Probe Deployment	Threads
	Small	1
	Standard	2
	Enterprise	4
Note: One thread is used initially. For Standard and Enterprise deployment, the actual number of threads used is gradually increased by 1, depending on load conditions and up to the maximum number of threads (configured in this setting).		

2. Restart the XML Enricher

Restart the **Universal Discovery XML Enricher** service on the Data Flow Probe machine.

3. Results

Navigate to

c:\hp\UCMDB\DataFlowProbe\runtime\xmlenricher\scans\incoming

and analyze whether the scan file processing is at an acceptable level.

If there is a large build up of the scan files in the **incoming** directory that does not get cleared after some time and continues to grow, this indicates that the XML Enricher's does not have enough resources to process scan files. In this case, the number of threads needs to be increased.

Verify the number of threads that the XML Enricher service is using. For details, see ["How to Check XML Enricher Health Using JMX" on page 568](#).

When increasing the number of threads, the amount of memory allocated to the JVM needs to be increased as well. If the Standard mode parameters are not sufficient, use the parameters for the Enterprise mode deployment.

How to Configure the Maximum Number of Threads to Process Scan Files

This task describes how to configure the maximum number of processing threads to allocate to processing scan files in the XML Enricher service for all management zones.

Note: This is a global parameter.

To configure the maximum number of threads to process scan files:

1. Prerequisites

Ensure that the Data Flow Probe is running.

2. Open the file

Open **<Probe installation folder>\conf\enricher.properties** file using any text editor.

where **<Probe installation folder>** is where you installed the Data Flow Probe.

3. Set a value for the maximum number of threads

Locate the parameter **max_enricher_thread_number=** and set a value.

- **Default:** 2
- One thread is used initially. Then the number gradually increases by 1, depending on load conditions.

The increase in the maximum number of threads needs to be done in concert with increasing the amount of memory for the XML Enricher. For details about this parameter, see [How to Configure XML Enricher to Suit the Probe Deployment Mode](#).

4. Restart the Data Flow Probe

Restart the Data Flow Probe service.

5. Results

- a. Navigate to **<DataFlowProbe>\runtime\xmlenricher\scans\incoming** and analyze whether the scan file processing has increased to an acceptable level. If not, consider increasing the value that you set in [step 3](#).
- b. Verify the number of threads that the XML Enricher service is using. For more information, see [How to Configure XML Enricher to Suit the Probe Deployment Mode](#).

How to Check XML Enricher Health Using JMX

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

1. Prerequisites

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

2. Connect to the Data Flow Probe

On the probe machine on which the XML Enricher service is running, launch your Web browser and enter the following address: **https://localhost:8453**.

3. View statistics

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

4. Results

Health statistics for the XML Enricher are displayed.

How to Limit the XML Enricher Port to Allow Local Connection Only

The port 34545 only listens on localhost when a Data Flow Probe is newly installed. However, for Data Flow Probes upgraded to the latest version, to limit the XML Enricher port to allow local connection

only, you need to perform a manual step.

To do so,

1. On the Data Flow Probe machine, locate the **WrapperEnricher.conf** file in the following folder:
c:\hp\UCMDB\DataFlowProbe\bin\xmlenricher
2. Open the file in any text editor.
3. Add the following setting to the **wrapperEnricher.conf** file manually.

```
# Make rmi listen on localhost only  
wrapper.java.additional.<the number>=-Djava.rmi.server.hostname=localhost
```

Note: Make sure this line is added to the end of settings starting with **wrapper.java.additional**.

For subsequent settings, make sure you manually adjust the value of *<the number>* part so that they are properly numbered.

4. Save the file.
5. Restart the Data Flow Probe.

How to Reprocess Scan Files

This task describes how to reprocess scan files.

1. Right-click a **Node CI** or any of its subtypes.
2. Select **Actions > Reprocess Scan File**. The scan file is moved from the **Processed** folder to the **Incoming** folder and then reprocessed.

For more information about reprocessing scan files, see ["Processing Scan Files" on page 519](#).

How to Import SAIs to the Data Flow Probe

This task describes how to import SAI files and then deploy the files to the Data Flow Probe. SAI files can be master delta files that are contained in Content Packs, or files can be User SAIs that are created using the SAI Editor. You can also use SAI files created by third parties.


Note: If you want to install the entire contents of a Content Pack, see the *UCMDB Discovery and Integrations Content Pack Release Notes*

To import SAIs to the Data Flow Probe:

1. Prerequisites

- Ensure that the UCMDB Server is running.
- Ensure that the Data Flow Probe server is running.
- Do one of the following:
 - Download a Content Pack from [ITOM Marketplace](#).
 - Ensure that user SAI files are stored on your computer.

2. Import the SAI files

Data Flow Management > Software Library, in the SAI Files pane, click  and select **Import SAI File** or **Import SAI file from CP**. For more information about these options, see "[SAI Files Pane](#)" on page 682.

3. Results

The Data Flow Probe is updated with the SAI files. To verify this, check the files at **C:\hp\UCMDB\DataFlowProbe\runtime\probeManager\discoverySaiResources\saiRuntime**.

Note: If you want to re-process scan files, see "[How to Reprocess Scan Files](#)" on the [previous page](#).

How to Import Normalization Rules to the Data Flow Probe

This task describes how to import normalization or discovery rules files and then deploy the files to the Data Flow Probe. These files are contained in Inventory Discovery Knowledge Pack.


Note: If you want to install the entire contents of a Content Pack, see the *UCMDB Discovery and*

Integrations Content Pack Release Notes.

1. Prerequisites

- Ensure that the UCMDB Server is running.
- Download a Content Pack from [ITOM Marketplace](#).

2. Import the normalization rules files

In **UCMDB > Adapter Management > Resources Pane**, click  and select **Import Normalization Rules from Content Pack**. For more information about this page, see "[Resources Pane](#)" on page 285.

3. Results

The Data Flow Probe is updated with the normalization rules files. To verify this, check the files at **C:<DataFlowProbe>\runtime\probeManager\discoveryResources\ruleEngine** where **<DataFlowProbe>** is the location where the Data Flow Probe server is installed.

How to Configure and Optimize Inventory Discovery

This task describes how to configure Inventory Discovery to improve recognition and to improve performance.

This task includes the following steps:

- "[Analyze discovery results](#)" below
- "[Optimize recognition](#)" below
- "[Increase performance](#)" on the next page

Analyze discovery results

- To analyze scan files, see "[Inventory Tools](#)" on page 534.

Optimize recognition

- To teach applications, see ["Application Teaching" on page 527](#).
- To configure software recognition options, see ["XML Enricher: Software Recognition Configuration Dialog Box" on page 650](#).

Increase performance

- To configure to use delta scan files, see ["How to Set up the Scanner to Handle Delta Scan Files in Manual Deployment Mode" on page 561](#).
- To optimize the XML Enricher engine, see ["Scan File Processing Power" on page 520](#).

How to Configure Analysis Asset Fields

The Analysis Asset Field configuration settings that affect the XML Enricher cannot be modified in the Web UI. You can change these settings by using the Viewer. To do this, follow these steps:

1. Select **Start > All Programs > UCMDB > Inventory Tools > Viewer** on the computer where the Data Flow Probe is installed.
2. Use **File > Options > Asset Fields** to configure the Analysis Asset Fields.

For more information, see ["Inventory Tools" on page 534](#).

How to Map Scan File Attributes to UCMDB

This task describes how to map attributes that are contained in scan files to UCMDB CIs.

This task includes the following steps:

1. ["Prerequisites" on the next page](#)
2. ["Select a CI to map" on the next page](#)
3. ["Select attributes to map" on the next page](#)
4. ["Results" on the next page](#)



1. Prerequisites

Before creating a mapping, perform an analysis on what information you want to map, what data element in the scan file contains the information you want to capture, where the data element in the scan file is located, and which UCMDB CI you want to store this information.

2. Select a CI to map


- a. Open the Hardware Mapping Configuration dialog box. To do this, perform one of the following:

Note: Alternatively, advanced users can manually edit the **ParseEnrichedScanFile.py** script file to create complex topologies. There is a commented out sample available in this script that demonstrates how to map the **hwAssetDescription** asset field to the node's **Description** attribute.

- i. **Adapter Management > Inventory Discovery by Scanner > Adapter Definition** tab, expand the **Global Configuration Files** pane, click **HardwareMappingConfig** and then click **Edit** .
 - ii. **Inventory Discovery Activity > Preferences Page**, then click the **Custom Mapping** button. For more information, see the section describing the Inventory Discovery Activity in the *Universal CMDB Discovery and Integrations Content Guide*.
- b. Click **Select CI**  to select a CI. The Select CI dialog box opens.

Note: This option is only available when **Hardware Mapping Configuration** is selected in the left pane.
 - c. Select a CI that you want to create a mapping.
 - d. In the CI Editor, select properties for the selected CI.

3. Select attributes to map

- a. Click **Select Attributes**  to select attributes. The Select an Attribute dialog box opens.
- b. Select properties for the selected attribute in the Attribute Editor.

4. Results

Verify that data in the scan file was mapped as expected to UCMDB by using the CI Type Manager. For more information, see "CI Type Manager" on page 1 in the *Universal CMDB*

Modeling Guide.

Mapping Hardware or Asset Fields to UCMDB - Use-Case Scenarios

This document describes common scenarios for customized mappings of data from scan files to UCMDB.

For a task related to this scenario, see ["How to Map Scan File Attributes to UCMDB" on page 572](#).

For concept details, see ["Custom Hardware or Asset Mapping" on page 534](#).

These use cases assume that the scanner has captured the data that you want from the target machine, and that the scanner has written the data to the scan file. Configuring the scanner to collect data and store it in an empty field in the scan file is beyond the scope of this document. For more information, see ["Asset Data Page" on page 630](#).

Note:

- The field names and attribute names described in this document are merely examples. The attribute names were selected because they should not impact out-of-the-box reconciliation rules in UCMDB. Before mapping, always perform an analysis to ensure that storing data in scan file fields and in CIs will not impact other data, or impact reconciliation. For information about reconciliation, see ["Reconciliation Overview" on page 739](#).
- Generally, most hardware and asset-related information is stored in an attribute under Node CI. If you create your own CI to store your data, it is recommended to create a relationship between your new CI and Node CI.

Tip: you can map several strings of data from scan file fields to several CI attributes as long as the CI attributes belong to the same CI in a single pass through the wizard. For example, to map String1 to NodeCI and to map String 2 to Node2CI. you must make two passes through the wizard.

User Scenario 1 (single attribute to existing CI)

This use-case scenario describes how to map a single string of hardware or asset data that is contained in a scan file field to an existing UCMDB CI attribute.


1. Background

Assume the following:


- Your scanner has written the collected data to the **hwAssetField1** field in the scan file.
- You want to store hardware and asset-related information in Node CI.

Tip: To learn about mapping data to a new CI that you create, skip to the next scenario on this page.

2. Select a CI that contains the attribute that you want to contain your mapped data

- a. Open the Hardware Mapping Configuration dialog box. For more information, see "[Hardware Mapping Configuration Dialog Box](#)" on page 600.
- b. Click . In the Select CI dialog box, expand **Configuration Item**, expand **Infrastructure Element**, and select **Node**. Click **OK**.
- c. Accept all of the defaults in the CI Editor. Notice that **Node** appears in the left tree pane.


3. Select an attribute to store your mapped data

- a. In the left tree pane, ensure that **Node** is selected and click . The Select an Attribute dialog box opens. This list contains all attributes for the Node CI.

Note: The list is not sorted alphabetically.

- b. In the Select an Attribute dialog box, click the Attribute field and select the **Note** attribute. Accept the defaults and click **OK**. Notice that this attribute name appears in the left tree pane.

Note: The **Note** attribute is a common attribute and data stored here will not cause any reconciliation rule issues. However, you can choose another available attribute. To see which attributes are not populated, or which attributes contain non-critical data, perform an analysis using the CIT Manager in UCMDB.

- c. In the Attribute Editor on the right pane, in the **Value** field, click . The Select a Shell Tag dialog box opens. Expand **Asset Data** and select the name of the scan file field that contains the data that you want to map.

Note: The names in this list are friendly names- mouse over each entry to see the scan file XML tag names for each entry. For example, **user field 1** is also called **hwAssetField1**.

- d. Select the **user field 1** attribute. Accept all defaults and click **OK**.

4. Results

After the Inventory Discovery by Scanner job runs, ensure that your mapped data is contained in **Node.Note** in UCMDB.

User Scenario 2 (multi-attribute to new CI)

This use-case scenario describes how to map multiple strings of hardware or asset data that is contained in scan file fields to multiple attributes under a newly-created UCMDB CI.

1. Background

Assume the following:

- Your scanner has written collected data to the **hwAssetField1** field and written collected data to **hwAssetField2** field in the scan file.
- You want to map the data to attributes under a new CI. Let assume the following about your new CI:


Note: For more information, see the section on how to create a new CI in the *Universal CMDB Modeling Guide*.

- You named your new CI **NewCI**.
- **NewCI** CI has some relationship defined with Node CI.



Note:

- Note the relationship type.
- Generally, most hardware and asset-related information is stored in an attribute under a CI that is connected, or has some relationship with **Node** CI.

2. Select your new CI

- a. Open the Hardware Mapping Configuration dialog box. For more information, see "[Hardware Mapping Configuration Dialog Box](#)" on page 600.
- b. Click . In the Select CI dialog box, select your newly-created CI. Select **NewCI**.
- c. In the relationship field, select the relationship type that you selected when setting up the CI in the CI Type Manager.
- d. In the Create New CI field, select **Yes**.
- e. Accept all of the defaults in the CI Editor. Notice that **NewCI** appears in the left tree pane.

3. Select attributes to store your mapped data

- a. In the left tree pane, ensure that **NewCI** is selected and click . The Select an Attribute dialog box opens. This list contains all attributes for **NewCI** CI.
 - These attributes were inherited based on which parent you selected when you created your new CI.
 - The list is not sorted alphabetically.
- b. Click the Attribute field and select the **Note** attribute. Accept the defaults and click **OK**. Notice that this attribute name appears in the left tree pane.
- c. In the Attribute Editor on the right pane, click the  in the **Value** field to open the Select a Shell Tag dialog box. Expand **Asset Data** and select the name of the scan file field that contains the data that you want to map.

Note: The names in this list are friendly names- mouse over each entry to see the actual tag names for each field. For example, **user field 1** is also called **hwAssetField1**.
- d. Select the **userfield1** attribute.
- e. Accept all defaults and click **OK**.
- f. Repeat this step to map your second string of data. For example, select the **UserLabel** attribute to store your data, and then select **user field 2** for the **Value** field.

4. Results

After Inventory Discovery by Scanner has run, ensure that your mapped data is contained in **NewCI.Note** and **NewCI.UserLabel** in UCMDB.

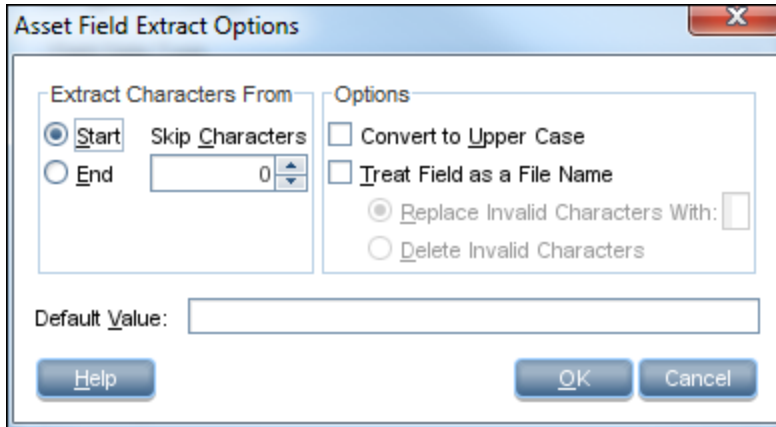
How to Set Extract Options

All calculated asset fields defined can be set up so that only part of the string is selected instead of the entire string. They can also be set up, for example, to use the last part rather than the first part of the string. This can be useful for obtaining the last part of a calculated field that is too long.

Various other settings for manipulating the field contents are also available.

To set extract options:

1. After you have selected the field data type, click **Extract**. The button is only enabled for those field that are calculated. This option is not available for user-entered fields. The **Asset Field Extract Options** dialog box is displayed.



2. In the **Extract Characters From** group box, specify whether you want to use the last part or the first part of the string. Select one of the following options:
 - o **Start** - Uses the first part of the string. Use the arrows next to the **Skip characters** box to specify how many characters are to be skipped from the beginning of the string.
 - o **End** - Uses the last part of the string. Use the arrows next to the **Skip characters** box to specify how many characters are to be skipped from the end of the string.

For example, **ABCDEF123**. If you select **End** and skip **4** characters, the result is **ABCDE**.

3. In the **Options** group box, select the options as follows:
 - o **Convert to Upper Case**- Select this option to convert the alphabetic characters to upper case, if required.
 - o **Treat Field as a File Name**- Select this option to treat the string in the asset field as a file name.

Some characters are invalid in file names, so any invalid characters can be replaced with the character specified in the **Replace Invalid Characters With** box. For example, underscore (**_**) is a valid file name character and can be used to replace invalid characters.

If you select the **Delete Invalid Characters** option then any invalid characters are deleted.

4. If the extracted field is empty or is not found, then a default value for the string can be specified in the **Default Value** box. For example, if the text string **Not Found** is entered in this box, then an empty field or a field that has not been found is assigned this default value.


Configure Filtering in UCMDB

This task describes how to use the UCMDB interface to filter the UCMDB CIs that are discovered.

1. Prerequisites

Before creating a filter, perform an analysis on what information you want to map and what data element in the scan file contains the information you want to filter.


2. Select a CI to filter

- a. Select **Adapter Management**.
- b. In the Resources tree, expand the **DDMiInfra** node and then expand the **Configuration Files** node.
- c. Right-click **GlobalFiltering.xml** and select **Open in Frame**.
- d. In the Global Filtering dialog box, click **Include** or **Exclude**.
 - **Include**. All CIs that do not match the filter are removed. If this marker is left empty, all results are sent to the server.
 - **Exclude**. All CIs that match the filter are removed. If this marker is left empty, all results are sent to the server.
- e. Click **Select CI Type** . The Select CI Type dialog box opens.

Note: This option is only available when **Include** or **Exclude** is selected in the left pane.

- f. Select a CI for which you want to create a filter, and click **OK**.

3. Select attributes to filter

- a. Click **Select Attribute** . The Select an Attribute dialog box opens.
- b. Select properties for the attribute, and click **OK**.

Note: You can use the "between" operator when filtering results, but only when the Object class is "ip_address" and the attribute name is "name".

For details on CI attribute types, see "Attributes Page" in the *Universal CMDB Modeling Guide*.

4. Activate and configure settings

In the Global Filtering Configuration Settings pane, select your options.

Available when: **Global Filtering Configuration** or **Include** or **Exclude** is selected in the left pane.

5. Results

Use the CI Type Manager to verify that data is filtered as expected in UCMDB. For more information, see "CI Type Manager" in the *Universal CMDB Modeling Guide*.

How to Enable Discovery of App-V Applications

This task describes how to enable detecting, recognizing, and utilization reporting for App-V virtual applications.

Note: For information on supported technologies, see ["Application Virtualization Supported Technologies" on the next page](#).

This task includes the following steps:

- ["Prerequisites " below](#)
- ["Configure package rule" below](#)
- ["Run Inventory Discovery" on the next page](#)
- ["Results " on the next page](#)

1. Prerequisites

- Install the Software Utilization plug-in on the discovery node. For more information, see ["How to Configure Software Utilization" on page 708](#).
- Install Microsoft App-V client version 5.0 on the discovery node.
- Ensure that Microsoft PowerShell is installed on the discovery node.

2. Configure package rule

To configure a package rule, see the section that describes configuring package rules in the *Inventory Tools User Guide* PDF document. For more information, see ["Inventory Tools" on page 534](#).

3. Run Inventory Discovery

Run Inventory Discovery. For more information on running Inventory Discovery, see the *Universal CMDB Discovery and Integrations Content Guide*.

4. Results

The **Installed Software** CI is populated with information about App-V virtual applications. For more information about CIs, see CI Selector in the *Universal CMDB Modeling Guide*.


Application Virtualization Supported Technologies

The following virtual application technologies are supported:

- Microsoft Application Virtualization (App-V)

How to Rename Scanner Executable Files

You can rename the file name for scanner executables when performing Inventory Discovery by Scanner.

1. Select **Universal Discovery > Discovery Modules/Jobs** tab > **Discovery Modules** pane > **Inventory Discovery by Scanner** job > **Properties** tab.
2. Expand the **Global Configuration Files** pane, click **ScannersConfigurationbyPlatform.xml**, and then click . The Script Editor opens.
3. In the Script Editor, search for the following tag: **<scanner-remote-executable-name>**. The following results are displayed:
 - a. The first occurrence is the global parameter.
Note: This value is overwritten by subsequent occurrences.
 - b. The second occurrence is for the Windows platform.
4. For each occurrence, type the file name that you want in the following tag:

```
<executable><File Name></executable>
```

where **<File Name>** is the name of the file that you want to rename for that platform.

Note:

- In **ScannersConfigurationbyPlatform.xml**, the properties in the **<platform name="all">** section will be taken ONLY when the properties are not set in a specific platform section. For example, if there is no **scanner-remote-executable-name** set in the **<platform name="windows" display-name="Windows">** section, the value **scan** will be taken from the **<platform name="all">** section.
- If you rename the scanner executable file, make sure that the configuration in the **<platform name="windows" display-name="Windows">** section is updated accordingly. For example, if you want to rename the scanner executable file from **scan.exe** to **udscan.exe**, the **scanner-remote-executable-name** in the **<platform name="windows" display-name="Windows">** section should be changed from **scan.exe** to **udscan.exe**.
- If the scanner executable file is only renamed in the **<platform name="all">** section but is not renamed in the **<platform name="windows" display-name="Windows">** section, the **Inventory Discovery by Scanner** job will upgrade the scanner on the remote machine even though the **IsScannerUpgradeAllowed** option is set to **false**.

How to Integrate BDNA Normalize with Universal Discovery

This task describes how to integrate BDNA Normalize. After BDNA is installed, and after the configurations are performed on the Data Flow Probe, the normalized installed software data produced by the scanner-based inventory is normalized using the BDNA Technopedia catalog instead of the Universal Discovery application library (SAI). To enable this integration, perform the following:

1. Configure the Data Flow Probe
 - a. Edit the **dataflowprobe.properties** file. To do this, go to **<DataFlowProbeInstallDir>\conf** directory.

where **<DataFlowProbeInstallDir>** is the directory where Data Flow Probe is installed.


- Find the following string and change the value to **true**:
com.hp.ucmdb.discovery.probe.agents.probemgr.xmlenricher.external.application.recognition=false (default = false).
- (Optional if you want to enable Debug) Find the following string and change the value to **true**:
com.hp.ucmdb.discovery.probe.agents.probemgr.xmlenricher.external.application.recognition.debug=false (default = false).

Note: For more information on Debug mode, see "[BDNA Normalize Integration](#)" on [page 536](#).

2. Install BDNA Normalize

Install BDNA according to the vendor instructions.

3. Configure BDNA

- a. Double-click the Normalize shortcut that should be created by BDNA Normalize on the Windows desktop.
- b. In the **Data Source** pane, locate **HP XSF** and then click . The **Normalize Settings** dialog box opens.

Note: If the HP XSF process has not been created, click on New Process and select "HP Universal Discovery (XSF)" as the datasource.

- c. Click the **Data Source** tab.
- d. Review the settings in the Input Folder - it should point to the **<DataFlowProbeInstallDir>\runtime\xmlenricher\Scans\ProcessedNew** directory.
- e. In Actions section, the XSF Out field should point to the **<DataFlowProbeInstallDir>\runtime\xmlenricher\Scans\ProcessedCore** directory.

4. Results

Data enriched by BDNA can be pushed using integration adapters to other systems.

Tip: Use the newly-created **RecognizedBy (recognized_by)** attribute for the Installed Software CI to locate and leverage BDNA-created data. If the value of this attribute is

"BDNA" - then installed software is normalized using the BDNA Technopedia catalog. If value is "SAI", the installed software CI is normalized using the Universal Discovery application library (SAI). Attribute values can be seen by using the **CI Types** pane.

For more information on CI Types and attributes, see "CI Type Manager Page" in the *Universal CMDB Modeling Guide*.

How to Discover Client IP Ranges Without SNMP

This task describes how to discover client type IP ranges without using SNMP.

1. Enable the option
 - a. Go to **Data Flow Probe > Adapter Management > Resources** pane. Click **Packages, AutoDiscoveryContent, Configuration Files**, and **globalsettings.xml**. The file opens in a text editor.
 - b. Locate the following line and change the value to true: **<property name="pingClientType">>false</property>**.
2. Configure the Infrastructure Activity
 - a. In **Infrastructure Activity > Preferences** page, select **Ping Sweep within the ranges of Management Zone**. For more information about this activity, see *Universal CMDB Discovery and Integrations Content Guide*.
 - b. Ensure that the following options are NOT selected: **IP/MAC Harvesting** and **Discover Network Devices in Client IP Ranges**.

How to Discover Windows Device Drivers using the Inventory Discovery by Scanner Job

The **Inventory Discovery by Scanner** job can report Windows device drivers. However, this feature is disabled by default. The discovery of the Windows device drivers needs to be enabled in the scanner configuration. To do so,

1. Open the **Scanner Configuration Generator** wizard. For more information about this wizard, see ["Scanner Generator Wizard" on page 605](#).
2. Navigate to the **Scanner Options** tab > **Troubleshooting** tab by clicking the **Next** button of the wizard.
3. Type `-incl:904` in the **Additional command line parameters to supply to the scanners** field.
4. Click **Next**.
5. Click **Finish**.

Note: The discovery of Windows device drivers using the **Inventory Discovery by Scanner** job requires UCMDB 10.22 CUP1 or later.

Scanner Command Line Parameters Overview

Scanner settings are typically configured when creating a scanner using the Scanner Generator. However, you may want to override these configured settings when manually running the scanner. Examples of when to override scanner configuration file settings are as follows:

- The scanner encounters a problem when trying to capture information during a scan.
- Assume the scanner is configured to save the scan file to a remote location. For example, a Data Flow Probe server or a Store and Forward server. In this scenario, you want to re-route the scan file to another location.
- Assume the scanner is configured to save the scan file to a remote location. However, a segment of the network is down. In this scenario, you want to re-route the scan file to another location.
- You want to optimize the scan performance for certain machines, or you want to optimize the scan performance at certain times.

Tip: Command line parameters and parameter values that are used to run the scanner can be viewed in Analysis Workbench, or they can be viewed in Viewer at **Hardware and Configuration** tab > **System Data** folder. This is useful when you want to check if the scan results were obtained from a scanner that was run with any special command line options. For more information about these Inventory Tools, see ["Inventory Tools" on page 534](#).

How to Use Command Line Parameters

You can specify command line parameters by:

- Typing the command from a command line (for example, the Windows command prompt, or the UNIX/Mac OS X shell). In UNIX/Mac OS X make sure you specify the path to the scanner.

For example:

```
/tmp/scanlinux-x86 -?
```

launches the Linux scanner from the /tmp directory and displays a list of valid command line options.

- Creating a Windows shortcut. Type the command line options (if any) after the quotation marks.

For example:

```
"C:\TEMP\Scanwin32-x86.exe" -?
```

launches the Win32 scanner and displays a list of valid command line options.

- Typing the command in the Windows Run command in the Start menu. Type in or navigate to the location where the scanner executable is located. Type the command line parameter or switch after the quotation marks.

For example:

```
"C:\TEMP\Scanwin32-x86.exe" -?
```

Scanner Command Line Parameters

Parameters that can be used to control the operation of the scanner and used to control which information is captured are as follows. These parameters are typically used in a command line interface to override parameter values that are contained in the scanner configuration file.

Note: Most of these parameter corresponds to an option in the Scanner Generator wizard. For more information, see "[Scanner Generator Wizard](#)" on page 605.

Command Line Parameters for Scanners

Parameter	Description
-?	The full list of command line options can be obtained by running the scanners with the -? or /? command line option.
-force	Do not check disk space when saving the scan file off-site. This may be useful when the operating system reports insufficient space, but this is actually due to access rights.
-incl:<switch>	<p>Enables (or includes) certain types of information collected in a scan. For a list of options, see "Scanner Information Type Parameters" on page 593.</p> <p>To include BIOS data and video data, include the following statement:</p> <pre>-incl:10 -incl:30</pre>
-excl:< switch >	<p>Disables (or excludes) certain types of information collect in a scan. For a list of options, see "Scanner Information Type Parameters" on page 593.</p> <p>To exclude BIOS data and video data, include the following statement:</p> <pre>-excl:10 -excl:30</pre>

Parameter	Description
<code>-scandays:<Count></code>	<p>Scan only if previous scan was more than Count days ago. Forces the scanner to perform the scan only if the previous scan was <Count> or more days ago.</p> <div data-bbox="581 426 1369 537" style="background-color: #f0f0f0; padding: 5px;"><p>For example: <code>-scandays:7</code></p></div> <p>For example, if the scanner is launched from a login script every day, it will only perform the scan every week.</p> <p>When the <code>scandays:<Count></code> parameter is specified, the scanner attempts to check when the last scan was run. If no previous scan file is found, no messages are displayed and the scan runs. If a scan file is found, the following message is added to the log file:</p> <pre>"Checking the age of Scan File "%s"</pre> <p>Where %s is the full name of the scan file it checks. If there is a problem determining the age of the scan file (for example, if it is a newer version or it is corrupt), it then outputs:</p> <pre>The age of the Scan File cannot be determined.</pre> <p>If it does manage to obtain the date, it outputs:</p> <pre>Last scan was %d days ago</pre> <p>Where %d is an integer number.</p>

Parameter	Description
<p>- scandayofweek:<Number></p>	<p>Scan only on specified day of week (0-Sun, 1-Mon, etc.). <Number> can be one of the following:</p> <ul style="list-style-type: none">0-Sunday1-Monday2-Tuesday3-Wednesday4-Thursday5-Friday6-Saturday <p>For example:</p> <pre>-scandayofweek:5</pre> <p>This will cause the scan to be performed on Fridays only. The scandays: and scandayofweek: options can be combined. For example:</p> <pre>Scanwin32-x86 -scandays:14 -scandayofweek:3</pre> <p>This causes the scan to be performed every other Wednesday.</p>
<p>-r:<path></p>	<p>The default path to the original scan files. A UNC path can also be entered as the argument to this option. The format for a UNC path is:</p> <pre>\\servername\sharename\path\</pre> <p>For example:</p> <pre>Scanwin32-x86 -r:\\Hewlett-Packard\ED\scanfiles\</pre> <p>Note: The user that is running the scanner must have read permissions to the specified UNC path.</p>

Parameter	Description
<code>-p:<path></code>	<p>Default off-site save path. The path can be one of the following types of values, depending on the destination of the scan file:</p> <ul style="list-style-type: none">• Normal file path - The full path name, beginning with the drive letter. For example: <code>-p:c:\Inventory\Scans</code>• UNC path - When running on Windows, a UNC path can be entered as the argument to this option. The format of a UNC path is: <code>\\servername\sharename\path\</code> For example: <code>-p:\\DataFlowProbeServer\Incoming\</code> The user running the scanner must have Write permissions to the specified path.• FTP/S URL - A destination URL of an FTP server. The format of the URL is: <code>ftp://<username>:<password>@<hostname> <port>/dir</code> For example: <code>-p:ftp://scanuser:scanpasswd@DataFlowProbeServer. mycompany.com/nm/scanner/uploadsans</code>• HTTP/s URL - A destination URL of an HTTP server. The format of the URL is: <code>http://<hostname>:<port>/dir</code> For example: <code>-p:http://DataFlowProbeserver.mycompany.com/nm/ scanner/uploadscan</code> The username and password is not supported here. If the username and password is required with HTTP saving, specify it in the Advanced Settings dialog in the Saving tab of the Scanner Generator. For detailed information, see "Save result to network (off-site)" on page 636.

Parameter	Description
	<p>The scanners support URL encoding in usernames, passwords, and directory names. In a URL, you can replace @ with %40, and the scanner translates %40 to @ before it calls the FTP server. For example, if you type scanuser%40mycompany, the scanner will translate that as scanuser@mycompany when it logs in to the FTP server.</p>
-cert	<p>Specifies the path to the certificate file. This path is used with offsite scan saving when performed using the secure SSL-based protocol, such as ftps or https, to specify the certificate file (for self-signed certificates) or the file containing certificate authority files (for ftps/websites running with the regular certificate issued by a certificate authority). To obtain the file containing all recent certificate authorities extracted from the Mozilla browser, see: http://curl.haxx.se/docs/caextract.html</p> <p>If the -cert command line option is not specified, the scanner still tries to save scan files using ftps/https, but without using any certificates.</p>
-paths	<p>Defines exactly which directories to scan; the parameter can be repeated as many times as necessary.</p> <p>For example:</p> <pre>scan -paths:/etc -paths:/var -paths:/bin</pre> <p>scans just /etc, /var and /bin and their subdirectories.</p> <p>Note: You must ensure that the Allow scanner command line to override this selection option is checked in the Scanner Generator Software Data page for this to work.</p>
-cfg	<p>Specifies the scanner configuration file.</p>

Parameter	Description
-log:<level>	<p>Specifies the level of debugging information that will be written to the scanner log when the scanner is running. The log is saved in the scan file and also as a separate file:</p> <ul style="list-style-type: none"> • In most cases, you can view the scanner log by using the Viewer. • If a problem has occurred that prevents the scanner from saving the scan file, you can view the scanner log file from the Diagnostic panel in the Device Manager. <p><level> can be one of the following:</p> <ul style="list-style-type: none"> • off: Detailed logging is turned off. This is the default. • debug: Debug messages are logged in addition to the regular scanner messages. They are more-detailed providing additional information. • trace: All regular, debug, and detailed messages are logged. The detailed messages provide tracing details as to scan runs, returned error codes, and software scanning. This option automatically enables the generation of the error log file.
-scripts	Specifies the path to a directory that contains pre/post scan scripts.
-scriptstimeout	Specifies the timeout (in minutes) for running pre/post scan scripts.
-l:<filename>	The default file name of the local scan file, local\$.xsf. If the path is specified in the file name, then the default path for storing the local scan file is also overridden.
-v	If set to on , the scanner does not make the local scan file read-only or hidden.
-d	<p>Specifies whether delta scanning is enabled or not.</p> <p>If set to on, this enables delta scanning if it is disabled in the scanner generator.</p> <p>If set to off, this disables delta scanning if it is enabled in the scanner generator.</p> <p>If the setting fails to specify on or off, the scanner prints the help message and returns.</p>
-t:<path>	The default path for storing temporary files.

Parameter	Description
-o:<filename>	<p>Takes the off-site scan file name from the command line.</p> <p>For example (non UNIX):</p> <pre>Scanwin32-x86 -o:r:\results\SC002154</pre> <p>Where r:\results\SC002154 is the path to the file SC002154.</p> <p>If a file name is not entered, the file is named Default.xsf. If the path is not specified, the file is placed in the directory configured for off-site scan files in the Scanner Generator. If the path is specified on the command line (even if it is relative), it replaces the path configured in the Scanner Generator.</p> <p>Example 1:</p> <pre>scanlinux-x86 -o:newname</pre> <p>Saves the off-site scan file, newname.xsf, to the location configured in the Scanner Generator.</p> <p>Example 2:</p> <pre>scanlinux-x86 -o:/tmp/newname</pre> <p>Saves the off-site scan file to /tmp/newname.xsf.</p> <p>Example 3:</p> <pre>scanlinux-x86 -o:subdir/newname</pre> <p>Saves the off-site scan file, newname.xsf, to the subdir subdirectory of the current directory.</p>
-home	Specifies the home path for storing aioptionrc files.
-pfiles	<p>Overrides the setting for the pfiles command.</p> <p>If set to on, this enables the use of the pfiles command.</p> <p>If set to off, this disables the use of the pfiles command.</p>

Scanner Information Type Parameters

The following parameter values can be used for enabling or disabling certain hardware and software scans when manually running the scanner.

These parameter values are used together with the **-excl** and **-incl** parameters. For more information, see ["Scanner Command Line Parameters Overview" on page 585](#).

Information Type	Parameter Value
BIOS data	10
BIOS extension	11
SMBIOS Information	12
Compaq Asset Tag	13
Plug and Play Version	14
Video data	30
Monitors	31
Port data	40
Keyboard and mouse data	50
Disk data	60
Local USB hard drives	62
Memory data	70
Swap files	72
CPU data	80
Operating system data	90
Device driver files	91
Cluster data:	92
Services	93
Virtual machine data	94
User profiles	95
OS registered applications	96
Containers	97
WMI software features	98
Packaged file data	99
Storage data	100
Devices	101

Information Type	Parameter Value
SCSI/IDE serial numbers	102
Network data	110
TCP/IP data	111
IPX data	112
Netbios data	113
Network shares	114
Bus data	120
PCI cards	121
PCMCIA cards	122
MCA cards	123
EISA cards	124
ISA PnP card detection	125
USB data	126
Peripherals	130
System configuration	150
Software identification tags	901
Running Process Detection	902
TCP/IP Connectivity Detection	903

Scanner File Locations

When you use activities to automate discovery, the Scanner is copied to the discovery node according to the default value in the Inventory Discovery by Scanner job adapter.

The default file location of the Scanner is as follows:

Platform	File Location Path
Windows	%SystemRoot%
	Note: %SystemRoot% is normally located at C:\Windows.

Platform	File Location Path
Solaris Sparc	\$HOME/.discagnt Note: \$HOME is normally "/", so the directory is "/.discagnt/".
Mac OS	~/.discagnt/
Linux	Note: The "~" symbol normally is "/var/root", so the directory is "/var/root/.discagnt/".
HP-UX	
AIX	

Web Server Configuration for Saving Scan Files via HTTP

Apache and IIS Web Servers

The Web Server needs to be configured to allow execution of the PUT command. Usually, by default web servers are set to enable POST and GET commands. You will need to ensure that if you are using HTTP saving that the PUT command is enabled in the directory.

The following is a quick description of what you would have to enable for HTTP saving on both Apache and IIS:

Apache 1.3	<p>If you are using basic authentication, do the following:</p> <ol style="list-style-type: none"> In the bin directory run: <pre>htpasswd -c "<path>\htpass" Username</pre> Enter the following in the htaccess file of the directory that you intend to save in: <pre>PUT_EnablePut On PUT_EnableDelete Off AuthType Basic AuthName "Write" AuthUserFile "<path>\htpass" Require user Username</pre> Download the mod_put.so file and put it into the modules directory. Enter the following into the httpd.conf file:
-------------------	--


	<pre>LoadModule put_module modules/mod_put.so</pre>
Apache 2.x	<ul style="list-style-type: none">• As mod_put is Apache 1.3 specific and is no longer available in Apache 2.x, mod_dav should be used instead to provide the HTTP PUT capabilities• Make sure that mod_dav is loaded. For example, the following line in the Apache web server configuration can be used to enable it: <pre>LoadModule dav_module modules/mod_dav.so</pre>• Then for a particular location you can enable mod_dav with the following setting: DAV On <p>Refer to the documentation for Apache's mod_dav module for more details.</p>
IIS	<p>Check the option that allows writing to the desired save directory. Ensure that you have given write access to the username and password that you plan on adding to the scanner's http save path.</p>

XML Enricher Directory Structure

The XML Enricher uses a directory structure on the Data Flow Probe computer under the probe's installation directory. By default, the root of this directory structure is:

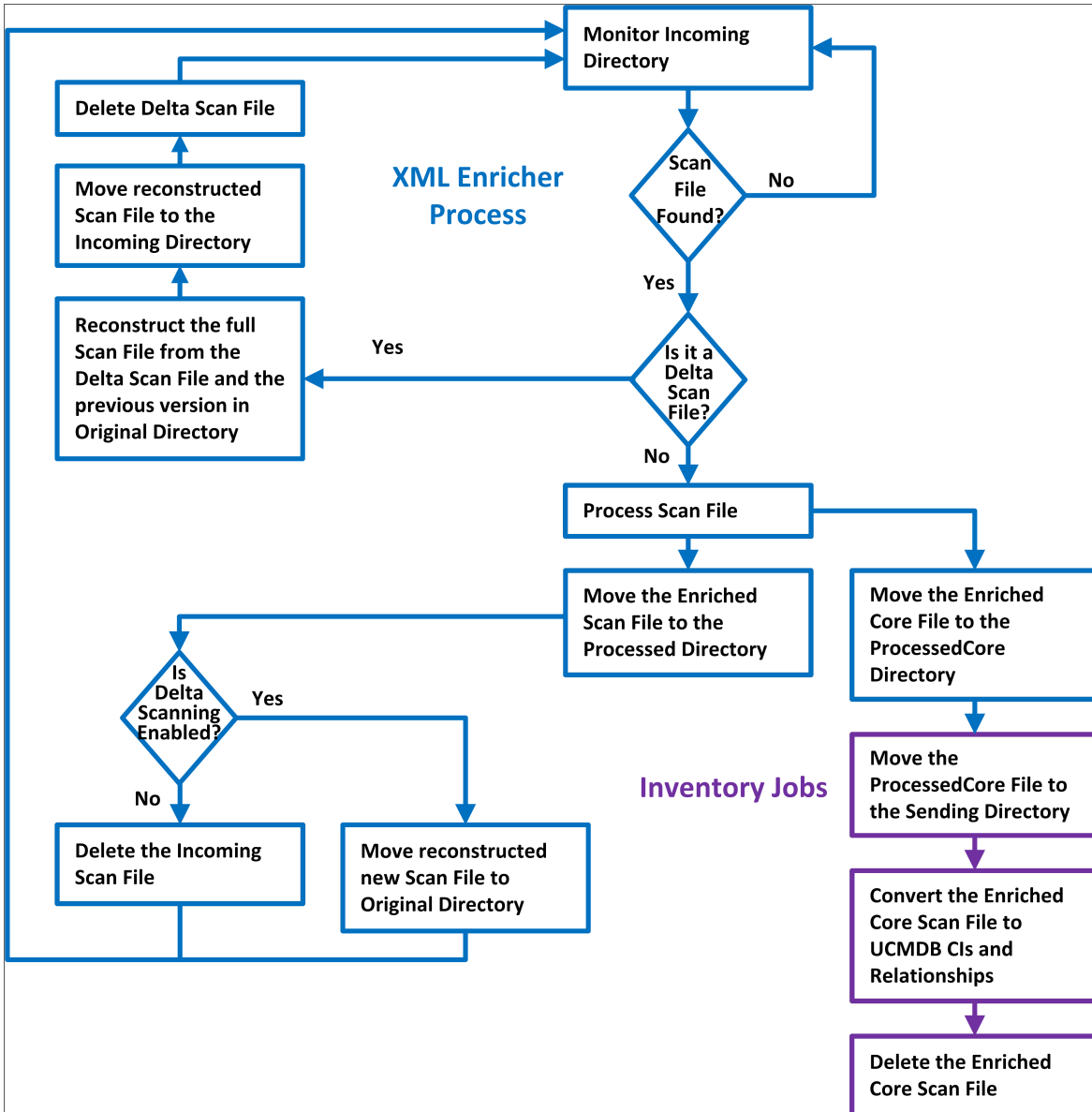
C:\hp\UCMDB\DataFlowProbe\runtime\xmlenricher

The following table shows various directories that are used by the XML Enricher.

Directory	Explanation
Scans	The base directory.
Scans\Failed	The base failure directory. Failed scans are moved to a subdirectory of this one.
Scans\Failed\Corrupt	Scans that cannot be read or may not be scan files are moved here.
Scans\Failed\Delta	If the original scan file is missing or there is an error applying the delta scan file to the original one, then those delta scan files will be moved here.
Scans\Failed\Error	When any other error occurs, scan files are moved here.
Scans\Incoming	The incoming directory. The Enricher looks for new scan files here.
Scans\Logs	Stores the log files. Manual deployment Scanners may save the log into the off-site location.
Scans\Original	This folder is used for delta scanning. It stores copies of original scan files, which are then used in conjunction with delta scan files to recreate the new version of the scan file.
Scans\Processed	The processed directory. Enriched scan files are created here.
Scans\Processed\ [user defined]	You can group the scan files based on Hardware fields. This is user-defined. Define the setting as follows: <ul style="list-style-type: none">• Go to Inventory Discovery by Scanner job > Properties > Global Configuration Files• Select EnricherServiceSettings.ini• Click the  button The XML Enricher Configuration dialog is displayed <ul style="list-style-type: none">• On the General tab, use the Scan File Management part See " Scan File Management " on page 651.

Directory	Explanation
Scans\ProcessedCore	Stores the processed core files.
Scans\Sending	The Inventory Discovery job moves the new processed core files here for further processing.
Scans\Temp	This is where the XML Enricher stores its temporary files.

The following flowchart shows how the enrichment process works for XSF and delta (DSF) scan files.



Enriched XSF File Structure

Scanfile.dtd describes the structure of the scan file in standard DTD format.

Note: The file is a text file, but is easiest to read with an XML reader.

An XSF scan file contains a sequence of elements, each of which have various attributes. Root elements are:

- **<hardwaredata>**
- **<applicationdata>**
- **<users>**
- **<applicationusage>**
- **<filedata>**
- **<storedfiles>**
- **<configurationdata>**

Inventory Discovery User Interface


This section includes:

Hardware Mapping Configuration Dialog Box	600
Scanner Generator Wizard	605
XML Enricher: Software Recognition Configuration Dialog Box	650




Hardware Mapping Configuration Dialog Box

Enables you to map scan file hardware attributes to UCMDB CIs.

To access	Use one of the following: <ul style="list-style-type: none">• Select Adapter Management > Resources pane > Inventory Discovery > Adapters > Inventory Discovery by Scanner. Click the Adapter Definition
------------------	---

	<p>tab, expand the Global Configuration Files pane, click HardwareMappingConfig, and click .</p> <ul style="list-style-type: none"> From the Inventory Discovery activity, go to the Preferences page and click the Custom Mapping button. <p>Note: This option is available only when Scanner Based Inventory Discovery is selected on the Preferences Page.</p>
Important information	Before creating a mapping, perform an analysis on what information you want to map, what data element in the scan file contains the information you want to capture, where the data element in the scan file is located, and which UCMDDB CI you want to store this information.
Relevant tasks	"How to Map Scan File Attributes to UCMDDB" on page 572
See also	Configuration Items (CIs) in the <i>Universal CMDB Administration Guide</i> .

User interface elements are described below:



UI Element	Description
	<p>Select CI. Opens the Select CI dialog box, enabling you to create a new mapping between a scan file attribute and UCMDDB CI properties.</p> <p>When the Select CI dialog box opens, select a CI that you want to create a mapping.</p> <p>Available when: Hardware Mapping Configuration is selected in the left pane.</p>
	<p>Select an Attribute. Opens the Select an Attribute dialog box, enabling you to add a mapping between a scan file attribute and a selected UCMDDB CI.</p> <ul style="list-style-type: none"> Attribute. Select an attribute from the drop down list to map to scan file attributes. Display Label. The name of the attribute Type. The data type of the attribute as it appears in the CI Type Manager. For more information, see the section describing the CI Type Manager in the <i>Universal CMDB Modeling Guide</i>.
	Enables you to delete the selected UCMDDB CI or attribute.

CI Editor

Enables you to define attributes of the UCMDDB CI that you want to map to scan file attributes.

Important information	This page is displayed when a CI is selected in the left pane.
------------------------------	--

User interface elements are described below:



UI Element	Description
CI Name	The display name of the CI that is selected in the left pane.
Relationship	<p>Click the ellipsis  to open the Select Relationship with Node CI dialog box, enabling you to select the relationship that you want for the mapping.</p> <p>If you want to remove the value in this field, click .</p> <p>Note:</p> <ul style="list-style-type: none"> • This is an optional field. • If there are no options available in the drop down list, there are no relationships that are created in UCMDB for the selected CI. • Selected values are ignored if they conflict with system values.
Kind	<p>The number of instances of the CI to map.</p> <ul style="list-style-type: none"> • Single. Only one instance of the selected CI is created in UCMDB. • Multiple. Multiple instances of the selected CI are created in UCMDB. <p>Select this option if there are multiple instances of a particular type of data (shell tag/field) that you want to map. For example, you want to map the hwCPU field. However, you notice that there are multiple instances of this field contained in the scan file. If single is selected, only the first instance of hwCPU is mapped. If you want to map more than the first instance of this data (i.e, the child data elements contained in the shell/parent element), select the multiple option. For example, if there are three instances of hwCPU in the scan file and you select multiple, three instances of the CI are created in UCMDB.</p>
Create New CI	<p>Enables you to create a CI instance for the selected CI.</p> <ul style="list-style-type: none"> • Yes. Create a new CI instance to map scan file information to a CI type when the CI type is not contained in the ParseEnrichedScanFile.py script. • No. Ignores mapping of the selected CI when the CI type is not contained in the ParseEnrichedScanFile.py script. <p>Default: No</p>
Parent Shell	<p>Opens the Select a Shell Tag dialog box, enabling you to select a structural part of the scan file where the information that you want to map is located. Select a value for this field if you want to define the value type for the mapped attribute as array. Otherwise, this is an optional field.</p>

Attribute Editor

Enables you to define properties of scan file attributes that you want mapped to UCMDB CIs.

Important information	This page is displayed when an attribute is selected in the left pane.
------------------------------	--

User interface elements are described below:

UI Element	Description
Attribute Name	<p>Displays the name of the attribute that is selected in the left pane. Click  to open the Select an Attribute dialog box to edit properties of the attribute.</p> <p>Note: If you change the attribute name, the previous attribute values are overwritten.</p>
Value Type	<p>The data type of the attributes in your scan file.</p> <ul style="list-style-type: none"> • Scalar. Non-composite value, such as boolean, numeric, or character data types. • Array. Collection of values or variables that are selected by one or more indices. <p>Note: This option is only available when there is a value for the Parent Shell field in the "CI Editor" on page 601.</p> <ul style="list-style-type: none"> • Pre/Post. Use mappings that are contained in scripts that can map scan file values to UCMDB CIs. • Script. Customize data parsing by using aJython script.
Value	<p>Values that are displayed correspond to the option that is selected in the Value Type field.</p> <ul style="list-style-type: none"> • Scalar. Click the ellipsis  to open the Select a Scalar Tag dialog box and then select a structural part of the scan file where your mapped information is located. • Array. Click the ellipsis to open the Select an Array Tag dialog box and then select a tag type that corresponds to the attribute tags in your scan file. <p>Note: If this option is selected, the only options that are displayed are tags for the value set for the Parent Shell field in "CI Editor" on page 601.</p> <ul style="list-style-type: none"> • Pre/Post. The Scanner reads the output of the pre- and post-scan scripts and captures all lines with the following structure: <attributename>=<value> The length of the <attribute> tag can be up to 256 characters, and the length of the <value> tag can be up to 1024 characters.

UI Element	Description
	<p>Note: The Scanner captures any script output line that contains an equal sign (=), except if the equal sign is the first character on the line.</p> <ul style="list-style-type: none">• Script. Enter your Jython script code. For more information, see Create Jython Code in the <i>Universal CMDB Developer Reference Guide</i>. <p>Note: The script must return a value.</p>
Overwrite	<p>Select an option to overwrite values that were generated by the ParseEnrichedScanFile.py script when the last Inventory Discovery job ran.</p> <ul style="list-style-type: none">• Yes. The values generated from this mapping overwrite previous values.• No. The values generated from this mapping do not overwrite previous values. <p>Default: No</p>

Scanner Generator Wizard

Enables you to configure and generate scanners to collect information.

To access	<p>Use one of the following:</p> <p>To create a new scanner configuration, or edit an existing scanner configuration (Enterprise Mode):</p> <ol style="list-style-type: none"> 1. In the relevant Management Zone, go to the Inventory Discovery activity > Preferences page. 2. Under Scanner-based Inventory Discovery, expand the Scanner Configuration pane, and click New/Edit Scanner Configuration. <p>To create/edit a manually deployed scanner (for Manual Deployment mode):</p> <ol style="list-style-type: none"> 1. Select Data Flow Management > Adapter Management > Resources > Inventory Discovery > Scanner Configuration Files. 2. Select the configuration file (.cxz) in the tree on the left, and click the Generate Scanners... button in the right pane.
Important information	<p>For details about the Enterprise and Manual Deployment scanner modes, see "Inventory Discovery Scanners" on page 509.</p>
Wizard map	<p>The Scanner Generator Wizard contains:</p> <p>"Scenario Page" > "Standard Configuration Page" > "Collection Page" > "Hardware Data Page" > "Software Data Page" > "Software Details Page" > "Asset Data Page" > "Scanner Options Page" > "Scanners to Generate Page" > "Generating Scanners Page"</p>

Scenario Page

This page enables you to select a mode for generating the scanner.

Important information	<p>General information about the wizard is available in "Scanner Generator Wizard".</p>
Wizard map	<p>The "Scanner Generator Wizard" contains:</p> <p>Scenario Page > "Standard Configuration Page" > "Collection Page" > "Hardware Data Page" > "Software Data Page" > "Software Details Page" > "Asset Data Page" > "Scanner Options Page" > "Scanners to Generate Page" > "Generating Scanners Page"</p>

User interface elements are described below:

UI Element	Description
Enterprise Mode	Automatically collect an inventory using the scheduling and launching capabilities of UCMDB. In this mode, several options are pre-configured to facilitate seamless scanner integration. Some of these options are not editable.
Manual Deployment Mode	Inventory scans are launched from login scripts or non-networked machines, and not automatically UCMDB.

Standard Configuration Page

This page enables you to select a default scanner setup or to select a previously stored setup.

Important information	General information about the wizard is available in "Scanner Generator Wizard" .
Wizard map	The "Scanner Generator Wizard" contains: "Scenario Page" > Standard Configuration Page > "Collection Page" > "Hardware Data Page" > "Software Data Page" > "Software Details Page" > "Asset Data Page" > "Scanner Options Page" > "Scanners to Generate Page" > "Generating Scanners Page"

User interface elements are described below:

UI Element	Description
Default Settings	<ul style="list-style-type: none">• Inventory Scan. Uses default configuration setting for the scanner. Defines a set of options suitable for a general inventory. Enough software information is collected to allow comprehensive inventory analysis. All hardware information is collected and a standard series of asset data fields are defined.• Shallow Scan. Defines a set of options to allow very quick scans. Because hardware scanning is very fast, most hardware items (some are disabled by default) are collected, but limited software scanning takes place, and the data collected is not sufficient to perform reliable software license recognition.• Detailed Scan. If scanning time is not a critical factor, this option can be used to collect the maximum amount of information. This, however, extends the scanning time significantly. Note: Use this option in special cases only.• Enable scanning of Java class file. If you select Inventory Scan or Detailed Scan (see above), you can enable Java scanning. Enabling this option does the following:<ul style="list-style-type: none">◦ Java .class files are stored in the scan file.◦ Java specific environment variables for targeted scanning is enabled.◦ Windows scanner adds the location of the Java Home directory to the list of directories for a targeted scan.

UI Element	Description
Stored Settings	<ul style="list-style-type: none">• Read From Server. Reads the settings from a previous Enterprise Mode configuration stored on the server. The drop down combo box lists previously configured scanner configurations. The names displayed with angle brackets around them (for example, <default>) are predefined configurations. It is possible to read predefined configuration settings, but it is not possible to overwrite them when generating the new configuration. If you choose a predefined configuration, you must rename it when you come to the last page of the Scanner Generator wizard in order to save it to the server. If you save this configuration, it will be available from the server with the other previous configurations.• Read From File. Replaces various configuration settings by reading information from files on the local machine. It can read parameters from previously generated scanners, scanner configuration files (.cxz), and scan files (.xsf). When the file name is provided, the Scanner Generator determines the type of the file based on the file extension, which eliminates the need to have a separate entry for each.

Collection Page

This page enables you to select the type of computer data to collect.

Important information	<ul style="list-style-type: none"> The selections you make on this page determine which of the data detail pages are displayed. When carrying out initial scanner deployments you might want to use hardware and asset data collection to establish basic information for the target machine. This can be followed up later by a more comprehensive scan that includes software data. General information about this wizard is available in "Scanner Generator Wizard".
Wizard map	<p>The "Scanner Generator Wizard" contains:</p> <p>"Scenario Page" > "Standard Configuration Page" > Collection Page > "Hardware Data Page" > "Software Data Page" > "Software Details Page" > "Asset Data Page" > "Scanner Options Page" > "Scanners to Generate Page" > "Generating Scanners Page"</p>

User interface elements are described below:

UI Element	Description
Hardware and Configuration	<p>If selected, the scan collects hardware and configuration data, including details of the processor, memory configuration, computer bus, attached cards, hard disks, attached drives, monitor, video adapter, keyboard, mouse, OS version, network protocols and addresses. See "Hardware Data Page".</p> <p>Note: In Enterprise mode, this option is always selected and cannot be disabled.</p>
Software Data	<p>If selected, the scan collects detailed information about files and directories on all scanned drives. The information collected about files can be defined (including the file types inventoried and the level of information collected). It is possible to define which drives are to be scanned based on the media of the drive, as well as determine which files are included in the scan file and which are ignored. See "Software Data Page".</p>
Asset Data	<p>If selected, the scan collects Asset data which consists of asset fields that can be collected automatically. See "Asset Data Page".</p>

Hardware Data Page

This page enables you select the hardware categories to be collected by the scanner.

Important information	<ul style="list-style-type: none"> By default, most hardware options are selected. Disable specific hardware detection routines if there is a known problem scanning these hardware items. You disable the hardware detection routines for a specific category by clearing the check box next to the item. All other hardware detection will take place as usual. The hardware options have equivalent command line options that can be used at run-time. For information about scanner command line options, see "Scanner Command Line Parameters Overview". General information about the wizard is available in "Scanner Generator Wizard".
Wizard map	<p>The "Scanner Generator Wizard" contains:</p> <p>"Scenario Page" > "Standard Configuration Page" > "Collection Page" > Hardware Data Page > "Software Data Page" > "Software Details Page" > "Asset Data Page" > "Scanner Options Page" > "Scanners to Generate Page" > "Generating Scanners Page"</p>

Hardware data items are described below:

Category	Description
BIOS information	<p>Collects information about the computer BIOS, including the computers asset tag, the BIOS date, ID, manufacturer and revision (where applicable).</p> <ul style="list-style-type: none"> BIOS extensions. Detects installed BIOS extensions, such as video or SCSI BIOS. SMBIOS. Collects hardware data from System Management BIOS. Plug'n'Play. Provides details of whether the BIOS installed on the computer is Plug and Play compatible. If the BIOS supports Plug and Play specification, the version of the specification is collected. <p>Note: Select these options if you want to collect data for software license compliancy. For more information, see "How to Calculate License Compliancy for IBM" on page 705.</p>
CPU Identification	<p>Identifies the CPU (model), establishes if it has got FPU (numeric coprocessor), MMX (MultiMedia eXtensions) and ISSE/SSIMD capability and reports the speed of the CPU, cache characteristics.</p> <p>For newer Intel and compatible processors, the manufacturer, model, family and stepping ID are reported.</p> <p>Select this check box if you want to collect data for software license compliancy. For more information, see "How to Calculate License Compliancy for IBM" on page 705.</p>

Category	Description
Memory	<p>Detects the total amount of memory installed on the computer, including the amount of conventional and extended memory.</p> <ul style="list-style-type: none"> • Swap File data. Collects data about swap files used for virtual memory.
Operating System	<p>Collects information about the operating system and its configuration.</p> <ul style="list-style-type: none"> • Device Driver Data. When this option is enabled, the Windows scanner enumerates all devices to determine which files are used as device drivers. Each file in this list is given the 'Device Driver' attribute when stored in the scan file. The device driver option is now disabled by default to increase speed of the hardware scanning. • Cluster Data. Collects information about Windows Server Cluster membership. It detects that the machine is part of a cluster, the name and description of the cluster and the list of nodes connected to the cluster. • Services. Collects information about installed operating system services. • Virtual Machines. Detects whether the scanner is running in VMware, Virtual PC, Terminal Services, Hyper-V, LPAR, vPar, or nPartition. From an asset management point of view, it is important to be able to determine which scanned machines are virtual (for example, so you do not pay too much maintenance for too many machines). • Profiles. Collects data about user profiles. • OS Registered Applications. Collects data about installed applications that are registered with the operating system. On Windows (pre-Vista), it collects data as displayed by the Add/Remove programs item in the Control Panel. On Windows (Vista and later), it collects data as displayed by the Programs and Features item in the Control Panel. On UNIX, it collects data from the system's software package manager. • Packaged File Data. Collects information about the relationship between the installed applications (packages) and the files that belong to them. When this option is set, it causes the scanner to interrogate the native operating system package manager to retrieve the relationship information. This ensures that the installed package rule-based recognition can correctly recognize the files as belonging to the installed package/application.

Category	Description
	<ul style="list-style-type: none"> • WMI Software Features. Collects the information about installed applications from WMI as stored in the Win32_SoftwareFeature class. The Win32_SoftwareFeature WMI class is not available on the Windows 2003 Server by default. The WMI provider that supports this class is an optional component on Windows 2003 Server, and it is not installed by default. To enable this WMI provider, you must go to Control Panel > Add Remote Programs > Add/Remove Windows Components > Management and Monitoring Tools > WMI Windows Installer Provider and install the WMI Windows Installer Provider component. Once this component is installed, the data collected by WMI Software Features hardware detection becomes available. • Containers. Collects data about containers available in the operating system. Currently, this is supported for Solaris zones, HP-UX nPartition/vPar, and AIX LPAR. • Software Identification Tags. Collects the information in software identification tag files, which are XML files that consist of identification and management information about a software product. These tag files uniquely identify the software product, providing data for software inventory and asset management. During the hardware detection phase, the Scanner collects the information from software tag files from the common system location, as well as from the top level directory of the application, in the event that software scanning of the installation locations is done. If you do not select the Software Identification Tags check box, the Scanner will not collect any information from tag files during the hardware detection phase. For detailed information, see "Software Identification Tags". • Running Processes. Collects information about running processes. <ul style="list-style-type: none"> ◦ TCP/IP Connectivity. Collects information about open TCP/IP connections for running processes. <p style="margin-left: 20px;">Note: The Running Processes option must be enabled to select this option.</p>
Video	<p>Records details of the Video Display Adapter, which include the adapter type (EGA, XGA, VGA and so on) and model/manufacture, where possible.</p> <p>In Windows the current desktop resolution and number of colors are also picked up.</p> <ul style="list-style-type: none"> • DDC Data. When connected to a VESA DDC compliant monitor, collects full monitor information.
I/O Ports	<p>Detects and reports on the number of serial and parallel ports, the I/O address for each, and for serial ports, the UARTs attached.</p>

Category	Description
SCSI / ASPI Detection	<p>Checks for the presence of an ASPI (Advanced SCSI Programming Interface) driver for a SCSI adapter. If the driver is available, the host SCSI adapter name is reported.</p> <ul style="list-style-type: none"> • SCSI/IDE/ATAPI devices. Detects installed devices, such as hard drives, CD-ROMs, tape drives and other such devices. Also detects Serial ATA disks. • SCSI/IDE/ATAPI serial numbers. Detects serial numbers of the installed devices (where available). Also detects the serial number of Serial ATA disks.
Network Information	<p>Detects the network configuration, including Logon Name, Workgroup Name, Machine ID, and Domain Name.</p> <p>Detects information such as multiple network adapters, gateways, DNS servers, subnet masks, DHCP status.</p> <p>Information about installed network protocols (TCP/IP, NetBIOS/NetBEUI, IPX/SPX) and network addresses is also provided.</p> <ul style="list-style-type: none"> • TCP/IP. Collects information about an installed TCP/IP protocol. This information includes domain, DNS Servers, Node type, NetBIOS Scope ID, WINS proxy status, NetBIOS resolution status. <p>Network adapter information (including description, IP address, IP routing status, subnet mask, default gateways, DHCP status, DNS suffix, autoconfiguration status) is also provided.</p> <ul style="list-style-type: none"> • IPX/SPX. Collects information about the IPX/SPX protocol. • NetBIOS/NetBeui. Collects information about the NetBIOS or NetBEUI protocol. • Shared Devices. Collects information about shared devices, such as disks and printers. <p>Note: In Enterprise Mode, you can disable subsets of network information. However, you should not disable ALL network information.</p>
Keyboard and Mouse	<p>Reports on the type of keyboard attached (extended or normal); whether a mouse is connected and mouse driver is loaded; the mouse brand and version of the driver, number of buttons and type of connection (serial, PS/2, bus).</p>

Category	Description
Disk Drives	<p>Collects advanced information about all attached disk drives. This information includes the type of the drive (floppy disk, hard disk, CD-ROM, network), the type of the file system (FAT, NTFS, HPFS), amount of total and free space, location of the hard drive partitions on the physical hard disk, and so on.</p> <ul style="list-style-type: none"> • Local USB Hard Drives Controls the way USB hard drives are treated. If selected (default setting), the USB hard drives are treated as local hard drives, and their size is counted towards the total and free space on the local hard drives, which is recorded in the hwDiskTotalFreeMB and hwDiskTotalSizeMB hardware fields. If the option is not selected, the USB hard drives are treated as removable drives, and their size are not counted towards the total size. Also, by default, the USB hard drives are not scanned during a “classic” local hard drive scan. However, you can enable scanning by selecting Software Details > Drives > Removable Drives > Other removable drives. This option is currently only applicable to the Windows scanner.
Bus Detection	<p>Detects the architecture of the bus used in the PC:</p> <ul style="list-style-type: none"> • EISA. Detects and reports details of EISA cards. • MCA. Detects and reports details of MCA cards. • PCI. Detects and reports details of PCI cards. • PCMCIA. Detects and reports details of PCMCIA cards. • ISA PnP Cards. Detects and reports details of ISA Plug and Play cards. • USB Data. Detects and reports details of the USB host adapters, hubs and devices attached to them. <p>Note: If the bus types checked for by the scanner are not available, the tests for checking the cards are not performed.</p>
Peripherals	<p>Checks for installed peripherals, such as printers, modems and sound cards.</p>
UNIX System Configuration	<p>Collects UNIX, Linux, and Mac OS X configuration information.</p>

Software Data Page

This page enables you to select the method for scanning software. The choice of scan method determines how extensive the software scan will be.

Important information	<ul style="list-style-type: none"> • Available: When Software Data is selected on the Collection Page (see wizard map below). • Under most circumstances, the default settings (which are determined by the presets chosen on the Standard Configuration page) are satisfactory for defining the software information collected, but the Scanner Generator allows the default options to be modified to create custom settings. • General information about the wizard is available in "Scanner Generator Wizard" on page 605.
Wizard map	<p>The "Scanner Generator Wizard" contains:</p> <p>"Scenario Page" > "Standard Configuration Page" > "Collection Page" > "Hardware Data Page" > Software Data Page > "Software Details Page" > "Asset Data Page" > "Scanner Options Page" > "Scanners to Generate Page" > "Generating Scanners Page"</p>

User interface elements are described below:

UI Element	Description
Targeted Directory Scan	<p>Enables optimum scanning speed and software license accuracy. Only selected locations are scanned, which are identified by the scanner from various sources, such as Windows shortcuts, Services, file associations, environment variables, and so on.</p> <p>Note: This option is most suitable for Windows/Mac OS X platforms.</p>
Classic Local Drive Scan	<p>Enables a complete scan of all local non-removable drives. This option takes longer to complete and is used when performing a detailed scan.</p>
Combined Scan	<p>Enables both of the previous options: scan all local hard drives as well as directories on the network pointed to by shortcuts, file associations and environment variables, such as PATH.</p>
Allow scanner command line to override this selection	<p>If you select this option, the default drive selection specified can be overridden by specifying a list of drive letters or directories to scan on the command line using the <code>-paths</code> command line option.</p> <p>An example of a command line override is:</p> <pre>Scanwin32-x86 -paths:C:\Windows -paths:D:</pre>

UI Element	Description
	<p>If you clear this option, you cannot change the scan selection by specifying drive letters or paths on the command line.</p> <p>For more information, see "Scanner Command Line Parameters Overview" on page 585.</p>

Software Details Page

This page enables you to select files and directories to scan and store.

Important information	<ul style="list-style-type: none"> • Available: When Software Data is selected on the Collection Page (see wizard map below). • This page displays a set of sub-tabs according to the selections made on the Software Data page. • General information about the wizard is available in "Scanner Generator Wizard" on page 605.
Wizard map	<p>The "Scanner Generator Wizard" contains:</p> <p>"Scenario Page" > "Standard Configuration Page" > "Collection Page" > "Hardware Data Page" > "Software Data Page" > Software Details Page > "Asset Data Page" > "Scanner Options Page" > "Scanners to Generate Page" > "Generating Scanners Page"</p>

This page contains the following tabs:

- "[Drives Tab](#)"
- "[Directories Tab](#)"
- "[File Scanning Tab](#)"
- "[Stored Files Tab](#)"

Drives Tab

Enables you to define which of the drives are to be scanned Options are provided for scanning all drives or just a particular type of drive.

Important information	Available for Classic Local Drive or Combined scans only. For details, see " Software Data Page " on page 615.
------------------------------	--

User interface elements are described below:

UI Element	Description
Local Drives	Hard disk drives visible and mounted by the current operating system. In Windows, normal hard disk drives are assigned drive letters by the operating system and are usually included in the scanning process.

UI Element	Description
Removable Drives	<p>Drives with non fixed media that can be removed or exchanged. Removable drives are normally not included for scanning:</p> <ul style="list-style-type: none"> • CD and DVD Drives. Scans the contents of CD and DVD drives. • Floppy Drives. Scans the contents of floppy drives. • Other Removable Drives. Scans other removable drives (for example, SyQuest drives). Scanning removable media is not usually recommended, because the content of these drives varies depending on the media currently in the drive. <p>Note: For detailed information about scanning automatically mounted drives, see Automount (AutoFS) Drives (below).</p>
Miscellaneous Drives	<p>Drives that are neither local nor removable, and may or may not have local physical media associated with them:</p> <ul style="list-style-type: none"> • Network Drives. Scans the contents of network drives. <p>Note: The network drives can be scanned by multiple computers.</p> <p>See Automount (AutoFS) Drives (below) for detailed information about scanning automatically mounted drives.</p> <ul style="list-style-type: none"> • SUBST Drives. Scans "virtual" drives created using the operating system's substitute command, SUBST, on Windows, or by the loopback file system (lofs) on UNIX. This is not normally desirable as a substituted drive can be scanned using both its true drive letter/path and substituted drive letter/path. <p>Note: Use this option with caution.</p> <ul style="list-style-type: none"> • Automount (AutoFS) Drives. When not selected (default), the scanner does not scan any auto-mounted drives. The scanner does not attempt to mount any indirect automount drives. It may mount a direct automount drive if it comes across its mount point during the software scanning process, but the direct automount drive itself is not scanned. <p>When selected, the automount drives are scanned only if all of the following conditions are met:</p> <ul style="list-style-type: none"> ○ The directory where the drive's mount point is located is, itself, being scanned, for example, it is located on a drive for which the corresponding drive-type check box is selected. ○ The drive-type check box for the real drive type of the automount drive is also selected. For example, an auto-mounted NFS drive is scanned only when the Network Drives check box is also selected.

UI Element	Description
	<ul style="list-style-type: none"> ○ The drive is a direct automount drive or if the drive is an indirect automount drive, it has to be either already mounted or during the scanning process the scanner has to encounter a symbolic link pointing to a location within the indirect automount drive's directory structure. <p>Example:</p> <p>The following example shows how these three conditions are met:</p> <p>A direct automount DVD drive mounted under /usr/local/cd (where /usr/local is located on a local hard drive) is scanned only when both Local Drives and CD and DVD Drives check boxes are selected.</p> <ul style="list-style-type: none"> ● Other Drives. Scans drives created using other devices drives (for example, RAM drives). <p>Note:</p> <ul style="list-style-type: none"> ○ Scanning drives created using device drivers can lead to false reporting of files on a computer. ○ Use this option with caution.

Directories Tab

Enables you to specify which directories to scan.

<p>Important Information</p>	<ul style="list-style-type: none"> ● Available for Targeted or Combined scans only. For details, see "Software Data Page" on page 615. ● For Windows operating systems, you can also scan desktop and Start menu shortcuts. ● By scanning only selected directories rather than complete drives, software scanning is made faster. ● Although you can specify the file systems and directories (known to the Scanner Generator) that you want to include or exclude during scanning, you can override the settings of the file systems and specific directories and files during software scanning by using the content in the override files. For details on how to add content to the override files, see "Scanner Options Page" on page 635.
-------------------------------------	---

User interface elements are described below:


UI Element	Description
Directories from shortcuts (Windows only)	<ul style="list-style-type: none"> • Start Menu. Scans the directories that are pointed to by shortcuts on the Start menu. • Desktop. Scans the directories that are pointed to by shortcuts on the desktop. • Only use shortcuts to files with these extensions. Scans only shortcuts that point to files with one of the specified extensions.
Directories from other sources	<ul style="list-style-type: none"> • Windows Services. Select to include directories containing Windows Services for targeted scanning. As the name implies, this option applies to Windows scanners only. • Java Home. Select if you want the scanners to add the Java Home directory to the list of directories for a targeted scan. This option applies to Windows scanners only. <p>Note: If you checked the Enable scanning of Java class files on the Standard Configuration page, this option is selected by default.</p> <ul style="list-style-type: none"> • Non-Global Zone Root Directories. Select if you want the scanners to add the Solaris non-global (local) zone root directories to the list of directories for a targeted scan. This ensures that all directories used by non-global zones are scanned during the software scanning process. This option applies to Solaris scanners only. • Packaged File Data. Select if you want to make sure that the directories where the files belonging to installed packages are located are added to the list of directories to be scanned. For this option to work, the Packaged File Data option must be enabled on the "Hardware Data Page" on page 609. • File Associations. Select if you want the scanners to add directories containing applications that are associated with various file types (for example NotePad for .txt files) to the list of directories for a targeted scan. This option applies to Windows scanners only. • Software Utilization. This setting instructs the scanner to include any directories from where used programs are executed. These directories will be included in the list of directories for a targeted scan. This ensures that the scanner collects the file data required for recognition of used applications. This option applies to all scanners. • Program Files/Applications. Select if you want the scanners to add the standard location for program files to the list of directories for a targeted scan. On Windows, it is the Program Files directory, which is normally located in the root of the Windows system drive (such as C:\Program Files). On Mac OS X, it is the /Applications directory where the applications are installed by default.
Directories from environment	<ul style="list-style-type: none"> • Include directories from these environment variables. If selected, the paths included in the environment variables specified here are also be added to the list to scan. If you specify multiple environment variables, you must

UI Element	Description
group	separate each name with a semicolon (;).
Shortcuts to excluded drives. (Combined scans only)	<ul style="list-style-type: none"> • Scan excluded drives. When selected, this option forces all directories pointed to by shortcuts to be scanned. If not selected, the directories that are located on the drives that are excluded by the drive selection on the Drives tabs are not scanned. <p>When selected, the scanners may scan directories on network volumes. This is particularly useful when scanning for software licenses as the scanner detects files that are part of a network install that is accessible from the machine.</p>
Shortcuts to the network/Used programs launched from the network. (Targeted Directory scans only)	<ul style="list-style-type: none"> • Scan network drives. When selected, this option forces all directories pointed to by shortcuts to be scanned. The scanners may scan directories on network volumes. This is particularly useful when scanning for software licenses as the scanner detects files that are part of a network install that is accessible from the machine. <p>If not selected, the directories that are located on the drives that are excluded by the drive selection on the Drives and Drive Selection tabs are not scanned. Usually shortcuts to network drives or network directories from which used programs were executed are not scanned.</p>

File Scanning Tab

Enables you to specify the level of detail for the information collected about files and directories and the methods used to check and identify files.

User interface elements are described below:

UI Element	Description
Collect File Data	Enables you to configure the file scanning options.
Files to Scan sub-tab	Enables you to specify how much information is collected about files and the checking processes used. <ul style="list-style-type: none"> •  Add. Opens the Select Files to Process dialog box, enabling you to add a filter for files to scan: <ul style="list-style-type: none"> ○ File Name. Specify the relevant wildcard file type to process. For example, *.tmp means all files with the .tmp extension. Multiple specifications, separated with semicolons, are also accepted. ○ Action. Select one of the following actions:




- **Signature.** Collects file signatures for the specified type of file.

The signature is an ISO checksum (CRC) of the first 8KB of the file. To calculate the signature, the scanner opens the file and reads the first 8KB from it. Collecting signatures helps to establish the file's identity. Two different files rarely have the same signature. Signatures are used by the software recognition in analysis tools to improve software application recognition. Also, only those fields for which signatures were collected can optionally be identified by the scanner (see "[File Identification sub-tab](#)" on the next page).

- **Ignore.** Ignores the type of file specified in the **File Name** box.
- **Attributes.** Select from the following options as required:
 - **Read Only.** Files with the read-only attribute are capable of being displayed, but not modified or deleted.
 - **Hidden.** Files with the hidden attribute are not normally visible to users. For example, hidden files are not listed when you execute the **Command Prompt DIR** command. However, most file management utilities allow you to view hidden files.
 - **System.** Files with the System attribute.

In general, if a given attribute is not selected, the entry having the attribute will not match, even if the file name does.

- **Size Range (Kb).** If required, select the **Limit Processing by File Size** and specify the maximum and minimum file sizes. Only files within this size range are processed.

-  **Edit.** Enables you to edit the selected file scan filter.
-  **Delete.** Deletes the selected file scan filter.
-  **Move up/Move down.** Enables you to change the order of the filters.

The order in which process selections occur is important. For example, use Ignore first before making Signature process selections.





This ensures that the Ignore items are processed first before a file needs to be opened. It may be necessary to ignore certain files, the content of which is constantly changing.

Examples of files to ignore because of changing content are files that are normally used as swap files, such as pagefile.sys.

- **<Files to Scan list>.** Displays the checking methods used for processing files. You can build up a prioritized list of filters which specify a sequence of checking processes to be used.

Note:

	<p>Using the options on this page, it is possible to define which files get their signature calculated and collected, based on criteria such as file extension, attributes or size.</p> <p>Only files that have signatures enabled are opened and are available for further processing. If a copy of the file name is all that is required, use the following command.</p> <p>Ignore *.*</p> <p>The file name, size and attributes may still be picked up in the scan file but no signatures are calculated. This greatly reduces scanning time, but because less data is collected, application recognition accuracy may be adversely affected.</p>
File Identification sub-tab	<p>Enables you to determine whether the scanner identifies files based on their content.</p> <ul style="list-style-type: none">• Identify File Type. Instructs the scanner to check every file that was selected for signatures to identify all executable and archive files. The scanner can identify LZH, LHA, ZIP, ARJ, ARC and PAK archives. Selecting this enables two further options:<ul style="list-style-type: none">◦ Process Archives as Subdirectories. Treats archive files as subdirectories and lists the files included in each archive (it does not extract information from within these files). If this option is not selected, archive files are not scanned for embedded files and directories.<p>If this option is selected, a further option is made available:</p><ul style="list-style-type: none">• Process Archives inside GZIP Files. Enables the handling of archives located in gzip files (such as .tar.gz files). These are tar archives that were compressed using gzip. This option instructs the scanner to process such archives.◦ Collect Internal File Identification. Collects internal file information included in the executable file, for example, version data and legal copyright. This option must be enabled if you are using Express Teaching to teach applications. For more information about Express Teaching, see "Express Teaching Overview" on page 691.◦ ELF Prelinking Aware. During software scanning, this option instructs the scanner to check if an executable file has been pre-linked by the ELF Prelinking Utility (prelink). The ELF Prelink Utility is used to speed up loading times of ELF shared libraries and executables by modifying them to reduce the number of the reallocations the dynamic linker needs to do to load them in memory. If this option is enabled, the scanner calculates the size and signature of the file before it was pre-linked. This is useful for accurate application recognition since the file size and signature are used to perform application matching. However, enabling this option does produce extra overhead during the scan as the scanner needs to run the pre-link utility to

	<p>obtain the original executable file. The pre-linked file is not modified by the scanning process; the original file is only reconstructed temporarily in order to collect the size and signature.</p> <p>Note: This is for Linux platforms only.</p> <ul style="list-style-type: none"> • Preserve Last Access File Date. Collects the Last Accessed time stamp for files (where available). The support for the Last Accessed time stamp varies depending on the operating system and file system used. <p>When this setting is used on UNIX computers, although the last access time is preserved, the ctime of the file gets changed. For this reason we recommend that you do not use this setting on Linux, Mac OS X or UNIX computers.</p> <p>Note: When this option is enabled, the XML Enricher can make use of this feature to accurately estimate the time when recognized applications were last executed.</p> <ul style="list-style-type: none"> • Process Software Id Tag Files. Enables the collection of information from software tag files during the software scanning phase. During the hardware detection phase, the information from tag files that are located in the common system location and in the root of the application's installation directory is picked up. The tag files stored in the root of the application's installation directory can be collected only if the application is in a standard package format, or a directory where the application is installed is scanned during the software scanning phase. <p>For more information, see "Software Identification Tags" on page 197.</p>
<p>File Information to Store sub-tab</p>	<p>Enables you to define which file details to store in the scan file.</p> <ul style="list-style-type: none"> •  Add. Opens Select Files to Process dialog box, enabling you to add filter criteria for file information to store. For details, see "File Information to Store tab > Select Files to Process Dialog Box" on page 627. •  Edit. Enables you to edit the selected filter. For details, see "File Information to Store tab > Select Files to Process Dialog Box" on page 627. •  Remove. Deletes the selected filter. •  Move up/Move down. Enables you to reorder defined filter criteria. • By default, store information on all files. If selected, and no other options are specified, then information about all files is stored in the scan file. • By default, discard information on all files. If selected, and no other options are specified, then no file data is stored in the scan file. • Do not store empty directories When selected (default), the scanner discards information about directories that have no files in them. This can include directories that may have files in them, but you have set up the scanner not to scan for these particular types of file.


	<p>Note:</p> <ul style="list-style-type: none"> • In addition to the default settings, you can define a prioritized list of filters, in a manner similar to that of the File to Scan page. Each filter can specify directories or files to be included or excluded from being stored. Each file and directory entry found during scanning is looked up in the list, and the first matching entry determines whether the entry is stored or not. • The options chosen here can dramatically affect both scanning speed and scan file size. Under normal circumstances, the default options are adequate. • Multiple filter criteria can be specified on each line if they are separated by a semicolon.
--	---

Stored Files Tab

Enables you specify the files to be collected and stored (embedded) in the scan file created for each computer scanned. The types of files usually collected are system configuration files.

Important information	<ul style="list-style-type: none"> • The collected files can be viewed in Viewer or exported from Analysis Workbench. For more information, see "Inventory Tools" on page 534. • If a targeted directory scan selection was made earlier and does not include a specific directory in which a stored file may be found (including the root directory), then any required stored file must be specifically defined here with the full path.
------------------------------	--

User interface elements are described below:


UI Element	Description
	Clears the list of files to store.
Store specific files	Enables you to select specific files to be collected and stored (embedded) in the scan file created for each computer scanned.
Only Store files smaller than	Enables you to limit the size of the files to be stored When large files are collected and stored, restricting the size of files collected can prevent creation of very large scan files.
<Files to Store list>	<ul style="list-style-type: none"> • <Right-click menu>. Enables you to add a new file to store, or delete a file from the list. • File Name to Store. Displays a default list of system files. The name of the files

UI Element	Description
	<p>can include wildcard characters unless a specific directory is used.</p> <p>For example, collecting the Config.sys file for each computer scanned across a population provides a snapshot of the system configuration for each computer. This enables the analysis and consolidation of system configuration across the computer population.</p> <p>Other commonly collected files are Net.cfg, Profile.ini, AutoExec.Bat, Win.ini, System.ini, and Boot.ini.</p> <p>Note: The one Universal Discovery specific file included in the list is the override file, called override.ini on Windows systems and .override.ini on UNIX/Mac OS X systems. This is an ASCII file used by the scanner at run-time to store a list of files to be ignored (that is not opened at run-time). For more details, see "Directories Tab" on page 619.</p> <ul style="list-style-type: none">• Found Where. Displays the location of the file.<ul style="list-style-type: none">◦ /etc directory. Stores the file only if it is found in the UNIX /etc directory.◦ /var directory. Stores the only file if it is found in the UNIX /var directory.◦ Any Root. Stores the file only if it is found in a root directory.◦ Anywhere. Stores the file wherever it is located.◦ Root of Boot Drive. Stores the file only if it is found in the root of the boot drive.◦ Specific directory. All the files in the specific directory are collected, but sub-directories are not included. <p>For example, the stored files could be configured to be:</p> <pre>C:\Documents*.*</pre> <p>In this case, the scanner stores all the files in the C:\Documents directory.</p> <ul style="list-style-type: none">◦ Specific File. A specific copy of the file is collected irrespective of whether it is included in the software scan. <p>For example, the list of specific stored files could be configured to be:</p> <pre>C:\Documents\config.txt Z:\net.ini /etc/fstab</pre> <p>In this case, the scanner storee the config.txt file from the C: drive (when scanning PCs), the net.ini on the Z: drive (if it is available, and only on PCs) and a file named fstab in the /etc directory (when scanning UNIX machines).</p>

UI Element	Description
	<p>Note: Files are stored only if the directory where the file is located is included in the software scan, unless the specific directory is specified.</p>

File Information to Store tab > Select Files to Process Dialog Box


This dialog box enables you to select files and file attributes to store after scanning.

To access	Select Scanner Generator wizard > Software Details page > File Scanning tab > File Information to Store tab, and click Add  .
------------------	---

User interface elements are described below:

UI Element	Description
Storage	Determines whether the filtered file information is to be stored or discarded.
Type	<p>Determines the type of files to include in the filter. The filter options differ depending on the file type selected here.</p> <ul style="list-style-type: none"> • Files. Filters all files. • Files inside Archives. Filters only archived files. • Directories. Filters only directory files.
Options (Files)	<p>When Type > Files is selected, the following filter options are available:</p> <ul style="list-style-type: none"> • Identified as Executable. Files that are identified as any kind of executable (such as .exe and .com). <p>Note: This takes effect only if the Identify File Type option in the "File Identification sub-tab" is selected.</p> • Has UNIX or Mac Executable Attribute. UNIX allows three different levels of access to a file for three different categories of users: owner, group, and other. <ul style="list-style-type: none"> ◦ Read. View the file or directory without making changes. ◦ Write. Make changes to the file or directory ◦ Execute. Execute the file or list files in a directory. <p>This option instructs the scanner to store or discard files that have executable file access in any of the user categories (namely, owner, group or other.)</p> • Identified as Archives. Files that are identified as compressed, such as .zip, .lzh. <p>Note: This takes effect only if the Identify File Type option on the "File</p>

UI Element	Description
	<p>Identification sub-tab" is selected.</p> <ul style="list-style-type: none"> • Scanned (i.e. Not Ignored). Includes all files that are not ignored on the File Scanning tab. • Matches Wildcard Mask(s). Includes files that match the wildcards specified here. <ul style="list-style-type: none"> ◦ Case-sensitive match. Includes all files that match regardless of case. <p>Available: When Matches Wildcard Mask(s) is selected.</p> <p>Note:</p> <ul style="list-style-type: none"> • All of the selected options are OR-ed together; that is, the entry is considered a match if any of the selected entries match. • The order and content of these options can affect scanning speed and function significantly. If the default is Discard, and a Store - Identified as executable entry is included, all files have to be scanned before the scanner can determine if they are to be discarded.
<p>Options (Files Inside Archives)</p>	<p>When Type > Files Inside Archives is selected, the following filter options are available:</p> <ul style="list-style-type: none"> • Matches Wildcard mask(s). Includes archived files that match the wildcards specified here <ul style="list-style-type: none"> ◦ Case Sensitive Match. Includes all files that match regardless of case. <p>Available: When Matches Wildcard mask(s) is selected.</p> <p>Note: Files discarded in this way are not scanned either, and a wildcard filter can speed up the scanning process.</p>
<p>Options (Directories)</p>	<p>When Type > Directories is selected, the following filter options are available:</p> <ul style="list-style-type: none"> • Named. If this option is selected, the directory name specified in the entry field must match 100% (however, it is not case-sensitive) in order for a match to be established. For windows directories, the directory name must include the drive letter. The path wildcards * and ? can be used for matching the directory name. The root directory \ or / cannot be excluded in this way. For example, \Private would match any directory where a directory <i>starts with Private</i> • Where Name Contains. If this option is selected, the name specified in the entry field is a partial string; any directory containing this string in its name is considered a match. <p>For example, Temporary would match any directory with Temporary anywhere in the name.</p>

UI Element	Description
	<ul style="list-style-type: none">• Case Sensitive Match. For either of the directory options, includes all directories that match regardless of case.• Include Subdirectories . For either of the directory options, includes subdirectories of matching entries as well. This is particularly useful for discarding entire directory trees, such as recycle folders, temporary Internet files and private directories. <p>Note:</p> <ul style="list-style-type: none">• The contents of filtered directories are not stored in the scan file. If the Do not store empty directories option (File Information to Store tab) is selected, filtered directories are considered to be empty and are not stored in the scan file either. If this option is not selected, the filtered directories are represented in the Directories and Files tab of the Viewer application by a No entry  icon.• Directories are filtered prior to scanning (that is, directories that are not stored are not scanned at all). Consequently, directory filters may speed up scanning.

Asset Data Page

This page enables you to define and set up the asset data collected by the scanners.


Important information	<ul style="list-style-type: none"> • Available: When Asset Data is selected on the "Collection Page" (see page 609). • The Asset Number sub-tab is available in Manual Deployment mode only. • General information about the wizard is available in "Scanner Generator Wizard" on page 605.
Related tasks	"How to Set Up Asset Fields for Data Collection" on page 547
Wizard map	<p>The "Scanner Generator Wizard" contains:</p> <p>"Scenario Page" > "Standard Configuration Page" > "Collection Page" on page 609 > "Hardware Data Page" > "Software Data Page" > "Software Details Page" > Asset Data Page > "Scanner Options Page" > "Scanners to Generate Page" > "Generating Scanners Page"</p>



Asset Data Tab

Enables you to configure customized asset information as each computer is scanned.

Important information	<ul style="list-style-type: none"> • Initially, a default list of entries is displayed . These can be modified to create a custom list of entries. For information about including other information about the user, see IT Universe Manager in the <i>Universal CMDB Modeling Guide</i>. • By default, asset fields are not mapped to any of the UCMDB CI attributes so the data is only available in the scan files. To map the needed asset fields, you must configure the mapping between the asset fields and the desired UCMDB attributes. For details, see "How to Map Scan File Attributes to UCMDB" on page 572. • Each row in the Asset Fields list defines a piece of asset data and results in one item being collected during the inventory.
------------------------------	---

User interface elements are described below:

UI Element	Description
	<p>Create New Field. Opens the Choose Field dialog box, enabling you to choose an asset field to be automatically collected. For more information about the available asset fields, see "Asset Fields" on page 548.</p>

UI Element	Description
	<p>Edit Field. Opens the Asset Field Configuration dialog box, enabling you to edit the type and settings for the selected asset field. For more information, see "Asset Field Configuration Dialog Box" on the next page.</p>
	<p>Delete. Deletes the selected asset field.</p> <p>Tip: To delete multiple asset fields simultaneously, hold the Ctrl or Shift key while selecting the fields.</p>
<p><Asset Fields list></p>	<p>Displays the asset fields to be collected by the scanner.</p> <ul style="list-style-type: none"> • Caption. The display name for the asset field, as is displayed in the Inventory Tools. • Field. The name of the asset field. • Field Type. The type of field. The field can be a calculated, derived, or automatic field type. For more information, see "Asset Field Configuration Dialog Box" on the next page.

Asset Number Tab

Enables you to set options for managing the asset number used to uniquely identify a machine.


<p>Important information</p>	<ul style="list-style-type: none"> • Available in Manual Deployment mode only. <p>In Enterprise mode the options for selecting the source is always from the Asset tag field.</p> <ul style="list-style-type: none"> • Each computer that is scanned needs to be identified by a unique tag known as the Asset Tag. Asset tags are generally assigned to allow each hardware item to be recorded and identified in an asset management tool, such as Asset Manager. The conventions used depend on the numbering system and asset registering policies adopted by your organization. Ensure that your asset numbers can be reconciled between Universal Discovery and Asset Manager.
-------------------------------------	--

User interface elements are described below:


UI Element	Description
Asset Tag Field	<p>If selected, this uses the value in the Asset Tag field created in the Asset Data tab. This is usually used as the unique key to identify each computer.</p> <p>Note: When this is selected (default) and an offsite scan file will be saved, an Asset Tag field must be defined in the Asset Data tab before you can continue with the wizard.</p>
Scanner Command Line (/o switch)	<p>An offsite scan file name can also be specified by the -o: command line option. This overrides the scan file name (as well as the path, if specified).</p> <p>To configure this, select the Scanner Command Line (/o) option. The scan file name is taken from the command line. This is entered using the -o: command line option when the scanner is started, using the name specified.</p> <p>For example:</p> <pre>Scanwin32-x86 -o:FP00017</pre>

Asset Field Configuration Dialog Box

Enables you configure asset fields to collect during scanning.

To access	Select Scanner Generator wizard > Asset Data page > Asset Data tab > asset field in the list, and click Edit Field  .
Important information	The asset data fields are automatically populated. The data is either calculated or derived. The data can be extracted from text files, the Windows registry, environment variables and WMI fields. All data entry fields can be given a default value.

User interface elements are described below:

UI Element	Description
	<p>Opens the Asset Field Extract Options dialog box, enabling you to set up calculated asset fields so that only part of the string is selected instead of the entire string. They can also be set up, for example, to use the last part rather than the first part of the string. This can be useful for obtaining the last part of a calculated field that is too long.</p> <ul style="list-style-type: none"> • Extract Characters From. Enables you to specify whether you want to use the first part or the last part of the string, and the number of characters to skip from the beginning or end of the string respectively. <p>For example, if you have the string ABCDEF123, selecting Start and skip 4 characters would result in the string EF123.</p> • Options. Enables you the configure how to treat the extracted strings: <ul style="list-style-type: none"> ◦ Convert to Upper Case. Converts the alphabetic characters to upper case, if required.

UI Element	Description
	<ul style="list-style-type: none"> ◦ Treat Field as a File Name. Treats the string in the asset field as a file name. In the case of characters that are invalid in file names, you can define a character to replace the invalid character, or have the scanner delete the invalid character. • Default Value. Enables you to define a default value for the string if the extracted field is empty or not found. <p>For example, if the text string Not Found is entered in this box, then an empty field or a field that has not been found is assigned the value, Not Found.</p> <p>Available for: Calculated fields only.</p> <p>Note: This button is not available for user-defined fields.</p>
Caption	The display name for the asset field. The caption is displayed in the Inventory Tools.
Field	The name of the asset field. Click the Choose button to select a field type. For a list of the available asset fields, see " Asset Fields " on page 548.
Max Width	The maximum number of characters for the asset field.
Field Data Type > Calculated Fields	<p>Calculated fields can be automatically populated from data extracted from text files, the Windows registry, environment variables and so on.</p> <ul style="list-style-type: none"> • Environment Variable Extract. Accepts data from a specified environment variable set in the operating system. • Registry Extract. Extracts its value from the Windows registry. The Data field must contain a valid registry key name to extract from, for example: <pre>HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\TimeZoneInformation\StandardName</pre> • Text File Extract. Extracts information from a single line in a named text file. This field type is normally used for the Asset Number field. This is used to extract the asset number from the file, Asset.bat, on the line containing the text: SET ASSETNO= Other useful file extracts include the predefined SMS, which extracts the SMS Unique Machine ID. • WMI Extract. Extracts and stores pieces of data on Windows available through the WMI interface. The Windows scanner populates this field (if set up) on systems where WMI is enabled.
Field Data Type > Derived Fields	<p>Derived fields have dependencies on the data of other types of fields. That is, the data they contain is derived from other fields.</p> <ul style="list-style-type: none"> • Sequence. Enables you to define a sequence of up to ten asset or hardware fields. Each of these fields returns a value depending on the machine or environment

UI Element	Description
	<p>running.</p> <p>The value returned as the result of the sequence field is the first of these fields that contains a non-blank value.</p> <ul style="list-style-type: none">• Combination. Uses a substitution string to replace occurrences of %1, %2 and so on. placeholders with the actual values of hardware or asset fields. An example of a Combination field can be found in the Description field of the default Asset Data tab. <p>Up to five fields can be combined into one.</p> <ul style="list-style-type: none">• OS/Scan. Allows a single field to collect different information for different operating systems. For example, you may want to extract information from a registry on Windows and from a file on UNIX. <p>For each scanner platform a separate asset field could be defined.</p>
Field Parameters	Enables you to configure parameters for the field type selected. For details about the parameters for each field type, see "Asset Field Parameters" on page 550.

Scanner Options Page

This page is used to configure the behavior of the scanner during the usual scanning process and under exception conditions, and how to save the inventory results.

Important information	General information about the wizard is available in " Scanner Generator Wizard " on page 605 .
Wizard map	The " Scanner Generator Wizard " contains: "Scenario Page" > "Standard Configuration Page" > "Collection Page" on page 609 > "Hardware Data Page" > "Software Data Page" > "Software Details Page" > "Asset Data Page" > Scanner Options Page > "Scanners to Generate Page" > "Generating Scanners Page"

Saving Tab

Enables you to set options for saving the inventory scan results.

Note: For **Enterprise Mode** some of the options are pre-set to optimal values and cannot be changed.

User interface elements are described below:

UI Element	Description
Save result locally	<p>Saves the scan file to the local machine.</p> <p>By default, the local scan file is called local\$.xsf. This default name can be changed by using the -l scanner command line option.</p> <p>The Windows scanner uses the Hewlett-Packard\Universal-Discovery subdirectory of the application data directory for all users.</p> <ul style="list-style-type: none"> • Enable delta scan files. Enables delta file scanning, where the scanners first save the complete scan files offsite by copying the local scan files. <p>Instead of sending a full scan file to a server after every scan, the scanners calculate the difference (the delta) between the last full scan and the current one - and transfer just this data. This can dramatically reduce the amount of network bandwidth used when using Universal Discovery. By default, delta scanning is enabled.</p> <p>The XML Enricher re-assembles the full scan files based on the previous scan and the delta scan. No other Universal Discovery component uses the delta scan file. The re-assembled scan can however, be used in the Viewer and Analysis Workbench</p>

UI Element	Description
	<p>inventory tools.</p> <p>Note: To set up the scanner to handle delta scan files in Manual Deployment mode, see "How to Set up the Scanner to Handle Delta Scan Files in Manual Deployment Mode" on page 561.</p> <p>Note: In Enterprise mode results are always saved locally—this setting cannot be changed.</p>
<p>Save result to network (off-site)</p>	<p>Saves the scan file to a remote (offsite) disk (such as floppy disk or network drive). Click Advanced to specify the file path or URL:</p> <ul style="list-style-type: none"> • File. Saves the results to the specified file path. In the File Path/URL field, specify the path as follows: <ul style="list-style-type: none"> ◦ Normal file path. The full path name, beginning with the drive letter. For example: <code>c:\Inventory\Scans</code>. ◦ UNC file path. The UNC path. Use the following format: <code>\\servername\sharename\path\</code> For example: <code>\\DataFlowProbe\ScansIncoming</code> <p>Note:</p> <ul style="list-style-type: none"> • The specified UNC path must have write access. Do not specify a file name here. • The offsite save location can be overridden by using the <code>-p:</code> or <code>/p:</code> command line option. For example: <code>Scanwin32-x86 -p:C:\Scanners\</code> • A UNC path can also be entered as the argument to this option. The format for the UNC path is: <code>\\servername\sharename\path\</code> For example: <code>Scanwin32-x86 -p:\\DataFlowProbe\ScansIncoming</code> • In Windows, if the UNC name specified is visible to the machine, the scan file will be saved to the specified location, even if it is not mapped to a drive letter. • On UNIX and macOS machines, the UNIX/macOS save path is used instead, allowing UNIX-style syntax for specifying directories to be used. On UNIX/macOS, do not use drive letters, and the save path must instead start with <code>'/'</code> (root) and point to a directory writable by the scanner. • FTP/FTPS. The scanner saves the scan file to the FTP or FTPS server specified in the File Path/URL field. If necessary, provide the username and password to access the specified path.

UI Element	Description
	<p>When an FTP location is specified with the -p scanner command line option, the user name and password can be encoded into the URL as follows:</p> <p>ftp://user:password@host:port/dir</p> <p>For detailed information, see the description of -p:<path> in "Scanner Command Line Parameters Overview" on page 585.</p> <ul style="list-style-type: none"> • HTTP/HTTPS. The scanner saves the scan file to a Web server specified in the File Path/URL field, if it has been configured to allow writing to a particular directory. If necessary, provide the username and password to access the specified path. <p>Ensure that the web server has been configured to allow saving to it using HTTP. For details, see "Web Server Configuration for Saving Scan Files via HTTP" on page 596.</p> <p>By default both the Incoming and Original directories of the XML Enricher are shared via HTTP. This can be changed to HTTPS by adjusting the Data Flow Probe configuration. See "Processing Scan Files" on page 519.</p> <p>Note: (For Manual Deployment Mode only) If you select Save result to network (off-site) and use HTTPS for the generated scanner in the Windows platform, make sure that the following DLL files from the Universal Discovery agent installation folder (for example, C:\Program Files\Hewlett-Packard\Discovery Agent\bin32) are copied to the same folder where the generated scanner locates:</p> <ul style="list-style-type: none"> ◦ libeay64-disc-v09.dll ◦ ssleay64-disc-v09.dll
<p>Always create log file</p>	<p>The log file stores progress messages for scanner hardware detection, indicates what directory data is scanned, how long the software scanning took, and contains the status of the scan file saving.</p> <p>A log file is always created if this option is selected. If this option is not selected, a log file is only created if an error is encountered.</p> <p>Depending on the saving options chosen, the log file is saved to the following locations:</p> <ul style="list-style-type: none"> • The same location as the local scan file. • The same location as the off-site scan file (if an off-site location has been specified). • In the scan file itself (as a stored file). <p>The name given to the log file is the same as the name of the scan file. For example, if the scan file is called: XSF014.xsf, then the log file generated will be called: XSF014.log.</p>

Settings Tab

Enables you to control the behavior of the scanner as it scans each computer, and how it interacts with users. By default, the scanner is made to run with the lowest priority, but goes to full speed when the screen saver is active.

User interface elements are described below:

UI Element	Description
Define how fast the scanner should run	<p>When Run scanners at low priority is selected, the scanners can be set to run at slower than normal speed, so that they do not impact on the users' work.</p> <p>Use the slider control to specify how slow or how fast the scanner should run.</p> <p>On different target platforms, the Run scanners at low priority setting has different impacts:</p> <ul style="list-style-type: none">• On UNIX and macOS, the scanner impacts CPU utilization by performing a renice of itself to run at a lower process priority. For example, if CPU is available when the scanner is set to run at Normal speed, the scanner will always utilize what it needs. If the scanner is set to run at Slow speed, on UNIX endpoints the NICE flag is specified for the process, which means that if there are other processes with higher priority than the scanner, they will utilize the CPU, but if there are no such processes active, then the scanner will utilize the CPU.• On Windows, the scanner's process priority is not adjusted. Instead, the scanner proactively sleeps during the scanning process. The duration of the sleep is tied to the slider setting - the slower the setting is, the longer the sleep delay:<ul style="list-style-type: none">◦ For software scanning: the duration of the sleep is 100 milliseconds, but how often the scanner sleeps depends on the priority slider and the scanner settings. For example, if the scanner is collecting signatures, at the slowest setting it will sleep 100 milliseconds after opening/processing one file, while at the fastest setting it will sleep 100 milliseconds after opening/processing 9 files.◦ For hardware scanning: the longest the scanner would sleep for is 1.5 seconds (between hardware tests) at the slowest setting. <p>Note: The software scanning logic is single-threaded, so the scanner will never use more than one logical CPU. As most modern servers have multiple logical CPUs available, on machines with two or more CPUs this would represent 50% or less usage overall.</p> <p>When Run scanners at low priority is not selected, the scanners on Windows platforms will not sleep and on UNIX/macOS platforms the scanners' process priority will not be changed when the scanning process is running. On Windows platforms, the CPU utilization consumed by the scanners depend on a number of factors - how fast the</p>

UI Element	Description
	<p>CPU is compared to the speed of the disk, the scanner configuration (for example, whether file signatures/identification is done or not), etc.</p> <p>If you select Increase scanning speed when the screen saver is running (Windows), the scanner increases its speed to normal as long as it detects that the screen saver is running. As soon as the screen saver disappears, the scanner runs slower again.</p>
<p>Define various time-outs used by the scanner</p>	<ul style="list-style-type: none"> • Retry off-site save after error. The scanner attempts to retry off-site scan file saving if an error occurs the specified number of times. • Delay before retrying off-site save. The scanners wait for the specified amount of time (in hours, minutes and seconds) before retrying the off-site scan file saving, if an error previously occurred in this process. • Maximum random delay before scan. (Windows scanner only.) The scanner waits for the specified amount of time (in hours, minutes and seconds) before doing anything on the machine. Default: 00:00:00 hh:mm:ss Maximum value: 23:59:59 hh:mm:ss <p>If the scanner is launched via a login script, using this option allows the saving of scan files to be spread over a longer period to avoid overloading the network at busy periods. For example, in the morning, when all users come to work, power up their computers, and start the scanners at approximately the same time.</p> <ul style="list-style-type: none"> • Maximum software scan run time. Sets the maximum amount of time (in days, hours, minutes, and seconds) that the scanner runs. This setting is useful in protecting the scanner from scanning large volumes which were inadvertently included into the software scanning scope. If the scanner reaches the configured maximum time, it saves the scan files with the partial software details recorded right to that moment, and exists with the exit code 7. Default: 00:00:00:00 dd:hh:mm:ss (No limit applies.) • Software scan cut-off time. Sets the local time of the day on the managed computer (using the 24-hour clock) when the software scan has to stop. This setting is useful as a safety feature in cases when there are certain periods of the day during which the scanning must not be performed. When the cut-off time is reached, the scanner saves the scan file containing the partial software inventory, and exits with the exit code 7. <p>Note: This option must be used with great care to avoid incomplete results being saved regularly. The inventory has to be scheduled early on during the day to allow the scanner to complete the full software inventory.</p> <p>Default: 00:00:00 hh:mm:ss, meaning the scan is not stopped. If, for example, you want to stop the scan before midnight, enter 23:59:59.</p>

UI Element	Description
Define other settings that control the scanner behavior	<p>Leave at least this amount of space in the Temp directory. Enables you to set the amount of the disk space (in MB) the scanner must reserve to be available in the Temp directory before failing.</p> <p>During software scanning the scanner stores the partial software scan result in the temp directory. If the amount of disk space available in the Temp directory is too low, normally the scanner uses all the available space and when none is left, it fails. However, during the time when no Temp space is available, other processes running on the system may start failing as well. This setting ensures that at least the specified amount of space is left reserved for other processes to continue their normal operation.</p> <p>For example, if 5 MB is specified, the scanner uses the space in the Temp directory until there is 5 MB of free disk space left, and when this limit is reached, the scanner fails.</p> <p>Note: This number must be an integer.</p> <p>Default: 0, meaning no limitation.</p>

Miscellaneous Tab

User interface elements are described below:

UI Element	Description
Terminate the scanner if the following environments are detected	<p>When the scanner is run inside a virtual environment, you may not want a full software scan to take place because this would scan the server for every virtual machine.</p> <p>When the scanner detects the selected virtual environment, the scanner exits without doing any processing with a special error level 20, allowing a script that launches the scanner to handle this situation and launch another scanner tailored for the virtual environment, if required.</p>
Impersonate currently logged in user (Windows)	<p>Defines whether to impersonate the currently logged in user.</p> <p>When this option is cleared, the scanner will run under the Windows LocalSystem account and will not try to impersonate any logged in user. The scanner then assumes that the LocalSystem account has the necessary privileges to capture all the software on that system.</p> <p>By default, this option is selected.</p>
Select the action to perform when no user	<p>Defines the action to take if there is no user logged into the computer (Windows scanner only).</p> <ul style="list-style-type: none"> • Scan immediately. Forces the scanner to run under the LocalSystem

UI Element	Description
is logged into the computer (Windows)	<p>account. It will not be able to collect the environment information for a particular user. The environment settings for the LocalSystem account will be detected. Also any program running under the LocalSystem account does not have access to network resources, so the scanner will not be able to access any files or directories on the network.</p> <ul style="list-style-type: none"> • Wait until someone logs in. Instructs the scanner to wait until an interactive user logs into the system. When this is detected, the scanner impersonates this user and executes using this user's account. This allows the scanner to collect environment information for the user. <p>Note: This setting is not suitable for standalone servers where interactive users rarely log in.</p> <ul style="list-style-type: none"> • Exit the scanner. The scanner simply exits without scanning the computer. <p>Note:</p> <ul style="list-style-type: none"> • Enterprise mode: The Windows scanner is launched via the Universal Discovery agent or by agentless NTCMD protocol. The agent itself, or the NTCMD protocol component, runs as a Windows service under the LocalSystem account. However, the scanner always tries to impersonate the account of the currently logged in user in order to collect the required network, environment, and other configuration information for the user. This setting specifies the scanner behavior when no user is logged in at the time the scan is scheduled. • Manual Deployment mode: The scanner runs under the account of the currently logged in user, so normally these settings do not apply. They might only take effect when the scanner is launched by a software distribution tool that can run it under the LocalSystem account. In this case, the above logic for Enterprise mode applies.
TCP/IP connectivity options	<p>Enable the use of the pfiles command. Enables the use of the pfiles command on the Solaris and HP-UX platforms.</p> <p>Default: No.</p>

Troubleshooting Tab

Enables you to set up additional troubleshooting options for the scanners.

User interface elements are described below:

UI Element	Description
Additional command line parameters to supply to the scanners	<p>You can specify additional content for the override files here. Although the options for the scanner are normally set using the Scanner Generator, it may be necessary to change some settings to allow better operation on some machines. The operation of a scanner can be modified with the use of the various command line parameters.</p> <p>Additional file scanning configuration specified in the override.ini (Windows) file and the .override.ini file (UNIX/macOS) can be entered in this field. The content specified here is processed by the scanner before processing the content of the override file (if available on the system where the scanner runs).</p>
Additional content for .override.ini file	<p>You can override the settings of the file systems, directories, and files during the software scanning process by specifying additional settings in the override file. As indicated, on Windows systems, the name of this file is override.ini. On UNIX and macOS systems, the name of this file is .override.ini. The override file must be located in the same directory as the scanner executable.</p> <ul style="list-style-type: none"> File Systems <p>Because it is always possible, particularly on UNIX and macOS systems, that some file systems are not in the list, you can create a file where you can specify any additional names of file systems that you want to include or exclude during scanning.</p> <p>You can also specify names of existing file systems in case you want to change the inclusion/exclusion of such file systems after the scanner has been generated.</p> <p>The format of the file is as follows:</p> <pre>[include] fs=<name of a file system> [exclude] fs=<name of a file system></pre> <p>There can be several fs entries in each section.</p> <p>For example, to ensure that all afs mount points are scanned, and that nfs and swap volumes are not, create the override file with the following contents and place it in the same directory as the scanner prior to running:</p> <pre>[include] fs=afs [exclude] fs=nfs fs=swapfs</pre> <p>Note:</p> <ul style="list-style-type: none"> The name of the file, the sections and the files systems are case-sensitive

UI Element	Description
	<ul style="list-style-type: none">○ For the feature to work correctly, the override file must be present in the directory in which the scanner resides.
	<ul style="list-style-type: none">● Directories and Files<p>The override file can also be used to exclude specific directories or files from being scanned without regenerating the scanner.</p><p>Note: Files can only be excluded; they cannot be included.</p><p>To make use of this file, add one or more</p><pre>dir = <name></pre><p>or</p><pre>file = <name></pre><p>entries to the [exclude] section of the override file. Excluded directory names must be fully qualified. Excluded file names can contain wild cards.</p><p>Note: When excluding files using the override file, the scanner may still store information about the excluded files in the scan file. Adding file entries to the override file ensures that the file will not be opened for any reason, so no file identification, signatures, or archive processing will happen for excluded files.</p><ul style="list-style-type: none">○ Example 1<p>Exclude a specific file system, two directories and all files with exe extension.</p><pre>[exclude] fs=autofs dir=/temp dir=/etc file=*.exe</pre>○ Example 2<p>This runs a scan without software on a Windows machine.</p><pre>[exclude] fs=FAT fs=NTFS</pre>○ Example 3 Virus Warning<p>Since the scanner opens files on the computer, if real-time antivirus software is in operation, it may detect a virus being present in a file.</p><p>Depending on the virus product being used, actions will have been defined to deal with an encountered virus. Some will try to deal with the problem and</p>


UI Element	Description
	<p>immediately disinfect the file. Others will try to move the infected file to a quarantine directory and rename its file extension. In this case, the quarantine directory may be scanned by the scanner later during its scan.</p> <p>To prevent this from happening, use the override file with *.vir specified for exclusion (where .vir is a typical quarantine file extension). Check the specific virus product to find the extension for this type of file.</p>

Scanners to Generate Page

This page is used to specify which scanners to generate and where they will be stored.

Important information	General information about the wizard is available in "Scanner Generator Wizard" on page 605 .
Wizard map	The "Scanner Generator Wizard" contains: "Scenario Page" > "Standard Configuration Page" > "Collection Page" > "Hardware Data Page" > "Software Data Page" > "Software Details Page" > "Asset Data Page" > "Scanner Options Page" > Scanners to Generate Page > "Generating Scanners Page"

User interface elements are described below:

UI Element	Description
	Generates the scanners based on the settings defined in the Scanner Generator wizard.
Output Options tab	Enables you to set up scanner descriptions, save the configuration to an HTML file if required, and (Enterprise Mode only) name the configuration (. cxz) file. See below.
Scanners tab	Enables you to select which of the scanners to generate. Available: In Manual Deployment mode only.

Output Options tab

Enables you to set up scanner descriptions, save the configuration to an HTML file if required, and (Enterprise Mode only) name the configuration (.**cxz**) file.

Having a scanner description is very useful for change control if different scanners are being developed for different circumstances. It is useful for documentation purposes, to have a file with the scanner's configuration stored in a file. If this step is missed, load the scanner or a scan file derived from it into Scanner Generator to produce the documentation.

User interface elements are described below:

UI Element	Description
Scanner	A description that identifies the scanner.

UI Element	Description
Description	<p>For example:</p> <p>Standard PC Inventory – May 18, 2012</p> <p>The scanner description is saved in the scan file as the hwScannerDescription hardware field, and subsequently in UCMDB in the description attribute of the inventory_scanner CI.</p>
Save scanner options to an HTML file	<p>Saves the scanner options to the specified HTML file. Enter the full path and file name.</p> <p>This instructs the Scanner Generator to output an HTML file containing a complete listing of all settings defined elsewhere in the program. The HTML file cannot be used by the Scanner Generator, but is intended for user/internal documentation purposes.</p> <p>Example of the ScannerOptions.html File</p> <p>You can look at a ScannerOptions.html file using an Internet browser such as the Microsoft Internet Explorer. The following shows the first few sections that you will find in the file:</p> <hr/> <p style="text-align: center;">Scanner Configuration</p> <p>General</p> <ul style="list-style-type: none"> • Product Version: 10.00 (01 Oct 2011) • Scan File Version: 7.60 (2011-10-01 15:56:52) • Platform: Win32 Scanner • Description: Scanner • Types of Data Collected: Software, Hardware, Asset Data • Default Scan File Name: DEFAULT <p>Hardware and Configuration</p> <ul style="list-style-type: none"> • Excluded Hardware: Compaq Asset Tag, Device Drivers, Installed Applications (WMI) <p>Software Data</p> <ul style="list-style-type: none"> • Allow scanner command-line to override this selection: Yes • Drives: Default • Drive Selection: Local hard disk, File, Unknown • Filesystem Types: FAT, Device Driven, HPFS, NTFS, ext, ext2, ufs, tmpfs, vxfs, hfs, hfs Extended, jfs, ext3, DVD-ROM <p>Directories</p> <ul style="list-style-type: none"> • Environment Variables: PATH;LIBPATH • Options: Scan subdirectories • Windows Only <ul style="list-style-type: none"> ○ Shortcuts: Start Menu, Desktop ○ Shortcut Extensions: exe;com;bat;cmd;ocx;dll ○ Windows Services: Yes ○ File Associations: Yes ○ Software Utilization: Yes
Scanner Generator Output (Enterprise)	<p>In Enterprise mode, the Scanner Configuration file (.cxz) is saved on the UCMDB database (resources for the InventoryDiscovery adapter) as well, using the same file name as the copy specified in the Configuration File Name to Use field.</p>




UI Element	Description
mode only)	<p>The configuration file is a compressed XML file containing the settings for the scanner you are currently configuring.</p> <p>When the scanners are used in the Enterprise Mode, they read the configuration from a separate configuration file. This is a binary file with a .cxz extension. The typical size of the configuration file is about 3 KB. As the size of the configuration file is significantly smaller than the size of the complete scanner, a separate scanner configuration is useful for repetitive inventory collection when the configuration of the scanner has been altered. In this case only a small configuration file is delivered to the user's computer to run with the original scanner instead of delivering the entire new scanner.</p>

Scanners tab

Enables you to select which of the scanners to generate.

Note: Available in Manual Deployment mode only.

User interface elements are described below:

UI Element	Description
Generate Scanners for	<p>Enables you to select scanners to generate.</p> <p>Selecting the check box adjacent to scanner enables the scanner.</p> <p>Click  or  to enable or disable all of the scanners in the tree respectively.</p> <p>Click  to reverse the scanners selected. That is, those that were enabled become disabled, and those that were disabled become enabled.</p> <p>When you hover over a scanner with the mouse, the status bar under the tree displays whether the scanner is enabled or disabled, and displays the full scan file name of where - on the local computer that runs the browser session - the scanner will be generated.</p> <p>Note: (Windows and Linux only) Use the 64-bit version of the scanner when running the scanner on a 64-bit computer to ensure that data is collected as expected.</p>
Base Scanner File Name	<p>The base name of the scanner (up to five characters).</p> <p>Make sure to use a fully qualified file name</p> <p>Alternatively, for each scanner, you can either have a file name to identify the</p>


UI Element	Description																										
	<p>operating system, or you can use a separate directory for each operating system.</p> <p>The initial part of this file name can be entered in the Base Scanner File Name box. The remaining three characters of the file name are used to describe the scanner executable.</p> <p>For example, by entering scan (the default setting) in the Base Scanner File Name box, the following scanners can be generated (if they have been selected in the Generate Scanners For section):</p> <table border="1" data-bbox="407 600 951 1346"> <thead> <tr> <th data-bbox="407 600 662 657">Scanner File Name</th> <th data-bbox="662 600 951 657">Scanner Type</th> </tr> </thead> <tbody> <tr> <td data-bbox="407 657 662 714">scanwin-x64.exe</td> <td data-bbox="662 657 951 714">Windows (x64)</td> </tr> <tr> <td data-bbox="407 714 662 770">scanwin-x86.exe</td> <td data-bbox="662 714 951 770">Windows (x86)</td> </tr> <tr> <td data-bbox="407 770 662 827">scanwinh-x64.exe</td> <td data-bbox="662 770 951 827">Windows (x64, hidden)</td> </tr> <tr> <td data-bbox="407 827 662 884">scanwinh-x86.exe</td> <td data-bbox="662 827 951 884">Windows (x86, hidden)</td> </tr> <tr> <td data-bbox="407 884 662 940">scansolaris-sparc</td> <td data-bbox="662 884 951 940">Solaris (SPARC)</td> </tr> <tr> <td data-bbox="407 940 662 997">scansolaris-x86</td> <td data-bbox="662 940 951 997">Solaris (x86)</td> </tr> <tr> <td data-bbox="407 997 662 1054">scanhpux-hppa</td> <td data-bbox="662 997 951 1054">HP-UX (HPPA)</td> </tr> <tr> <td data-bbox="407 1054 662 1110">scanhpux-ia64</td> <td data-bbox="662 1054 951 1110">HP-UX (ia64)</td> </tr> <tr> <td data-bbox="407 1110 662 1167">scanaix-ppc</td> <td data-bbox="662 1110 951 1167">AIX (POWER)</td> </tr> <tr> <td data-bbox="407 1167 662 1224">scanlinux-x86</td> <td data-bbox="662 1167 951 1224">Linux (x86)</td> </tr> <tr> <td data-bbox="407 1224 662 1281">scanlinux-x64</td> <td data-bbox="662 1224 951 1281">Linux (x64)</td> </tr> <tr> <td data-bbox="407 1281 662 1337">scanmacosx-x86</td> <td data-bbox="662 1281 951 1337">Mac OS X (x86)</td> </tr> </tbody> </table>	Scanner File Name	Scanner Type	scanwin-x64.exe	Windows (x64)	scanwin-x86.exe	Windows (x86)	scanwinh-x64.exe	Windows (x64, hidden)	scanwinh-x86.exe	Windows (x86, hidden)	scansolaris-sparc	Solaris (SPARC)	scansolaris-x86	Solaris (x86)	scanhpux-hppa	HP-UX (HPPA)	scanhpux-ia64	HP-UX (ia64)	scanaix-ppc	AIX (POWER)	scanlinux-x86	Linux (x86)	scanlinux-x64	Linux (x64)	scanmacosx-x86	Mac OS X (x86)
Scanner File Name	Scanner Type																										
scanwin-x64.exe	Windows (x64)																										
scanwin-x86.exe	Windows (x86)																										
scanwinh-x64.exe	Windows (x64, hidden)																										
scanwinh-x86.exe	Windows (x86, hidden)																										
scansolaris-sparc	Solaris (SPARC)																										
scansolaris-x86	Solaris (x86)																										
scanhpux-hppa	HP-UX (HPPA)																										
scanhpux-ia64	HP-UX (ia64)																										
scanaix-ppc	AIX (POWER)																										
scanlinux-x86	Linux (x86)																										
scanlinux-x64	Linux (x64)																										
scanmacosx-x86	Mac OS X (x86)																										
Output Directory	The directory where the generated scanners are saved.																										
Output Directories	<p>The manner in which scanner files are named and stored.</p> <ul style="list-style-type: none"> • One Directory. All scanners that are selected are stored in one directory. • Separate Directories. All scanners that are selected are stored in individual subdirectories named per the operating system. <p>Note: Scanner file names are changed to scan.exe.</p>																										

Generating Scanners Page


After you have selected the scanners to be generated and have clicked **Generate**, the last page of the Scanner Generator wizard is displayed. This page shows the progress information during the generation of the actual scanner executable.

Important information	<p>General information about the wizard is available in "Scanner Generator Wizard" on page 605.</p> <p>In Enterprise Mode, the scanner configuration is generated instead of stand-alone scanners, and the configuration is uploaded to the UCMDB server and stored in the UCMDB database as the Scanner Configuration resource files in the Inventory Discovery adapter. If you chose to generate your scanner from a stored default predefined configuration on the server when you were on the Standard Configuration page, you will be told to rename it, since default predefined configurations cannot be overwritten.</p> <p>Right-clicking anywhere in the log window displays a shortcut menu which allows you to:</p> <ul style="list-style-type: none">• Save the contents of the window to a log file.• Copy the contents of the log window to the clipboard.• Clear the log window. <p>If a scanner already exists with the same name in the chosen directory, a confirmation message is displayed. This allows you to choose whether to overwrite the existing scanner.</p> <p>After the scanners have been generated, click Finish to exit the Scanner Generator. The generated scanners can be found in the directory specified in the Scanners tab of the Scanners to Generate page.</p>
Wizard map	<p>The "Scanner Generator Wizard" contains:</p> <p>"Scenario Page" > "Standard Configuration Page" > "Collection Page" > "Hardware Data Page" > "Software Data Page" > "Software Details Page" > "Asset Data Page" > "Scanner Options Page" > "Scanners to Generate Page" > Generating Scanners Page</p>

XML Enricher: Software Recognition Configuration Dialog Box


To access	<p>Use one of the following:</p> <ul style="list-style-type: none"> • Select Data Flow Management > Software Library, and click . • Select Universal Discovery > Discovery Modules/Jobs > Discovery Modules > Hosts and Resources > Inventory Discovery > Inventory by Scanner > Properties tab > Global Configuration Files pane, and double-click EnricherServiceSettings.ini. • Select Universal Discovery > Discovery Modules/Jobs > Discovery Modules > Hosts and Resources > Inventory Discovery > Inventory by Scanner > Inventory Discovery by Manual Scanner Deployment > Properties tab > Global Configuration Files pane, and double-click EnricherServiceSettings.ini. • When creating or editing an Inventory Discovery activity, in the Preferences tab click Mapping Options. For details, see the <i>Universal CMDB Discovery and Integrations Content Guide</i>.
Related tasks	<p>"How to Configure XML Enricher to Suit the Probe Deployment Mode" on page 564</p>
See also	<ul style="list-style-type: none"> • "XML Enricher" on page 521 • "Enriched Scan File Structure" on page 530

User interface elements are described below:

UI Element (A–Z)	Description
	Restores the XML Enricher settings to the default setting.
General tab	Enables you to set general XML Enrichment options. See "General Tab" below.
SAI Recognition tab	Enables you determine how the XML Enricher uses the SAI files for application recognition. See "SAI Recognition Tab" .

General Tab

User interface elements are described below:

UI Element (A–Z)	Description
Basic	<ul style="list-style-type: none"> • Process Utilization Data. By default this option is set to Yes. If you want to stop processing utilization data, change this option to No. • Application Recognition. There are the following options for Application recognition: <ul style="list-style-type: none"> ◦ Software application index (SAI). This is the default setting. Instructs the XML Enricher to use the Software Application Index files (.zsai) to perform application recognition. The SAI files contain a database of software applications. By default, only executable files are sent to the recognition engine for processing. You can set this so that all files are sent to the recognition engine by modifying the filter settings. See "Filtering" on page 654. ◦ No recognition. Disables any application recognition. When recognition is disabled, scan file processing is slightly faster as no file information is sent to the recognition engine for processing. However, the processed scan files are not enriched with application data, and no application data is added to the UCMDB database. • Import unrecognized files. By default, this option is set to No. If you want to use Express Teaching to teach applications, change this option to Yes. For more information about Express Teaching, see "Express Teaching Overview" on page 691.
Scan File Management	<p>Enables you to configure how to manage the scan files.</p> <p>Group Processed Scan Files. The grouping commands help you organize your scan files in the processed directory. You can group your scan files based on the value of the hardware fields collected by the Scanners. For example, if the grouping is done on the hwHostOS field, all scan files for computers having the same operating systems are grouped in the corresponding directory for that operating system.</p> <p>Clicking the  button opens the Scan File Group dialog box, enabling you to create a scan file group:</p> <ul style="list-style-type: none"> • Group processed scan files by hardware field. Select a hardware field from the drop-down list. Details of the field are displayed in the Detail pane. <div style="border-left: 2px solid black; padding-left: 10px; margin-left: 20px;"> <p>Note: The value of the selected hardware field is used as the name of a subdirectory under the Processed directory. If the chosen field is blank in a scan file, that file is moved to a Blank directory.</p> </div> • Value to use if hardware field is blank. Because the directory name cannot be empty, when the value of the selected hardware field is empty, the string configured in this field is used instead to name the subdirectory.

SAI Recognition Tab

User interface elements are described below:

<p>SAI Files</p>	<p>Enables you to specify the SAI files that the XML Enricher uses to recognize applications. The master SAI set comes with the latest Content Pack and is available in the sai.zip package. For details about deploying your own SAI files, see "SAI Files Pane" on page 682.</p> <ul style="list-style-type: none"> • <SAI Files grid>. For each SAI file that appears in the list, the following information is displayed: <ul style="list-style-type: none"> ◦ Use. Specifies whether an SAI file is used by the XML Enricher. The XML Enricher only uses the selected SAI files. ◦ Name. The name of the SAI file. ◦ ID. The ID for the user SAI file. <div style="border-left: 2px solid black; padding-left: 10px; margin-left: 20px;"> <p>Note: Because a master SAI file does not have an ID, it displays an ID of N/A. Each user SAI receives an integer ID on creation. The ID must be unique within the organization. The UD tools (including XML Enricher and Inventory Tools) need all user SAIs they load to have a different ID. It is therefore important to ensure IDs are unique.</p> </div> ◦ Size. The size (in kilobytes) ◦ Type. The file type: Master (read-only) or User (editable) ◦ Date. <ul style="list-style-type: none"> • Master SAI files: The date the file was created. • User SAI files: The date the file was last saved. ◦ Description. The description given to the SAI file when it was created. • SAI File Used to Store Rule-Created Items. Specifies the SAI file to which items created by rules are added. These rules are present within the SAI files themselves. You can specify additional rules by using the SAI Editor. <p>If this field is left blank, Universal Discovery creates a file called Auto.zsai and puts this in the same location as the first Master SAI.</p> <div style="border-left: 2px solid black; padding-left: 10px; margin-left: 20px;"> <p>Note:</p> <ul style="list-style-type: none"> ◦ For descriptions of SAI files, see "Software Application Index (SAI) Files" on page 523. ◦ For more information about SAI files and the process of application recognition, see the SAI Editor documentation. </div>
<p>Advanced</p>	<p>Determine how the XML Enricher performs the SAI application recognition. The</p>

SAI Options	<p>available options are as follows:</p> <ul style="list-style-type: none">• Level 3 recognition heuristics. This option determines when the XML Enricher processes scan files for a particular machine.<ul style="list-style-type: none">◦ Yes. The XML Enricher waits until all the files in all the directories on that machine have been read before issuing its final recognition information. More accurate recognition is achieved.◦ No. Machine-based recognition does not take place, and recognition data is returned after each directory is loaded.<p>A time overhead of about 10% is normal when Level 3 recognition heuristics is enabled.</p><p>Default: Yes.</p>• Auto-identify unrecognized device driver file.<p>If this option is set to Yes, it instructs the XML Enricher to mark files that meet the following criteria as recognized in the enriched scan file:</p><ul style="list-style-type: none">◦ They cannot be identified by standard SAI recognition.◦ They have the Device Driver attribute.<p>Files used as Device Drivers represent a large portion of the files that are not identified by the Application Library. Being able to identify these automatically can significantly reduce the effort required to achieve good recognition rates.</p><p>Default: Yes.</p>• Override OS language. Works in conjunction with the Preferred language option (below). If you specify a Preferred language, and you set the Override OS language option to Yes, the recognition engine overlooks the OS locale setting and uses the Preferred language that you specify.<p>Default: No</p>• Report multiple installations of the same version. Specifies whether to report multiple instances of the same application version that are installed.<p>Default: No</p><p>Note: If a user wants to report multiple installations of the same version software, set the correct scan configurations for Inventory Discovery by Scanner job so that scanner can collect enough information into a scan file.</p>• Preferred language. Enables you to specify the language that the XML Enricher uses when it encounters more than one language version of the same application. For example: if there are two application versions in the SAI (one English and one French) that are very similar, or the same in terms of the comprising files, setting the preferred language to French favors French applications if the recognition ratings for these application versions are the
--------------------	--

	<p>same.</p> <p>This option works in conjunction with the Override OS Language option (above).</p> <p>Default: Neutral. No preferred language is set.</p>
Filtering	<p>Determines what types of files the XML Enricher processes:</p> <ul style="list-style-type: none">• Use only files with the following extensions. Specifies the extensions of the particular file types processed by the XML Enricher. Type the extensions that you want to use directly into the box. Separate extensions with commas or semicolons. Only these file types are processed.• Use only executable files. Specifies that only executable files should be processed by the recognition engine. This includes *.exe, *.com, *.dll and other files containing executable code. Default: Yes• Look also for files within archives. Specifies that files within archive files should be processed. The following archive file types are supported: ARJ, ZIP v1, ZIP v2, LHA, LZH, ARC, CAB, TAR, GZIP, TAR/GZIP, and PAK. Default: No• Regular expressions used to filter junk files. Some files may be executable but are of no interest for licensing or other purposes. These files are often identifiable by file name. For example: TMP[0-9]*\.\\$\\$\\$. This option enables you to specify file names that should be ignored by the XML Enricher. Do this by entering regular expressions in the multi-line edit box - one expression on each line. Files whose names match the regular expressions are ignored. When the XML Enricher matches a file name against a junk filter regular expression, the file name is first converted to lowercase. For this reason, all letters entered as part of the regular expression must be in lowercase for a match to successfully occur.

Chapter 16: Just-In-Time Discovery

This chapter includes:

Just-In-Time Discovery Overview	655
How to Configure Just-In-Time Discovery	655

Just-In-Time Discovery Overview

Universal Discovery integrates with RUM to provide real time, passive discovery and monitoring of topology changes in a given environment. This is known as the Just-In-Time (JIT) discovery mechanism.

One or more RUM Engines can be configured to interact with Universal Discovery's Data Flow Probes. The RUM Engine gathers information from RUM Probes in its network, and passes relevant information on to the Data Flow Probes. From the Universal Discovery perspective, the RUM Engines behave as passive discovery probes, where the Data Flow Probes are the active probes.

The passive probes also send notifications about discovered information to the Data Flow Probes. Notifications can include, for example, changes in environment topology, such as an unseen IP address, or software that is not running. You configure these notifications in Universal Discovery. Based on these notifications, the Data Flow Probes report, add, or remove relevant CIs to or from the UCMDB Server, or designate them as candidates for deletion.

For details about setting up the passive discovery probes and running JIT Discovery, see "[How to Configure Just-In-Time Discovery](#)" below.

How to Configure Just-In-Time Discovery

This task describes how to set up Just-in-Time discovery to provide passive, real-time discovery and monitoring of traffic in a given environment.

To learn more about Just-In-Time discovery, see "[Just-In-Time Discovery Overview](#)" above.



1. Prerequisites

Real User Monitor (RUM) version 9.20 or later must be installed on a separate server, and must be

running and configured to integrate with a Data Flow Probe.

Note: The Micro Focus RUM Installation can be downloaded from [Software Support](https://softwaresupport.softwaregrp.com) (<https://softwaresupport.softwaregrp.com>). Search for **BAC Real User Monitor**.

To configure Micro Focus RUM to integrate with a Data Flow Probe:

- a. In RUM, select **Configuration > UD Probe Connection Settings**.
 - b. Enter the host name of the Data Flow Probe to which the RUM Engine is to report, and port through which it is to send data to the Data Flow Probe.
 - c. Select a connection protocol.
 - d. Leave Authentication, Proxy, and SSL settings empty.
 - e. Save your configuration.
2. Configure passive discovery probe notifications and removal verification policy
- a. In **Data Flow Management > Data Flow Probe Setup >**, select the domain where the passive discovery probe (RUM Engine) resides.
 - b. In the Domain and Probes pane, click **Passive Discovery Probes**.
 - c. In the **Passive Discovery Probes Pane** configure the passive probe notification options and removal verification policy. For details see "[Passive Discovery Probes Pane](#)" on page 126.
 - d. In the **Domains and Probes** pane select the passive discovery probe that you want to configure
 - e. In the **Passive Discovery Probe details > Passive Discovery Integrated Ranges** pane, configure the ranges over which the passive discovery probe should perform discovery, and the ports it should monitor. For details, see "[Passive Discovery Probe Details Pane](#)" on page 128.
 - f. Ensure that the passive probe status is **Connected**, If it is suspended, click the **Resume Probe**  button in the Domains and Probes pane toolbar.
3. Activate passive Just-in-Time discovery
- a. Go to the **Universal Discovery > Discovery Modules/Jobs** tab.
 - b. Under **Network Infrastructure > JIT Discovery** select **JIT Passive Discovery**.
 - c. Click the **Activate Selected Discovery Jobs**  button. When the passive probes are activated, they download configuration (ranges and notifications) and start to report

notifications to the Data Flow Probe.

Chapter 17: Discovery Progress and Results

This chapter includes:

Managing Problems With Error Reporting	658
Data Validation on the Data Flow Probe	659
Filtering Discovery Results	660
How to View the Current Status of Discovered CIs	661
How to Find Discovery Errors	661
How to Manage Discovery Errors	662
How to Enable Content Data Validation	663
Content Data Validation Jython Scripts	664
Discovery Progress and Results User Interface	666

Managing Problems With Error Reporting

During discovery, many errors may be uncovered, for example, connection failures, hardware problems, exceptions, time-outs, and so on. You can drill down from the Trigger CI that caused the problem to view the error message itself.

DFM differentiates between errors that can be ignored (for example, an unreachable host) and errors that must be dealt with (for example, credential problems or missing configuration or DLL files). Moreover, DFM reports errors once, even if the same error occurs on successive runs, and reports an error even if it occurs once only.

For details on severity levels, see "Error Severity Levels" in the *Universal CMDB Developer Reference Guide*.

Error Table in Database

All DFM errors are saved to the **discovery_problems** table in the Probe Manager database schema. (The error information is saved to the database—and is not handled in the Probe's memory—to guarantee delivery to the server.) The Probe holds the latest list of problems for each Trigger CI. After each run, the Probe checks for changes and reports them in the Discovery Progress pane. For details, see "[Discovery Progress Dialog Box](#)" on page 670.

Data Validation on the Data Flow Probe

After discovery or integration, results are processed, each one verifying a different aspect of the outgoing discovery result - class model validation, redundant results validation, and so on. This is called the **result processing chain**.

This section includes:

- ["Class Model Data Validation" below](#)
- ["Content Data Validation" below](#)

Class Model Data Validation

The CIT model resides on the Data Flow Probe (as well as in the CMDB). This enables data validation to take place on the Probe when receiving data from services. Problems are generated for a specific Trigger CI and displayed to the user.

The following validation takes place on the Probe:

- The CIT of the CI is compared to that in the CIT model.
- The CI is checked to verify that all key attributes are present (on condition that the **CmdbObjectId** attribute is not defined).
- The CI's attributes are checked to verify that they are all defined in the CIT.

All invalid attributes raise an error, which reports on a specific CI. When the Probe finds invalid data that is related to the CITs, all data that the Probe has collected on that CI is dropped by the Probe and is not sent to the server.

See also: ["Server-Side Data Normalization" on page 749](#).

For details on attributes, see CI Type Attributes in the *Universal CMDB Modeling Guide*.

Content Data Validation

Content that comes out-of-the-box with the Discovery and Integrations Content Pack uses standard libraries. However, user-defined packages might not be compatible with the standard APIs and can

send invalid data to the UCMDB server.

To provide strong validation for data reported to the UCMDB server, UCMDB allows for additional content data validation before the data is sent to the UCMDB server, and indication of any invalid data. To perform content data validation, you can create validation Jython scripts and specify them in the dedicated configuration file, **dataValidationlibs.xml**.

The Content Data Validation module loads and executes sets of Jython scripts defined in the **dataValidationlibs.xml** file. The content data validation Jython scripts should contain the **ValidateData** function, which is the entry point for data validation execution.

For details about how to configure the content data validation Jython scripts, and for some examples, see ["Content Data Validation Jython Scripts" on page 664](#).

To enable or disable Content data validation in UCMDB, see ["How to Enable Content Data Validation" on page 663](#).

Filtering Discovery Results

You can filter results sent by the Probe to the Universal CMDB server. You would probably need to filter irrelevant data regularly during production runs and specifically when you are testing a limited environment.

There are two levels of filtering:

- **Adapter filtering.** The Probe filters the results for a specific adapter and sends to the CMDB only those filtered CIs. You define an adapter filter in the Results Management pane in the **Adapter Configuration** tab. For details, see ["Adapter Configuration Tab" on page 259](#).
- **Global filtering.** Universal Discovery filters the results of all jobs running on a Probe. You define global filters in the **globalFiltering.xml** file. For details, see ["Configure Filtering Using the globalFiltering.xml File" on page 231](#) or ["Configure Filtering in UCMDB" on page 579](#).

The order of filtering is as follows:

1. During a discovery run, the Data Flow Probe first searches for an adapter filter and applies the filter to the results of the run.
2. If there are no adapter filters, Universal Discovery searches for a global filter and applies that filter to the results.
3. If no filters are found, all results are sent to the UCMDB Server.

How to View the Current Status of Discovered CIs

This task describes how to view the current status of discovered CIs.

1. Prerequisites


Verify that the Probe is enabled and is connected to the Universal CMDB server. For details, see ["How to Start a Data Flow Probe" on page 56](#).

2. Access Data Flow Probe status

- a. Go to **Data Flow Management > Data Flow Probe Status**.

- b. Select a connected Probe, and click .

The Progress list displays the current status of every job that ran or is running on the Probe. For details about the information displayed, see ["Data Flow Probe Status Window" on page 149](#).

- c. To view details about a particular job, select the job in the Progress list and click the **View Job progress**  button. For details about the properties displayed, see ["<Job Name> Dialog Box" on page 148](#).

How to Find Discovery Errors

This task describes how to investigate problems that arise during discovery.

Note: For details about severity levels and so on, see ["Managing Problems With Error Reporting" on page 658](#).

1. Prerequisites

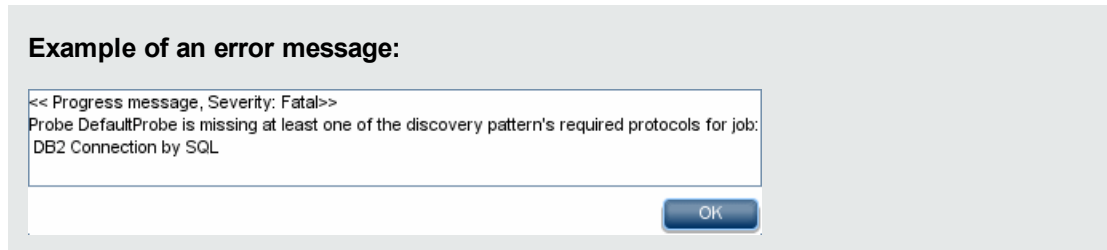
Set up DFM. For details, see ["Data Flow Management Setup" on page 28](#).

2. Select the Module/Job

You can view error messages for one job, one module, or all modules. For details on running a job, see ["How to Run Module/Job-based Discovery" on page 470](#).

3. Locate the Problem CI

Use the Discovery Progress user interface to drill down to the error messages. For details, see ["Discovery Progress Dialog Box" on page 670](#).



How to Manage Discovery Errors

This task describes how to investigate problems that arise during a discovery run.

Note: For details about severity levels and so on, see ["Managing Problems With Error Reporting" on page 658](#).

1. Prerequisites

Set up DFM. For details, see ["Data Flow Management Setup" on page 28](#)

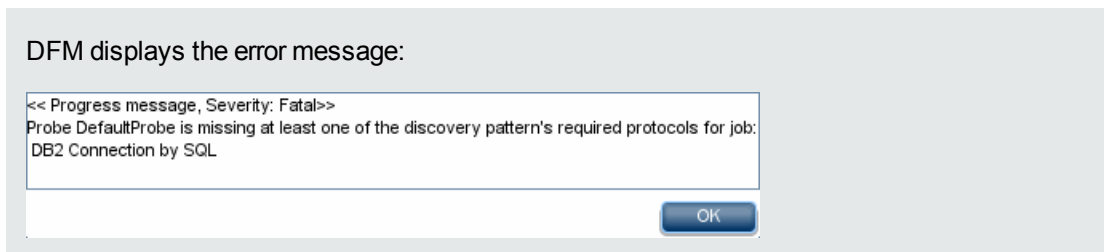
2. Run the discovery job

You can view error messages for one job, one module, or all modules. For details on running a job, see ["How to Run Module/Job-based Discovery" on page 470](#).

3. Locate the problem CI

Use the Discovery Progress pane to drill down to the error messages. For details, see ["Discovery Progress Dialog Box" on page 670](#).

Example:



4. Troubleshoot the problem

- For Fatal errors, you should contact Micro Focus Software Support.
- For other errors, check the CIs. For example, a Trigger CI that does not fall within the Probe's range may show an error.
- For details on setting communication logs, see ["Execution Options Pane" on page 260](#).
- For details on managing problems, see ["Managing Problems With Error Reporting" on page 658](#).

How to Enable Content Data Validation

This task describes how to enable or disable the execution of content data validation.

1. In the **DataFlowProbe.properties** file (located in **c:\hp\UCMDB\DataFlowProbe\conf**), set the **appilog.agent.local.process.result.dataValidation.content** parameter as follows:
 - **true**. Enables content data validation (default)
 - **false**. Disables content data validation
2. Restart the Probe to update the changes.
3. If you are enabling validation, ensure that your content data validation configuration file, **dataValidationlibs.xml**, is defined with the necessary Jython and library scripts. For details, see ["Content Data Validation Jython Scripts" on the next page](#).

For more information about Content Data Validation, see ["Content Data Validation" on page 659](#).

Note: The value given to the **appilog.agent.local.process.result.dataValidation.content** parameter in the **DataFlowProbe.properties** file can be overridden on an adapter level by adding the **"enableContentDataValidation"** parameter to the adapter parameters. If this parameter is absent among the adapter parameters (by default), the value defined in the

DataFlowProbe.properties file is used.

Content Data Validation Jython Scripts

The Content Data Validation Jython scripts are divided into main scripts and library scripts. Each "main" script must have the **ValidateData** function which is the entry point for the execution of data validation. The **ValidateData** function has the following parameters:

- **TaskResults.** Provides the API accessing data objects.
- **Environment.** Provides the API for accessing Environment information, such as the Probe Gateway name, the Probe Gateway IP, and the domain name.

The **dataValidationlibs.xml** file is a configuration file where you define which scripts to execute and which to execute as libraries. The file is divided into sections which logically define the data validation execution.

Example of the dataValidationlibs.xml File

```
<datavalidation parserClassName="com.hp.ucmdb.discovery.  
library.communication.downloader.cfgfiles.  
ContentDataValidationConfigFile">  
    <script name="dataValidator1.py">  
        <library name="validator1.py"/>  
    </script>  
    <script name="dataValidator2.py" cit="Node,Process">  
        <library name="validator2.py"/>  
        <library name="validator3.py"/>  
    </script>  
</datavalidation>
```

where:

- **validator<x>.py** is a library script.

Libraries must be ordered according to their dependency. In this example, **validator3.py** uses **validator2.py**, so **validator3.py** appears after first **validator2.py**.

- The **cit** parameter lists the CITs that the script receives for validation. In this example, the **dataValidator2.py** script receives only **Node** and **Process** CITs for validation.

Handling Errors and Warnings

- **addError/addWarning**. Use this API from the TaskResults parameter to attach error/warning to triggered CIs. Bulk is reported to the UCMDB server.
- **raise ContentDataValidationException**. Use to report an error message if the bulk should be discarded.

Example of API Usage

- **Main Script**

```
#dataValidator1.py

import validator1

def ValidateData(TaskResults, Environment):
    logger.info('probe gateway is :', Environment.
getProbeGatewayID())

    logger.info('probe gateway ip is :', Environment.
getProbeGatewayIP())

    logger.info('probe domain is :', Environment.
getProbeManagerDomain())

objectsForUpdate = TaskResults.getResultObjects()
size = objectsForUpdate.size()
if size > 0:
    for i in range(0, size):
        object = objectsForUpdate.get(i)
        validator1.validate(object, TaskResults)
```

```
        if object.getObjectClass() == 'host':  
            TaskResults.addError(100, 'host CIT is not in class  
model')  
        pass
```

- **Library Script**

```
#validator1.py  
  
from com.hp.ucmdb.discovery.library.results.resultprocess import  
ContentDataValidationException  
  
def validate(object, TaskResults):  
    if object.getAttribute('description') == None:  
        TaskResults.addWarning(100, 'No description set for the object  
of type ' + object.getObjectClass())  
    if object.getAttribute('host_hostkey') == None:  
        // fatal error, all bulk and all previous errors will be removed  
        from bulk  
        // this error will be shown in UI  
        raise ContentDataValidationException, 'Attribute host_hostkey is  
absent'
```


Discovery Progress and Results User Interface

This section includes:



Choose CIs to Add Dialog Box	667
Discovered/Created/Last Updated CIs Dialog Box	668
Discovery Progress Dialog Box	670
Discovery Results Tab/Pane	678
Related CIs Window	680
Show Results for Triggered CI Dialog Box	681

Choose CIs to Add Dialog Box

Enables you to choose CIs to run with selected jobs.

To access	Select Discovery Progress > Drill down to the CI instances, and click the Add CI  button. For more details, see "Discovery Progress Dialog Box" on page 670 .
Relevant tasks	<ul style="list-style-type: none"> • "How to Find Discovery Errors" on page 661 • "How to Manage Discovery Errors" on page 662 • "How to Run Module/Job-based Discovery" on page 470
See also	<ul style="list-style-type: none"> • "Universal Discovery Overview" on page 416 • "Modules/Jobs-based Discovery Overview" on page 467 • "Managing Problems With Error Reporting" on page 658

User interface elements are described below (unlabeled elements are shown in angle brackets>):

UI Element (A–Z)	Description
	<p>Adds the CI to the list of triggers that run with the discovery job.</p> <p>Note: If you choose CIs with an error status, a message is displayed when you add the CI.</p>
Search CIs	<p>Contains filters with which you can limit the number of CIs that appear in the Search Results pane.</p> <ul style="list-style-type: none"> • . Displays the search results. • By Discovery Query. Select a Discovery query to search for those CIs that match the query. • Show only CIs containing. To search for CIs that include a certain text, enter the text here. • Exact match. Select to search for CIs with the exact match of the text label. (By default, you search by entering part of a text. For example, searching for 10 within the IP CIs finds all the IPs that contain 10 in their address. Entering 10 then selecting Exact match finds no results.)
Search Results	<p>Displays a list of triggered CIs answering to the criteria set in the filter. To add the CIs to the list in the triggered CIs pane, select the CIs. You can make multiple selections.</p>



UI Element (A–Z)	Description
	<ul style="list-style-type: none"> • CIT. The CI type of the selected triggered CI. • CI. The label of the triggered CI. • Related Host. The label for the node related to the triggered CI. • Related IPs. The IPs of the related node. • Reported. The time that the CI was reported. <p>Page. The list of CIs is divided into pages. The number in the Page box indicates which page is currently displayed. To view other pages, use the up and down arrows, or type the page number, and press Enter.</p> <p>To determine the number of CIs that appear on a page, right-click the up or down button and choose the required number. The default is 25.</p>

Discovered/Created/Last Updated CIs Dialog Box

The Discovered CIs dialog box enables you to view all CI instances found for a selected query node.












The Created/Last Updated CIs dialog boxes enable you to view all CI instances that were created or updated during the last discovery run.



The Created by <Job> dialog box displays the CI instances created when running a selected job.

To access	<p>These dialog boxes are accessible from various places in the Universal Discovery window, and all display information about discovered CI instances.</p> <ul style="list-style-type: none"> • A job's Dependency Map tab. Right-click a CI, a job or a relationship. For more information, see "Discovery Module/Jobs – Dependency Map Tab" on page 489. • Discovery progress: Drill down to a CI and click Show additional data . • Discovery Results: Select a CI and click View Created/Updated Instances .
Important Information	<p>When viewing discovery results, the CI instances displayed are retrieved from the server when this dialog box opens. The number of CIs may differ from the number of CIs displayed in the Results pane because some created CIs may have been merged or deleted since they were created by the job.</p>
Relevant tasks	<ul style="list-style-type: none"> • "How to Find Discovery Errors" on page 661 • "How to Manage Discovery Errors" on page 662 • "How to Run Module/Job-based Discovery" on page 470

See also	<ul style="list-style-type: none"> • "Universal Discovery Overview" on page 416 • "Modules/Jobs-based Discovery Overview" on page 467 • "Managing Problems With Error Reporting" on page 658
-----------------	---

User interface elements are described below (unlabeled elements are shown in angle brackets>):

UI Element (A-Z)	Description
	Specify the CIT you want displayed in the table. The table also includes the children of the selected CIT.
	Delete from CMDB. Deletes the selected CI from the database.
	Properties. Opens the Configuration Item Properties dialog box for the selected CI.
	Refresh. Refreshes the list of CI instances.
	Set Filter. Filters the CI instances you want to display for the selected discovery. Opens the Filter CI Instances dialog box.
	Clear Filter. Clears the filter definitions you created in the Filter CI Instances dialog box.
	Select Columns. Enables you to select the columns to be displayed. For details, see "Select Columns Dialog Box" in the <i>Universal CMDB Modeling Guide</i> .
	Enables you to set the sort order of the CI instances. For details, see "Sort Column Content Dialog Box" in the <i>Universal CMDB Modeling Guide</i> .
	Find. Displays the Find toolbar.
	Send Mail. Enables you to send the table data in an email.
	<p>Choose the export format for the table data. The available options are:</p> <ul style="list-style-type: none"> • Excel. The table data is formatted as an .xls (Excel) file that can be displayed in a spreadsheet. • PDF. The table data is exported in PDF format. <div style="border-left: 2px solid black; padding-left: 10px; margin-left: 20px;"> <p>Note: When exporting to PDF, select a reasonable number of columns to display to ensure that the report is legible.</p> </div> • CSV. The table data is formatted as a comma-separated values (CSV) text file that can be displayed in a spreadsheet. <div style="border-left: 2px solid black; padding-left: 10px; margin-left: 20px;"> <p>Note: For the CSV formatted table data to display correctly, the</p> </div>

UI Element (A-Z)	Description
	<p>comma (,) must be defined as the list separator. In Windows, to verify or modify the list separator value, open Regional Options from the Control Panel, and on the Numbers tab ensure that the comma is defined as the List Separator value. In Linux, you can specify the list separator in the application that opens the CSV file.</p> <ul style="list-style-type: none"> • XML. The table data is formatted as an XML file that can be opened in a text or XML editor. <p>Tip: To extract HTML code from the report:</p> <ul style="list-style-type: none"> ○ Save the file as HTML ○ Open the file in an HTML editor ○ Copy the relevant table into the target file
 Rows per page	Select the number of rows to be displayed on each page. You can also manually enter value for the number of rows per page.
	Click to navigate through the results page by page or to jump to the first or last page.
<CI Instances>	The CI instances created during the discovery. You can double-click an instance to open the Configuration Item Properties dialog box for that CI.
<CI instances shortcut menu>	For details, see "IT Universe Manager Shortcut Menu" in the <i>Universal CMDB Modeling Guide</i> .

Discovery Progress Dialog Box





This dialog box displays the progress of running discoveries, and enables you to drill down to discovered CI instances.

To access	Use one of the following: <ul style="list-style-type: none"> • In the CI Instances dialog box, right-click a CI instance, click Actions, and select Show Discovery Progress. • Select Data Flow Management > Universal Discovery: <ul style="list-style-type: none"> ○ Zone-based Discovery tab > a node in the tree > Discovery Status pane (on the right) > Progress tab. ○ Discovery Modules/Jobs tab > a node in the tree > Details tab (on the right) > Discovery Progress pane.
------------------	--

Important information	The discovery progress information displayed is the last status known by the UCMDB server for each job Trigger CI within the context selected for discovery.
Relevant tasks	<ul style="list-style-type: none"> • How to Check the Status of Application Discovery (Rediscover a View) in the <i>Universal CMDB Modeling Guide</i>. • "How to Find Discovery Errors" on page 661 • "How to Manage Discovery Errors" on page 662 • "How to Run Module/Job-based Discovery" on page 470
See also	<ul style="list-style-type: none"> • Error Messages Overview in the <i>Universal CMDB Developer Reference Guide</i> • "Universal Discovery Overview" on page 416 • "Modules/Jobs-based Discovery Overview" on page 467 • "Managing Problems With Error Reporting" on page 658




Triggered CIs View - Progress/Status Matrix

Displays the status of triggered CIs through the progress of discovery.

UI Element (A-Z)	Description
	Refresh. Refreshes the matrix.
	<p>Add CI. Opens the Choose CIs to Add dialog box, enabling you to add a newly-discovered CI to the triggered CI list. For details, see "Choose CIs to Add Dialog Box" on page 667.</p> <p>Available: Discovery Modules/Jobs view only, when you select a module/job.</p>
	Rerun Discovery. Enables you to rerun the selected discovery modules/jobs.
	<p>Pause / Resume. Enables you to pause or resume the selected discovery</p> <p>Note:</p> <ul style="list-style-type: none"> • When you pause an active job: <ul style="list-style-type: none"> ◦ triggers that are currently running continue to run until they are finished ◦ all the execution information is retained, including errors • Jobs are paused based on their defined job execution policies. For details, see "Job Execution Policies" on page 36. <p>Available: Discovery Modules/Jobs view only</p>

UI Element (A-Z)	Description
Progress bar	<p>Displays the percentage of new trigger CIs that have completed the discovery process for the set of jobs contained within the focus area that you have selected for discovery since the last time the activity was modified.</p> <p>Note: When you activate discovery, the trigger CIs list are prepared. During this time, discovery progress may not be reflected immediately.</p> <p>Thereafter, discovery progress is automatically refreshed every 30 seconds.</p>

Understanding the Progress/Status Matrix and the Progress Bar

Progress Status	Total			
Pending Probe	Displays the total number of trigger CIs waiting for the Probe to pick them up for execution.	Displays the number of triggered CIs successfully waiting for the Probe to pick them up for execution.	--	--
Reached Probe	Displays the total number of triggered CIs that reached the Probe, and may have started running.	Displays the number of triggered CIs that successfully reached the Probe, and may have started running.	Displays the number of triggered CIs that successfully reached the Probe and have started running, but have warnings.	--
Completed	Displays the total number of triggered CIs that completed running (successfully or unsuccessfully).	Displays the number of triggered CIs that successfully completed running.	Displays the number of triggered CIs that successfully completed running, but have warnings.	Displays the number of triggered CIs that failed to complete running, did not reach the Probe, or were not picked up by the Probe for execution.
Total	Displays the total number of triggered CIs.	Displays the total number of successful triggered CIs.	Displays the total number of triggered CIs that were successful, but had warnings	Displays the total number of failed triggered CIs.

Note: When discovery is kicked off by schedule, as opposed to manually being started, trigger

CI's that have completed at least once do not go back into **Pending Probe** and **Reached Probe** status, and are therefore not reflected in the **Pending Probe** and **Reached Probe** rows of the Progress/Status Matrix. However, when consecutive runs of the trigger CI's complete, their statuses **are** reflected in the appropriate status column of the **Completed** row of the matrix.







Similarly, since the progress bar displays the percentage of completed trigger CI's, the progress bar does not change unless new trigger CI's are dispatched or an existing trigger CI is manually rerun.



CI Count View

Clicking a link in the Triggered CI's view enables you to view the number of triggered CI's for each discovery job that have reached the selected stage of discovery and with the selected status.

Important Information	In the Discovery Modules/Jobs view, the CI Count job is displayed only when standing on a module which contains 2 or more jobs. If there is only one job in the module, clicking the triggered CI displays the CI Instances view.
------------------------------	---







User interface elements are described below (unlabeled elements are shown in angle brackets>):








UI Element (A-Z)	Description
	Up one level. Enables you to go back to the Triggered CI's view.
	Show triggered CI's. Enables you to drill down to individual triggered CI's.
	Refresh. Refreshes the table.
	<p>Remove CI. Deletes the selected CI. The CI is deleted from the specific job or activity job.</p> <p>Available: Discovery Modules/Jobs view only, when you select a module category and select a job.</p>
	Rerun Discovery. Enables you to rerun the selected discovery jobs. The execution complies to the defined execution policy for the relevant discovery jobs.
	<p>Pause / Resume. Enables you to pause/resume a selected job.</p> <p>Note:</p> <ul style="list-style-type: none"> • When you pause an active job: <ul style="list-style-type: none"> ◦ triggers that are currently running continue to run until they are finished ◦ all the execution information is retained, including errors

UI Element (A-Z)	Description
	<ul style="list-style-type: none"> Jobs are paused based on their defined job execution policies. For details, see "Job Execution Policies" on page 36. <p>Available: Discovery Modules/Jobs view only</p>
CI Count	Displays the number of triggered CI per job that have reached the selected stage of discovery and with the selected status.
Job Name	Displays the list of jobs that have reached the selected stage of discovery and with the selected status.
Show errors /Show warnings	<p>Displays the Triggered CIs > Completed with Errors / Completed Successfully with Warnings view, listing all error/warning messages, their related jobs, severity, and count information.</p> <p>The Show errors option is available for links in the Failures  column of the Triggered CIs view only.</p> <p>The Show warnings option is available for links in the Failures  column of the Triggered CIs view only.</p> <p>Right-clicking an error message from the Completed with Errors view or a warning message from the Completed Successfully with Warnings view enables you to do the following:</p> <ul style="list-style-type: none"> Remove CI Rerun Discovery Show All <Error Message> Issues. Displays all similar discovery issues related to a specific job, thus allowing you to view all CIs impacted by this particular discovery issue. <p>Available:</p> <ul style="list-style-type: none"> Available only when accessing the Discovery Progress dialog box from IT Universe Manager. Available for all users with the View Discovery Status and Error and Show Discovery Progress permissions.

CI Instances View

Clicking a job in the **CI Count** view displays the triggered CIs for that discovery job.

UI Element (A-Z)	Description
	Up one level. Enables you to move up a level of information.
	Refresh. Refreshes the list of triggered CIs.
	<p>Add CI. Opens the Choose CIs to Add dialog box, enabling you to add a newly-discovered CI to the triggered CI list. For details, see "Choose CIs to Add Dialog Box" on page 667.</p> <p>Available: Discovery Modules/Jobs view only</p>
	<p>Remove CI. Deletes the selected CI. The CI is deleted from the specific job or activity job.</p> <p>Available: Discovery Modules/Jobs view only</p>
	<p>Filter CIs. Enables you to filter the displayed CIs.</p> <ul style="list-style-type: none"> • By Status. Available only when viewing the CIs of a particular discovery job in the Discovery Module/Jobs view. <ul style="list-style-type: none"> ◦ All. Displays all the Trigger CIs. ◦ Waiting for Probe. Displays the Trigger CIs that are ready to be dispatched and are waiting for the Probe to retrieve them. ◦ In Progress. Displays the Trigger CIs that are active and are running on the Probe. ◦ In progress (being removed). Displays the Trigger CIs that are being removed from the Trigger CIs list. ◦ Success, Failed, Warning. Displays only those CIs that have the selected status. • By Probe. Displays only the CIs triggered by a selected probe/cluster. Click to open the Select Probes dialog box. • By Dispatch Type. Displays a list of CIs according to one of the following options: <ul style="list-style-type: none"> ◦ All. Displays both CIs that are used to manually activate the job and Discovery TQL queries that are used to automatically activate the job. ◦ Manually Added. Displays the CIs that are used to manually activate the job. ◦ By Discovery Query. Displays the CIs that are used to automatically activate the job. • Reset. Click to remove any filters.
	Show Message. When there are warnings/errors, opens a message box containing all the warning/error messages for the triggered CI.

UI Element (A-Z)	Description
	Show additional data. Opens the Discovered CIs dialog box, enabling you to view additional information about the CI. For details, see "Discovered/Created/Last Updated CIs Dialog Box" on page 668 .
	<p>Show results for triggered CI. An ad hoc request is sent to the Data Flow Probe and retrieves the latest results of the job (CIT name and number of discovered CIs) that is running on a specific trigger CI.</p> <p>This ad hoc request does not run the job, but brings the results of the previous job run that are stored in the Probe's database. If the job has not yet run for this trigger CI, a message is displayed. See "Show Results for Triggered CI Dialog Box" on page 681.</p> <p>If no communication log exists on the Probe, a message is displayed. You can choose to always create communication logs. For details, see "Adapter Configuration Tab" on page 259.</p>
	Rerun Discovery. Enables you to rerun the discovery on the selected CI.
 / 	<p>Pause / Resume. Enables you to pause/resume a selected discovery.</p> <p>Note:</p> <ul style="list-style-type: none"> • When you pause an active job: <ul style="list-style-type: none"> ◦ triggers that are currently running continue to run until they are finished ◦ all the execution information is retained, including errors • Jobs are paused based on their defined job execution policies. For details, see "Job Execution Policies" on page 36. <p>Available: Discovery Modules/Jobs view only</p>
Look for 	To search for a specific Probe, related host, or related IP, enter part of its name in the box and click the  button.
<CI Instances table>	Displays all the CI instances discovered by selected job. You can drill down into any CI instance. If triggered CIs failed, or succeeded with warnings, you can drill down further to better understand the cause for the warning or failure.
<right-click menu>	<p>In addition to some of the functionality described above, right-clicking a CI enables you to do the following:</p> <ul style="list-style-type: none"> • Debug. Enables you to debug a CI. You can: <ul style="list-style-type: none"> ◦ View Communication Log. View the communication log. ◦ Go to Adapter. Go directly to the job's adapter

UI Element (A-Z)	Description
	<ul style="list-style-type: none"> ◦ Go to Job. Go directly to the job's details (Discovery Modules/Jobs view only) ◦ Edit Script. Select a script to edit ◦ Rerun discovery <ul style="list-style-type: none"> • Enable Communication Log. Creates a log file for this session. The log file contains information about the connection between the Probe and a remote machine. <p>Note: To capture results about the connection, see the Enable Communication Log And Record Results option on this menu.</p> • Enable Communication Log And Record Results. Creates a log file for this session. The log file contains information about the connection between the Probe and a remote machine. Additionally, it enables capturing the discovered results; these discovered results may help in investigating various discovery problems. • Enable Scanner Debug Log. Used for most scanner debugging purposes. • Enable Scanner Trace Log. Used for more comprehensive scanner debugging purposes. <p>Note: Communication log files are created on the Probe Manager under the C:\hp\UCMDB\DataFlowProbe\runtime\communicationLog folder. For details on how the communication logs work, see Record DFM Code in the <i>Universal CMDB Developer Reference Guide</i>.</p> • Download Scanner Log. Saves the debug or trace log to a specified location. <p>If a log for the selected CI is unavailable, enable the debug or trace log using the Rerun Discovery menu option.</p> • Run from step. <p>Enables you to manually run the job on the selected CI from a particular step in the job's workflow. This is useful if you do not want to rerun the whole discovery job on the CI, but only a part of it.</p> <p>Note:</p> <ul style="list-style-type: none"> ◦ The workflow steps are defined in the job's adapter file. You can view or edit the workflow in the Adapter Definition tab for the relevant adapter. For details, see "Adapter Definition Tab" on page 253. ◦ You cannot run the job from particular step if the status of the CI is Waiting for probe or In Progress.





UI Element (A-Z)	Description
	<p>Available: In the Discovery Modules/Jobs view; For CIs that trigger workflow-based jobs</p> <ul style="list-style-type: none"> • Reprocess Scan File. Reprocesses the scan files of the selected CI. <p>Available: In the Discovery Modules/Jobs view; For CIs that trigger workflow-based jobs</p>

Discovery Results Tab/Pane

This tab/pane displays the discovery results from discovery job runs or from discovery activities that ran in Management Zones.

To access	<p>Select Data Flow Management > Universal Discovery:</p> <ul style="list-style-type: none"> • Zone-based Discovery tab > a node in the tree > Discovery Status pane (on the right) > Results tab. • Discovery Modules/Jobs tab > a node in the tree > Details tab (on the right) > Discovery Results pane.
Important Information	<p>UCMDB includes a purging mechanism for managing old discovery result statistics. This mechanism enables faster display of discovery result statuses. That is, the old result records are merged and are therefore still available for the user. This feature is controlled by two system parameters:</p> <ul style="list-style-type: none"> • appilog.collectors.ResetDiscoveryStatisticsIntervalHours.name=Reset Discovery Statistics Interval by Hours. This property defines the interval of merging discovery results (the interval for running the purging mechanism). • appilog.collectors.DiscoveryStatisticsArchiveDays.name=Discovery results statistics archive period. This property defines the number of days after which discovery results are archived (the number of days after which the statistics are considered old).
Relevant tasks	<ul style="list-style-type: none"> • "How to Find Discovery Errors" on page 661 • "How to Manage Discovery Errors" on page 662 • "How to Run Module/Job-based Discovery" on page 470
See also	<ul style="list-style-type: none"> • "Universal Discovery Overview" on page 416 • "Modules/Jobs-based Discovery Overview" on page 467 • "Managing Problems With Error Reporting" on page 658

User interface elements are described below (unlabeled elements are shown in angle brackets):

UI Element (A-Z)	Description				
	<p>Refresh. Retrieves the latest discovery results from the server (job results are not automatically updated in the Results pane).</p>				
	<p>View Instances. Displays all new and updated CIs. Select a CIT and click:</p> <ul style="list-style-type: none"> • View Created Instances to view CIs created during the discovery • View Updated Instance to view CIs updated during the discovery <p>Note: When you double-click a row, created CI instances are displayed.</p> <p>Available: When the discovery results include created or updated instances.</p>				
	<p>Select the time range or Probe for which to display discovery results and statistics.</p> <ul style="list-style-type: none"> • By Time Range: <ul style="list-style-type: none"> ◦ All. Displays results for all job runs. ◦ From Now/Last Minute/Last Hour/Last Day/Last Week. Choose a period of time for which to display results. ◦ Custom Range. Opens the Change Timeframe dialog box where you can enter the date or choose a From and To date and time from the calendar. Click Now to enter the current date and time. Click Last Day to enter the current date and time in the To box and yesterday's date and time in the From box. Click OK to save the changes. • By Probe: To view results by Probe, select to open the Choose Probe dialog box. Selecting All Data Flow Probes displays the results for all of the Data Flow Probes. 				
	<p>Show all declared CI Types. By default, only discovered CITs are listed in the table; the Discovered CIs column includes CITs if the number of CIs found is greater than zero. Click the button to display every CI that can be discovered by the job, even if the Discovered CIs value is zero:</p> <div data-bbox="386 1482 927 1692" style="border: 1px solid gray; padding: 5px;"> <p>Statistics Results</p> <p>Filter: Time Range[All] Last Updated: 09/21/2009 02:54:23</p> <table border="1"> <thead> <tr> <th>CIT</th> <th>Discovered CIs</th> </tr> </thead> <tbody> <tr> <td>Database</td> <td>0</td> </tr> </tbody> </table> </div>	CIT	Discovered CIs	Database	0
CIT	Discovered CIs				
Database	0				
<p><Results grid></p>	<p>Displays the discovery results and statistics.</p> <ul style="list-style-type: none"> • CIT. The name of the discovered CIT. <p>You can configure discovery so that any object reported by the job and whose CIT is</p>				

UI Element (A–Z)	Description
	<p>not defined in the adapter's discovered CITs list is marked in red. Objects include those added by the Probe result mechanism.</p> <p>To set this parameter:</p> <ol style="list-style-type: none"> Select Administration > Infrastructure Settings Manager. Select the General Settings category. Locate the Enable statistics results validation according to adapter parameter. Change the value to True. <ul style="list-style-type: none"> Created. The number of CIT instances created in the period selected or for the selected Probe. Deleted. The number of CIT instances deleted in the period selected or for the selected Probe Discovered CIs. The number of CIs that were discovered for each CI type. Total. The total number of CIs in each column. Updated. The number of CIT instances that were updated in the period selected.
Filter	The time range set with the Set Time Range button.
Last updated	The date and time that the Results grid was last updated.

Related CIs Window

Enables you to view, in map format, the CIs that are related to a selected CI.

To access	In the Discovered CIs dialog box, right-click a CIT and select Get Related CIs .
Important Information	Related CIs are CIs that are the parent, child, or sibling of an existing CI.
Relevant tasks	<ul style="list-style-type: none"> "How to Find Discovery Errors" on page 661 "How to Manage Discovery Errors" on page 662 "How to Run Module/Job-based Discovery" on page 470
See also	<ul style="list-style-type: none"> "Universal Discovery Overview" on page 416

	<ul style="list-style-type: none"> • "Modules/Jobs-based Discovery Overview" on page 467 • "Managing Problems With Error Reporting" on page 658
--	---

User interface elements are described below (unlabeled elements are shown in angle brackets):



UI Element (A-Z)	Description
<right-click menu>	For details, see "Shortcut Menu" in the <i>Universal CMDB Modeling Guide</i> .
<menu>	For details, see "Toolbar Options" in the <i>Universal CMDB Modeling Guide</i> .
<Topology Map>	For details, see "Topology Map Overview" in the <i>Universal CMDB Modeling Guide</i> .

Show Results for Triggered CI Dialog Box

Enables you to view the results of running an ad hoc request to the Probe. Discovery acquires the results by running the job on a selected Trigger CI. In the case of an error, a message is displayed.

To access	Select Discovery Progress > Drill down to the CI Instances, right-click a CI, and select Show Results for Triggered CI .
Relevant tasks	<ul style="list-style-type: none"> • "How to Find Discovery Errors" on page 661 • "How to Manage Discovery Errors" on page 662 • "How to Run Module/Job-based Discovery" on page 470
See also	<ul style="list-style-type: none"> • "Universal Discovery Overview" on page 416 • "Modules/Jobs-based Discovery Overview" on page 467 • "Managing Problems With Error Reporting" on page 658

User interface elements are described below:

UI Element (A-Z)	Description
	Select a CIT and click to display additional information in the Show Results for Triggered CI dialog box.
	Click to open a topology map showing a result map for the Triggered CI. Right-click a CIT to view its properties.

Chapter 18: Software Library

This chapter includes:

Software Library Overview	682
Software Library User Interface	682

Software Library Overview

The Software Library Viewer enables you to view the contents of Software Application Index (SAI) files that are contained in the UCMDB software library. Additionally, you can export, import, and also deploy SAI files to the Data Flow Probe.

Software Library User Interface

This chapter includes:









SAI Files Pane	682
Software Library Window	684
Advanced Search Dialog Box	689


SAI Files Pane

This pane enables you to view the all of the SAI files that are contained in UCMDB.

To access	Data Flow Management > Software Library
Important information	<p>Highlight an SAI file and view related information about that file in the Applications pane and the Details pane.</p> <p>Tip: Highlight multiple SAI files to see related information about all the files in the Details pane.</p> <p>Note: By default, the last SAI file that was used by the user is displayed, or the default global SAI file is displayed. To set a default SAI file, update the parameter in Infrastructure Settings Manager Page in the <i>Universal CMDB Administration</i></p>






	<i>Guide.</i>
Relevant tasks	"How to Teach Applications Using Express Teaching Wizard" on page 692
See also	"Express Teaching Overview" on page 691

UI Element	Description
	<p>New SAI File. Enables you to perform the following:</p> <ul style="list-style-type: none"> • New SAI file. Opens the New SAI dialog box enabling you to create a new user SAI file. <p>Note: Newly-created files take a few minutes to create before you can teach to the file.</p>
	<p>Delete. Deletes the selected User SAI file.</p>
	<p>Export. Exports the selected SAI file.</p>
	<p>Import. Enables you to select a method to import SAI file information to the UCMDB server.</p> <ul style="list-style-type: none"> • Import SAI file. Opens the Import SAI dialog box, enabling you to import a User SAI file or an archive (.zip) file to UCMDB. In the dialog box, ensure that you click the file type drop-down button to select the correct file type. <p>Note: User SAI files on the Data Flow Probe are overwritten. This action cannot be undone.</p> <ul style="list-style-type: none"> • Import SAI from CP. Opens the Import SAI from CP dialog box, enabling you to import the master SAI files only that are contained in a Content Pack Update archive file.
	<p>Advanced Search.</p>
	<p>Refresh. Refreshes the information that is displayed in the pane.</p> <p>Note: Perform this after you import master SAI files from a Content Pack Update to UCMDB.</p>
	<p>Deploy. Deploys the selected User SAI file to a Data Flow Probe from UCMDB.</p>
	<p>Opens the Express Teaching wizard, enabling you to teach applications to Universal Discovery. For more information, see "Express Teaching Overview" on page 691.</p>

UI Element	Description
	<p>Available when: A user SAI file is selected.</p> <p>Not available when: Multiple user SAI files are selected.</p> <p>Note: The user SAI file that is selected is the file that is used when using Express Teaching.</p>
	Opens the Software Recognition Configuration wizard. For more information, see " XML Enricher: Software Recognition Configuration Dialog Box " on page 650.

Software Library Window









This window enables you to view the contents of the SAI files that are contained in the UCMDDB software library, including details about publishers and applications.


To access	Select Data Flow Management > Software Library .
Important information	<ul style="list-style-type: none"> Previously-selected SAI files are selected by default. Otherwise, the first SAI file that is displayed is selected. To view SAI file details and statistics for multiple SAI files, select at least two SAI files in the SAI pane. The following iconography appears in multiple panes: <ul style="list-style-type: none">  Indicates a Master SAI file.  Indicates a User SAI file.  Indicates a publisher.  Indicates an application.  Indicates a User SAI file is being created and will be ready in a few minutes. While this icon is displayed, Express Teaching is disabled for this file.
Relevant tasks	"How to Teach Applications Using Express Teaching Wizard" on page 692
See also	"Express Teaching Overview" on page 691

SAI Pane

The SAI pane displays the list of SAI files that are contained in UCMDDB.

User interface elements are described below:

UI Element	Description
	<p>New SAI File. Opens the New SAI dialog box, enabling you to create a new user SAI file.</p> <p>Note:</p> <ul style="list-style-type: none"> • Newly-created files take a few minutes to create before you can teach to the file. • You do not need to type in a file type suffix. • Valid characters are: a-z, A-Z, 0-9, blank space, underline and hyphen.
	<p>Delete. Deletes the selected user SAI file.</p>
	<p>Export. Exports the selected SAI file.</p>
	<p>Import. Opens an Import SAI dialog box, enabling you to import SAI file information to the UCMDB server.</p> <ul style="list-style-type: none"> • Import SAI file. Opens the Import SAI dialog box, enabling you to import a User SAI file or an archive (.zip) file to UCMDB. In the dialog box, ensure that you click the file type drop-down button to select the correct file type. <p>Note: User SAI files on the Data Flow Probe are overwritten if the files have the same file names. This action cannot be undone.</p> <ul style="list-style-type: none"> • Import SAI from CP. Opens the Import SAI from CP dialog box, enabling you to import the master SAI files only that are contained in a Content Pack Update archive file.
	<p>Advanced Search. Opens the Advanced Search dialog box, enabling you to find detailed information that is contained in SAI files. For more information, see "Advanced Search Dialog Box" on page 689.</p>
	<p>Refresh. Refreshes the information that is displayed in the pane.</p> <p>Note: Perform this after you import SAI files from a Content Pack Update to UCMDB.</p>
	<p>Deploy. Deploys the selected user SAI file from UCMDB to Data Flow Probe servers.</p> <p>Available when: User SAI files that contain newly-taught applications which have not been deployed to the Data Flow Probe.</p>
	<p>Opens the Express Teaching Wizard, enabling you to teach applications to Universal Discovery. For more information, see "Express Teaching Overview" on page 691.</p> <p>Available when: A user SAI file is selected and ready for teaching.</p> <p>Not available when: Multiple SAI files are selected.</p>




UI Element	Description
	<p>Note: The user SAI file that is selected is the file that is used when using Express Teaching.</p>
	<p>Opens the Software Recognition Configuration Wizard, enabling you to set options for scan file recognition. For more information, see "XML Enricher: Software Recognition Configuration Dialog Box" on page 650.</p>

Publishers and Applications Pane

The Publishers and Applications pane displays publisher and application information that are contained in the selected SAI files.

Important information	Available when: Only one SAI file is selected in the SAI pane.
------------------------------	---

User interface elements are described below:

UI Element	Description
	<p>Refresh. Refreshes the information that is displayed in the pane.</p> <p>Note: Perform this after you import master SAI files from a Content Pack update to UCMDB.</p>
	<p>Expands the contents of the directory tree enabling you to view the applications.</p>
	<p>Collapses the contents of the directory tree and hides the applications.</p>

Details Pane

The Details pane displays detailed information about the selected SAI file, the selected publisher, and the selected application.

Important information	<ul style="list-style-type: none"> • Contains multiple sub-panes and contains multiple tabs depending on your selection in the Publishers and Applications pane. • To see the SAI file details and statistics of an SAI file, select an SAI file or SAI files in the SAI Files pane. Ensure the root of the Publishers and Applications pane is selected. • To see details of a publisher, select an SAI file in the SAI pane and also select a publisher in the Publishers and Applications pane.
------------------------------	--

	<ul style="list-style-type: none"> • To see details of an application, select an SAI file in the SAI Files pane and also select an application in the Publishers and Applications pane. • Some tabs are displayed only when an SAI file is selected in the SAI pane and the root of the Publishers and Applications pane is selected.
--	---


User interface elements are described below:



UI Element	Description
Details Tab	<p>Displays sub-panes that show detailed information about the selected SAI file.</p> <p>Note: The information contained in these tabs are displayed in tabular form when multiple SAI files are selected in the SAI pane.</p> <p>The following sub-panes are displayed:</p> <ul style="list-style-type: none"> • SAI File Details. Displays detailed information about a selected SAI or application. <ul style="list-style-type: none"> ◦ Name. Name of the SAI file. ◦ Description. Description of the SAI file. ◦ ID. ID number of the SAI file. ◦ Date. For master SAI files, the date the SAI file was released. For user SAI files, the creation date. ◦ Type. Type of the SAI file. <ul style="list-style-type: none"> • Possible values: Master or User. ◦ In Use. Specifies whether the SAI file is used by the XML Enricher to enrich scan files. • Statistics. Displays statistics about the selected SAI file or SAI files that are selected in the SAI pane. <ul style="list-style-type: none"> ◦ Publishers. Number of publishers. ◦ Applications. Number of applications. ◦ Versions. Number of versions. ◦ Releases. Number of releases. ◦ Package Rules. Number of package rules. ◦ Version Data Rules. Number of version data rules.
Application Types Tab	Displays application types that help you to identify the different types of software that are contained in the selected SAI file.
Operating Systems Tab	Displays the names of the operating systems that are contained in the selected SAI file.
Languages	Displays the languages that are contained in the selected SAI file.

UI Element	Description
Tab	
File Based Tab	<p>Displays sub-panes that show detailed information about applications and their release and version information.</p> <p>Available when:An application is selected in the Publishers and Applications pane.</p> <p>The following sub-panes are displayed:</p> <ul style="list-style-type: none"> • Application Details Pane. Displays detailed information about the application. • Release and Versions Pane. Displays release and version details. <ul style="list-style-type: none"> ◦ Releases. Displays the releases that are associated with the application. ◦ Versions. Displays any versions that are associated with the selected release in the Releases sub-pane. ◦ Licensing Releases. Displays the releases that the selected application licenses. For example, a Microsoft Office suite. ◦ Licensed Releases. Displays any releases that are licensed by the selected application. For example, Microsoft Word.
Rule Based Tab	<p>Displays sub-panes that show package rule and version rule information about the selected SAI file.</p> <p>Available when:An application is selected in the Publishers and Applications pane.</p> <p>The following sub-panes are displayed:</p> <p>Package Rules Pane and Version Data Rules Pane.</p> <ul style="list-style-type: none"> • Commercial. Commercial or license type of the package or application. • Language. Language of the package or application. • Package Name. Name of the package or application used to recognize the application. • Package Type. File type of the application package. • Operating System. Operating system on which the package or application runs. • Release Match. Scan file data field that contains the release information, and also the regular expression used to extract the release information. • Version Match. Scan file data field that contains the version information, and also the regular expression used to extract the version information. <p>Note: All version data rules are for Windows only.</p>

Advanced Search Dialog Box

This dialog box enables you to find information contained in the SAI files that are in the UCMDB software library.

To access	Select Data Flow Management > Software Library , and click  .
Relevant tasks	"How to Import SAIs to the Data Flow Probe" on page 569
See also	"Software Library Window" on page 684

UI Element	Description
Search for words	Enter an alphanumeric string to search. Note: <ul style="list-style-type: none"> • Auto-complete is enabled. • Limited approximate string matching is enabled. For example, "microsoft" is returned when you type "micro" or "soft". However, "microsoft" is not returned when you type "microsoftx" or "xmicrosoft" Tip: Click the drop-down menu to see previous search strings.
	Executes the search. Available when: All required search criteria have been met.
Scope	Specifies the SAI files that you want to include in your search. Default: The selected SAI file in the SAI pane is pre-populated. Use the browse button to select or deselect SAI files.
	Opens the Search Scope dialog box, enabling you to select the SAI files that you want to search.
Search in	Select at least one of the following information items to include in your search: <ul style="list-style-type: none"> • Publisher Name • Application Name • Release Name • Version Name • File Name
Limit to	Specifies the maximum number of results for your search.

UI Element	Description
results	Default: Unlimited
Go to	Displays the location of the search result in the Publishers and Applications pane of the Software Library. Available when: A search result row is selected.

Chapter 19: Express Teaching

This chapter includes:

Express Teaching Overview	691
Unrecognized Files	691
How to Teach Applications Using Express Teaching Wizard	692
How to Deploy User SAI Files	694
How to Clean Up Unrecognized Files	694
How to Clean Up Aged Unrecognized Files	695
How to Send a Publisher File to Micro Focus	696
Express Teaching User Interface	697

Express Teaching Overview

Express Teaching is a wizard that improves application recognition by increasing the amount of applications that are recognized on discovery nodes. Express Teaching is a web-based, lighter alternative to teaching applications than SAI Editor or Analysis Workbench.

Note: For Windows only.

During the teaching process, information contained in unrecognized files is matched to information contained in Software Application Index (SAI) files. When the wizard is completed and you are finished with all of your teaching updates, then you deploy your updates to the Data Flow Probes.

To teach applications using the Express Teaching wizard, see ["How to Teach Applications Using Express Teaching Wizard" on the next page](#).

Unrecognized Files

Unrecognized files are files that are stored on remote machines and not recognized by Universal Discovery. The information about these files are usually imported and stored by the Data Flow Probe. For more information on how to configure the XML Enricher to import unrecognized files, see ["XML Enricher: Software Recognition Configuration Dialog Box" on page 650](#).

Periodically, you may want to remove unrecognized files for the following reasons:

- Large amounts of unrecognized files are causing performance problems
- Large amounts of unrecognized files are consuming large amounts of hard drive space
- You have deleted a Node CI instance for a node, and you want to remove unrecognized files that are associated with the deleted node

You can remove all unrecognized files, or you can remove unrecognized files that reach an aging threshold.

To clean up all unrecognized files, see ["How to Clean Up Unrecognized Files" on page 694](#).

To clean up aged unrecognized files, see ["How to Clean Up Aged Unrecognized Files" on page 695](#).

How to Teach Applications Using Express Teaching Wizard

This task describes how to teach applications to Universal Discovery using the Express Teaching wizard.

1. Prerequisites

Ensure that the Data Flow Probe is installed and running.

2. Configure the XML Enricher Service

Ensure that the XML Enricher service that is running on the Data Flow Probe is configured to import unrecognized files.

To do this, In the Software Recognition Configuration Dialog Box, select **import unrecognized files**. For more information, see ["XML Enricher: Software Recognition Configuration Dialog Box" on page 650](#).

3. Run Inventory Discovery

For more information about setting up inventory discovery, see the *Universal CMDB Discovery and Integrations Content Guide*.

4. Teach applications

Start the Express Teaching Wizard to teach applications to Universal Discovery. Teaching applications ensure better application recognition during inventory discovery. To do this, see ["Express Teaching Wizard" on page 697](#).

5. Deploy the SAI file

Tip: If you plan to teach more than one application, skip this step. When you are finished teaching applications, perform this step.

After teaching applications, deploy the SAI delta file to the Data Flow Probe. To do this, see ["How to Deploy User SAI Files" on the next page](#).

6. Enrich scan files- Optional

You can reprocess scan files that are currently on the Data Flow Probe. When you do this, scan files that were created from the last Inventory Discovery job are enriched with information about the applications that you taught in step 4. Additionally, the unrecognized files that were associated with those taught applications are immediately removed from the unrecognized files list in Express Teaching Wizard.

To reprocess scan files, see ["Processing Scan Files" on page 519](#).

Alternatively, you can wait to see results until the next Inventory Discovery job occurs.

7. Results

- The files that you used to teach applications should not appear in ["Select Files Page" on page 699](#).
- Verify that the taught application has been recognized and reported to UCMDb. To do this, go to **Modeling > CI Type Manager**. Under **NodeElement**, right-click the **Installed Software** CIT and select **Show CIT Instances**.
- If teaching did not yield the expected results, use the SAI Editor inventory tool. For more information, see ["Inventory Tools" on page 534](#).

How to Deploy User SAI Files


This task describes how to deploy User SAI files to Data Flow Probes after using the Express Teaching wizard.

1. Prerequisites

You used the Express Teaching wizard and want to deploy one or more User SAI files to Data Flow Probes.

Note: The XML Enricher service on the Data Flow Probe may be restarted after you perform this task.

2. Select a file

- a. In Data Flow Management, go to the Software Library module and click . The User SAI dialog box opens.
- b. From the list, select the User SAI files you want to deploy to the Data Flow Probe. Alternatively, to deploy all User SAI files that have been created since the last deploy operation, select **Deploy all User SAI files**.

3. Deploy the SAI file

Click **Deploy** to deploy the selected User SAI files to the Data Flow Probes.

4. Results

Verify the deployment is successful by viewing the User SAI file at the following location on the Data Flow Probe machine:

```
c:\hp\UCMDB\DataFlowProbe\runtime\probeManager\discoverySaiResources\saiRuntime
```

How to Clean Up Unrecognized Files

This task describes how to remove unrecognized files from the Data Flow Probe.

1. Clear all the data from the Data Flow Probe

Run the **clearprobedata.bat** script. For details, see ["How to Clear Data Flow Probe Data" on page 73](#).

2. Results

All unrecognized files are deleted from the Data Flow Probe.

How to Clean Up Aged Unrecognized Files

This task describes how to configure the Data Flow Probe to automatically remove unrecognized files that have not been used to recognize applications and are no longer needed to store.

1. Locate the file

Locate the **DataFlowProbe.properties** file in the following folder:

C:\hp\UCMDB\DataFlowProbe\conf

2. Set the aging threshold

Find the **UnrecognizedFileExpirationTime** parameter and change the value to the number of days that the Data Flow Probe waits before deleting unrecognized files.

Note:

- **Default:** 30 days
- The value should be longer than the longest interval used for inventory scanning.

3. Restart the Data Flow Probe service

Restart the Data Flow Probe. To do this, see ["How to Start a Data Flow Probe" on page 56](#).

4. Results

Unrecognized files are deleted.

How to Send a Publisher File to Micro Focus

This task describes how to export the **vendors_mapping.properties** file and send it to Micro Focus Support. This file contains normalization information about publishers/vendors. You should perform this task periodically and after you use the Express Teaching wizard.

This task includes the following steps:

1. ["Prerequisites " below](#)
2. ["Locate the file" below](#)
3. ["Export the file" below](#)
4. ["Send the file to Micro Focus" below](#)
5. ["Result" below](#)


1. Prerequisites

You have recently used the Express Teaching wizard.

2. Locate the file

In **Adapter Management** expand **Inventory Discovery**, expand **Configuration Files**, and then click **vendors_mapping.properties**. The file contents are displayed in the right pane.

3. Export the file

- a. Click  to open the file in an external editor. For example, Notepad.
- b. In the **Full Path** field, type or browse an external editor executable file.
- c. Save the file as a text file.

4. Send the file to Micro Focus

Open an Support ticket and send the file.

5. Result

The file is included in the next Discovery and Integration Content Pack. For more information, see the *Universal CMDB Discovery and Integrations Content Guide*.


Express Teaching User Interface

This chapter includes:

Express Teaching Wizard 697

Express Teaching Wizard

This wizard enables you to teach applications to Universal Discovery using information from unrecognized files.

To access	Select Data Flow Management > Software Library , and click  in the SAI Files pane.
Important information	<ul style="list-style-type: none"> • Ensure XML Enricher is configured to import unrecognized files. For more information, see "XML Enricher: Software Recognition Configuration Dialog Box" on page 650. • Ensure that a recent Inventory Discovery job has run. For more information, see "Inventory Discovery Activity in the <i>HPE UCMBD Discovery and Integrations Content Guide - Discovery Activities</i>." • Ensure the Data Flow Probe is connected and running.
Relevant tasks	"How to Teach Applications Using Express Teaching Wizard" on page 692
Wizard map	"Select a Probe Page" > "Select an Application Page" > "Select Files Page" > "Select Application Details Page" > "Review Data Page" > "Summary Page"
See also	"Express Teaching Overview" on page 691

Select a Probe Page

This page enables you to select a Data Flow Probe to perform application teaching.

Important information	<ul style="list-style-type: none"> • If there are multiple domains in your environment, click the domain name to expand the list of Data Flow Probes running in that domain.
------------------------------	---

	<ul style="list-style-type: none"> If you receive the "no unrecognized files" message, review the Important information section of "Express Teaching Wizard" on the previous page. Ensure you select the Data Flow Probe that corresponds to the IP range for the application.
Wizard map	Select a Probe Page > "Select an Application Page" > "Select Files Page" > "Select Application Details Page" > "Review Data Page" > "Summary Page"
Relevant tasks	"How to Teach Applications Using Express Teaching Wizard" on page 692
See also	"Express Teaching Overview" on page 691

User interface elements are described as follows:

UI Element	Description
Domains and Probes	Select a Data Flow Probe. Note: For more information, see "Data Flow Probe Setup Window" on page 105 .



Select an Application Page

This page enables you to select an application that you want to teach.

Note: The displayed applications are derived from meta data that are contained in unrecognized files on the Data Flow Probe that you selected on ["Select a Probe Page" on the previous page](#).

Important information	<ul style="list-style-type: none"> Use one of the following methods to find applications that you want to teach: <ul style="list-style-type: none"> If you know which application or publisher you want to teach, type this information into the appropriate fields and then click Search. If you want to see the entire list of applications that are associated with unrecognized files, click Search. Limited approximate string matching is automatically enabled for the Application Name and Publisher fields. For example, "Xadobe" and "adobeX" are both returned when you type "adobe".
Wizard map	"Select a Probe Page" > Select an Application Page > "Select Files Page" > "Select Application Details Page" > "Review Data Page" > "Summary Page"
Relevant tasks	"How to Teach Applications Using Express Teaching Wizard" on page 692
See also	"Express Teaching Overview" on page 691

User interface elements are described as follows:

UI Element (A-Z)	Description
Application Name	<p>Column. Applications that are associated with unrecognized files.</p> <p>Text Field. Type the name of an application that you want to teach and then click Search. For more information on how to enter information in this field, see the Important information section.</p>
Description	Additional information about the application that is associated with unrecognized files.
File Count	<p>Number of unrecognized files that are associated with the application.</p> <p>Note: The value in this column reflects the number of unnormalized files that are associated with the application.</p>
Minimum nodes	Enables you to filter the results by clicking or selecting a minimum number of nodes where the unrecognized files were scanned.
Node Count	Number of nodes where at least one unrecognized file was scanned.
Publisher	<p>Column. Publisher names that are associated with unrecognized files.</p> <p>Text Field. Type the name of the publisher you want to teach and click Search. Alternatively, click  to open the Publisher dialog box where you can select from a list of all publishers.</p> <p>For more information on how to enter information in this field, see the Important information section.</p> <p>Note: Publisher names are normalized. Therefore, publisher names may appear slightly differently.</p> <p>Click  to open the Publisher dialog box and display a list of all publishers.</p> <p>Tip: To improve normalization of publishers, see "How to Send a Publisher File to Micro Focus" on page 696.</p>
Version	<p>Version number that is associated with the application.</p> <p>Note: This may be different to the version of the file associated with the application.</p>

Select Files Page

This page enables you to specify which files to use to teach the application.

Important information	<ul style="list-style-type: none"> • At least one file must be selected. • To select all files, select the check box at the top. • Selecting a main file is recommended. Main files identify the application. An application can have multiple main files, but normally there is only one. If a Main file is found, the application is considered present.
Wizard map	"Select a Probe Page" > "Select an Application Page" > Select Files Page > "Select Application Details Page" > "Review Data Page" > "Summary Page"
Relevant tasks	"How to Teach Applications Using Express Teaching Wizard" on page 692
See also	"Express Teaching Overview" on page 691

User interface elements are described as follows:

UI Element	Description
File Name	<p>Column. Names of files that are associated with the application.</p> <p>Text Field. The name of the selected file.</p>
File Size	<p>Column. Size of the files (in kilobytes) that are associated with the application.</p> <p>Text Field. The size of the selected file (in kilobytes).</p> <p>Note: N/A appears when Care About Size is set to No.</p>
Care About Size	<p>Yes. The size of the file is used as a recognition criterion.</p> <p>Default: Yes.</p> <p>No. The size of the file is not used as a recognition criterion. As a result, only the match on the file name is needed to produce a successful file match. Moreover, the application is recognized only if the file is a main file.</p>
Relation to App	<p>Indicates the relationship between the file that is selected and the application.</p> <p>By default, the first executable file that is found which is associated with the application is marked as Main.</p> <ul style="list-style-type: none"> • Main. Indicates that an application is installed when this file is detected. • Associated. Indicates that a file may belong to an application but does not necessarily require a license. • 3rd party. Indicates a file that is included with the application but is produced by a third party.
File information tab	<p>Displays detailed information about files for the selected unrecognized file in the top pane.</p> <ul style="list-style-type: none"> • File Type. Type of the executable file. For example, Win32.exe, where exe is the file type.


UI Element	Description
	<ul style="list-style-type: none"> • Product Version. Application version number associated with the application. <p>Note: This may be different than the file version of the file that is associated with the application.</p> <ul style="list-style-type: none"> • Product Name. Name of the application that is associated with the selected file. • File Version. Version number of the selected file. • Publisher. Publisher name that is associated with the selected file. • File Signature. A checksum of the first 8 kilobytes of a file. • Description. Additional information about the selected file.
File source tab	Displays the normalized list of scan file names that contain the selected unrecognized files.






Select Application Details Page

This page enables you to select details for the application. You can also create new application details.

Important information	<ul style="list-style-type: none"> • All fields on the main page are mandatory. • Operating System and Language fields are automatically set according to the version that is selected. • (Applicable for all fields) If the name in the meta data of the unrecognized file was successfully matched to an entry in the SAI, the name will be highlighted in the search results. If there is no match, no entry is highlighted and you must select another variation of the name or create a new entry.
Wizard map	"Select a Probe Page" > "Select an Application Page" > "Select Files Page" > Select Application Details Page > "Review Data Page" > "Summary Page"
Relevant tasks	"How to Teach Applications Using Express Teaching Wizard" on page 692
See also	"Express Teaching Overview" on page 691

User interface elements are described as follows:

UI Element (A-Z)	Description
Application	<p>The name of the application that you want to teach.</p> <p>Available when: A publisher is selected.</p> <p> . Opens the Application dialog box, enabling you to filter by application name and</p>

UI Element (A-Z)	Description
	<p>select another variation of the application name.</p> <p>Note: This list contains unnormalized data.</p> <p> . Opens the New Application dialog box, enabling you to create a new application. Type a name and a description. From the drop down list, select an application type which is stored as an attribute for the application. Then, select the application you just created.</p>
Publisher	<p>The publisher name of the application.</p> <p> . Opens the Publisher dialog box, enabling you to filter by publisher name and select another variation of the publisher name from the unnormalized list.</p> <p> . Opens the New Publisher dialog box, enabling you to create a new publisher. Type a name and description.</p>
Release	<p>The release number for the application.</p> <p>Available when: An application is selected.</p> <p> . Opens the Releases dialog box, enabling you to filter by releases and select another release.</p> <p> . Opens the New Release dialog box, enabling you to create a new release. Type a name.</p>
Version	<p>Version number for the application.</p> <p>Available when: A release is selected.</p>

Review Data Page

This enables you to review information about the application before the information is saved.

Wizard map	"Select a Probe Page" > "Select an Application Page" > "Select Files Page" > "Select Application Details Page" > Review Data Page > "Summary Page"
Relevant tasks	"How to Teach Applications Using Express Teaching Wizard" on page 692
See also	"Express Teaching Overview" on page 691

Summary Page

This page enables you to view the details of the application that was saved to the user SAI file.

Wizard map	"Select a Probe Page" > "Select an Application Page" > "Select Files Page" > "Select Application Details Page" > "Review Data Page" > Summary Page
Relevant tasks	"How to Teach Applications Using Express Teaching Wizard" on page 692
See also	"Express Teaching Overview" on page 691

User interface elements are described as follows:

UI Element (A-Z)	Description
Continue	Starts the Express Teaching wizard again so you can teach more applications.
Finish	<p>Closes the Express Teaching wizard. When you are finished teaching, deploy your updates to the Data Flow Probe. To do this, see "How to Deploy User SAI Files" on page 694.</p> <p>Note: You may want to improve publisher/vendor normalization by sending a file to Micro Focus Support. For more information, see "How to Send a Publisher File to Micro Focus" on page 696.</p>

Chapter 20: Software License Compliancy

Software License Compliancy Overview	704
Software Utilization	704
How to Calculate License Compliancy for IBM	705
How to Calculate Licenses for Oracle	707
How to Configure Software Utilization	708

Software License Compliancy Overview

Universal Discovery helps manage your software costs and license compliancy obligations by identifying software inventory, measuring use activity, and automatically linking complex licensing and licensed application relationships. These activities enable your organization to better align software spending with business priorities. Moreover, tracking and maintaining software license information ensures that only the allowed number of licenses are in use, and that there are enough licenses for everyone using the software. This is often used when limited license counts are available to avoid violating strict license controls.

Universal Discovery builds relationships between licensed and licensing installed applications. Additionally, Hewlett-Packard provides documentation to help you calculate your license obligations for the following installed software packages:

- IBM. See ["How to Calculate License Compliancy for IBM" on the next page.](#)
- Oracle. See ["How to Calculate Licenses for Oracle" on page 707.](#)

To run a report that shows relationships between licensed and licensing applications, see Application License Report in the *Universal CMDB Modeling Guide*.

To calculate software use activity, see ["How to Configure Software Utilization" on page 708.](#)

Software Utilization

Universal Discovery can collect information about the software that is used on discovery nodes. The information that is collected can be used to optimize software license costs, for example, by eliminating unused or under-utilized software installations.

Software Utilization data shows the number of days that an application was used (as a percentage) over a period of time.

Universal Discovery includes a plug-in that collects software utilization data by monitoring the processes that are running on the discovery node. There is a separate file for each day, and there is also a file that contains aggregated utilization information for a utilization period. This summary file is an XML file called **discusg.cxu**. It is encoded using UTF-8 and then compressed using the gzip file format. When a discovery node is scanned, the Scanner collects a copy of the **discusg.cxu** file and stores its content in the scan file in a folder called **Software Utilization Data**. Then, the **XML Enricher** extracts and processes the software utilization data. The XML Enricher does the following during its processing:

- Extracts and parses the XML data out of the stored file.
- Calculates the software utilization for each recognized application and adds this information to the enriched scan file.
- Adds a **Utilized** flag to the file attributes.

Tip: From a software recognition perspective, any files that appear in the scan file that are unknown and have a high software utilization rate should be marked for teaching. For more information about Application Teaching, see ["Application Teaching" on page 527](#).

For more information, see ["How to Configure Software Utilization" on page 708](#).

To see platform-specific file location information for software utilization data files, see ["Universal Discovery Agent File Locations" on page 195](#).

For details on how to view software utilization data by using Inventory Tools, see ["Inventory Tools" on page 534](#).

For more information on how software utilization data is reported, see Reports in the *Universal CMDB Modeling Guide*.

How to Calculate License Compliancy for IBM

You can calculate your license compliancy position for the IBM software packages using the Processor Value Unit, which is a unit of measure used to differentiate licensing of IBM software on distributed processor technologies. The number of required licenses per processor is determined by multiplying the number of processor chips where IBM software is installed by the number of cores per chip. Then, the resulting value is multiplied by a processor value unit multiplier that IBM provides.

You can also see reports on PVU values if you configure adapters to push certain data to **Asset Manager**. For more information, see the section describing integrations in the *Universal CMDB Discovery and Integrations Content Guide*.

Note: License calculations of full capacity (non-virtualized) environments are supported only.

This task includes the following steps:

1. ["Locate the scan file data that you want to use for the calculation" below](#)
2. ["Find the processor value unit " on the next page](#)

1. Locate the scan file data that you want to use for the calculation

Open a scan file using **Viewer**. For more information, see ["Inventory Tools" on page 534](#). Then, locate certain data in scan files to determine the vendor and processor technology. To do this, refer to the following table:

Processor Attributes Mapping

Generic Name	Universal Discovery Field Name	UCMDB CI/Attribute Name
Processor Vendor	hwCPUVendor	CPU/CPU_Vendor
Processor Name	hwCPU_Type	CPU/CPU_Specifier
Server Model Number (required for IBM only)	hwBIOSMachineModel	Node/Discovered_Model
Maximum Number of Sockets per Server	hwPhysicalCPUCount	Calculate Raw Count of CPU CI Instances for Each Node
Processor Model Number	hwCPUDescription	CPU/CPUType
Processor Type (Cores per Socket)	hwCPUCoreCount	CPU/Core_Number
	hwPhysicalCPUCount	Calculate Raw Count of CPU CI Instances for Each Node

Note:

The values of the fields in the **Universal Discovery Field Name** column can be viewed by opening a scan file in the **Viewer**. In the Viewer, the data is contained at **Hardware and Configuration > Hardware Data > CPU Data > CPUs** or **BIOS**.

The values of the fields in the **UCMDB CI/Attribute Name** column can be viewed at **UCMDB > Modeling > CI Type Manager**. For more information, see "CI Type Manager" in the *Universal CMDB Modeling Guide*.

Use a search engine to map **Server Model Number** values in the **Universal Discovery** column or the **UCMDB CI/Attribute Name** column to the **Server Model Number** column in the IBM Processor Value Unit table. Enter the value into the search engine and perform basic analysis to derive the correct value.

The **Processor Model Number** value is contained in a long string. For example, in the string "Intel(R) Core (TM) i5 CPU M540 @ 2.53GHz" the Processor Model Number value is "M540". To find **Processor Model Numbers** locally on a discovery node, see more information at [IBM Processor Model Number Discovery Guide](http://www-01.ibm.com/software/lotus/passportadvantage/x86_server_processor_model_number_discovery_guide.html#windows) (http://www-01.ibm.com/software/lotus/passportadvantage/x86_server_processor_model_number_discovery_guide.html#windows).

To calculate **Processor Type (Cores per Socket)** using the corresponding field in the **Universal Discovery Field Name** column, use the following calculation:

[hwCPUCoreCount/hwPhysicalCPUCount]

If the value is equal to 1, the processor is a single (one) core processor type.

To calculate Processor Type (Cores per Socket) using the corresponding field in the **UCMDB CI/Attribute Name** column, use the following calculation:

[CPU/Core_Number]/Calculate Raw Count of CPU CI Instances for Each Node]

2. Find the processor value unit

Go to the [IBM PVU Licensing](#) table to find the processor technology for which you want to calculate the processor value unit. Then, find the multiplier in the **PVUs Per Core** column.

Note: Not all processor names are listed in the IBM PVU Licensing table.

How to Calculate Licenses for Oracle

Universal Discovery for Oracle License Management Service allows clients to run an internal Oracle compliance discovery job which publishes the results within the Universal Configuration Management Database.

To download the Universal Discovery (UD) for Oracle License Management Implementation Software (Oracle LMS) tool and the user guide, go to [UD Content Packs on ITOM Marketplace](#).

For more information, see [Universal Discovery for Oracle License Management Services](#).

How to Configure Software Utilization

Configure Software Utilization depending on your method of discovery, and on your discovery node platform.

To configure software utilization in a Management Zone, perform the following:

Zone-based Discovery

1. Infrastructure Discovery wizard: On the Universal Discovery Agent Deployment page, select a value for **Software Utilization Period**.
2. Inventory Discovery wizard: On the Preferences page, select **Scanner-based Inventory Discovery** and expand the Mapping Options pane. In the **Model per user data when number of users is at least** box, select or enter the number of users.

Note: The default scanner configuration file is already configured to collect utilization data. However, if you customize the scanner configuration file using the Scanner Generator, on the **Software Details** page ensure that **Software Utilization** is selected. For details on the Scanner Generator wizard, see ["Inventory Discovery Scanners" on page 509](#).

Manual

- **Windows.** When installing the UD Agent using the Agent Installation wizard, on the **Software Utilization** page, ensure that you select a value for the **Software Utilization Period** option. For more details, see ["Agent Installation Wizard" on page 183](#).
- **UNIX.** Use command line parameters when installing a discovery package on a discovery node. For more information, see ["Universal Discovery Resources for UNIX" on page 191](#).

Agentless Discovery

When configuring and deploying discovery resources using manual methods, in the **Scanner Generator > Software Details > "Directories Tab" on page 619**, ensure that the select the **Software Utilization** option is selected.

Part VI: Service Discovery

Chapter 21: Business Service Discovery

This chapter includes:

Service Discovery Overview	710
How to Create Service Discovery Activities	711
How to Edit Service Discovery Activities	712
How to Run Service Discovery	712
Service Discovery User Interface	714

Service Discovery Overview

Service Discovery enables you to configure and run activities to discover your business services and applications. The discovery process starts from a CI that represents the URL of a specified service, and continues only with other CIs that can potentially be related to the service.

The Service Discovery process builds dependency graphs from the consumer-provider components that make-up a service, as follows:

1. A business-service CI is connected to the start-point component.

The start-point component is the first CI referred by the URL of the service. This is the URL through which the service is consumed by users or by other business services.

2. The start-point component is connected to its neighbor components with consumer-provider relationships.

These neighbor components are the providers that are directly used by the start-point component. In this context, these neighbor components take on a consumer role.

3. The start-point's neighbor components (now taking on consumer roles) are connected via consumer-provider relationships to their own neighbors (their providers).

Discovery recursively connects neighbors to additional neighbors of these neighbors via consumer-provider relationships, until all the components that make up the service are connected.

Often, a component or running software may be both a consumer and a provider.

For more information about consumers and providers, see "Providers and Consumers" in the *Universal CMDB Developer Reference Guide*.

Service Scope

You use service-border rules to define when one service ends and another one starts. These rules enable the discovery process to categorize consumer-provider relationships as either **internal** or **external**.

- An external consumer-provider relationship connects two components that belong to different business services.
- An internal consumer-provider relationship connects two components that belong to the same business service.


The discovery process can report this category for consumer-provider relationships, since it is populated as the value of an attribute of the consumer-provider relationship.

You can therefore define the service scope to be all the components reachable from the start-point component by a path made only of internal consumer-provider relationships (that is, only consumer-provider relationships labeled as internal).

While discovering a service's components, the discovery process halts when it reaches a new provider that is connected by an external consumer-provider relationship. This means that the discovery process does not discover a provider's neighbors. To enable this functionality, you must define service-border rules before you initiate the discovery process.

However, in many cases, you want to discover the service before defining the service-border-rules. You want to see which components make up the service, and only then define the service-border-rules for these discovered components. To limit the discovery process and prevent it from endlessly discovery neighbors of neighbors, use the Hop Limit setting when you create a Service Discovery activity.


How to Create Service Discovery Activities

1. **Prerequisites.** You must have a valid Automated Service Modeling license to create service discovery activities.
2. Go to **Data Flow Management > Service Discovery**.
3. Click . The New Service Discovery Activity dialog box opens.
4. Enter the details for the new Service Discovery activity.

For more information, see ["New/Edit Service Discovery Activity Dialog Box" on page 731](#).

5. When you are finished, click **OK**.

How to Edit Service Discovery Activities

1. Go to **Data Flow Management > Service Discovery**.
2. Select a service discovery activity and click . The Edit Service Discovery Activity dialog box opens. You can do the following:
 - select a different template that contains parameter overrides
 - change the activity's scheduling
 - Change the maximum number of hops for the activity.

For more information, see ["New/Edit Service Discovery Activity Dialog Box" on page 731](#).

3. When you are finished, click **OK**.

How to Run Service Discovery

This task describes how to map services and their components.

This task includes the following steps:

- ["Prerequisites" below](#)
- ["Set up the Data Flow Probes" on the next page](#)
- ["Create an activity" on page 714](#)
- ["Run an activity" on page 714](#)
- ["Monitor the discovery process" on page 714](#)
- ["View discovery results" on page 714](#)

1. Prerequisites
 - a. Verify that the Data Flow Probe is installed on a Windows machine.

Note: The Data Flow Probe installed on a Linux platform is intended for the CMS Sync integration only, but not for discovery.

- b. Verify that the relevant packages are deployed.

If you need to deploy discovery packages, see "How to Deploy a Package" in the *Universal CMDB Administration Guide*.

- c. Ensure that the **Enable Search** option is enabled.

To change the status of the **Enable Search** option, do the following:

- i. Select **Administration > Infrastructure Settings Manager > General Settings category > Search Engine Enabled**.
- ii. Set the value to **True**.
- iii. Restart the UCMDB Server.

2. Set up the Data Flow Probes

- o **Determine the network range**

Determine the network range of the network to be discovered. For details, see "[New/Edit Range Dialog Box](#)" on page 131.

Note:

- You must configure the probe's IP address in the probe range.
- A Service Discovery activity will only try to connect to those IP addresses that may potentially be relevant for the discovered services, not to every IP address in the range. Make sure the network range is wide enough and contains all the IP addresses for your discovered services.

- o **Set the relevant credentials**

To enable the Data Flow Probes to connect to servers or applications using specific protocols, you must set the relevant credentials (for example, UD, NTCMD, SNMP, TTY, or WMI). For details on protocol parameters, see the *Universal CMDB Discovery and Integrations Content Guide*.

Note: The Data Flow Probe tries to connect to a node by using each credential in turn. Universal Discovery then saves the successful credential. The next time the Data Flow Probe connects to this node, it first tries to connect using the successful credential.

3. Create an activity

In the Service Discovery module, create a Service Discovery activity that will model a business service. For more information, see ["How to Create Service Discovery Activities" on page 711](#).

4. Run an activity

In the Service Discovery module, click **Activate**  to run a Service Discovery activity. For more information, see ["Service Discovery Page" on page 734](#).

5. Monitor the discovery process

You can monitor CIs being discovered in the discovery job's Discovery Progress pane, or from the Data Flow Probe Status Window. For details, see:

- ["Discovery Progress Dialog Box" on the next page](#)
- ["Data Flow Probe Status Window" on page 149](#)

6. View discovery results

- In UCMDB, You can display overall results for a discovery job or you can filter the results by time range, by Data Flow Probe, or by cluster. Each time you log in to UCMDB and access the Universal Discovery window, the results are updated so that the data displayed is the latest for the selected module or job.

For details on viewing discovery results, see ["Discovery Status – Results Tab" on page 729](#).

- You can also view models you have created in the Service Modeling module in the UCMDB Browser.

Service Discovery User Interface

This section includes:

Discovery Progress Dialog Box	715
Discovery Status – Progress Tab	722
Discovery Status – Results Tab	729

New/Edit Service Discovery Activity Dialog Box	731
Service Discovery Activity Templates Dialog Box	733
Service Discovery Page	734




Discovery Progress Dialog Box


This dialog box displays the progress of running discover activities, and enables you to drill down to discovered CI instances.

To access	Select Data Flow Management > Service Discovery > a node in the tree > Discovery Status pane (on the right) > Progress tab.
Important information	The discovery progress information displayed is the last status known by the UCMDB server for each job Trigger CI within the context selected for discovery.
Relevant tasks	<ul style="list-style-type: none"> • "How to Check the Status of Application Discovery (Rediscover a View)" in the <i>Universal CMDB Modeling Guide</i>. • "How to Find Discovery Errors" on page 661 • "How to Manage Discovery Errors" on page 662 • "How to Run Service Discovery" on page 712
See also	<ul style="list-style-type: none"> • "Error Messages Overview" in the <i>Universal CMDB Developer Reference Guide</i> • "Service Discovery Overview" on page 710 • "Managing Problems With Error Reporting" on page 658




Triggered CIs View - Progress/Status Matrix




Displays the status of triggered CIs through the progress of discovery.

UI Element (A-Z)	Description
	Refresh. Refreshes the matrix.
	<p>Add CI. Opens the Choose CIs to Add dialog box, enabling you to add a newly-discovered CI to the triggered CI list. For details, see "Choose CIs to Add Dialog Box" on page 667.</p> <p>Available: Discovery Modules/Jobs view only, when you select a module/job.</p>
	Rerun Discovery. Enables you to rerun the selected discovery modules/jobs.

UI Element (A-Z)	Description
	<p>Pause / Resume. Enables you to pause or resume the selected discovery</p> <p>Note:</p> <ul style="list-style-type: none"> When you pause an active job: <ul style="list-style-type: none"> triggers that are currently running continue to run until they are finished all the execution information is retained, including errors Jobs are paused based on their defined job execution policies. For details, see "Job Execution Policies" on page 36. <p>Available: Discovery Modules/Jobs view only</p>
<p>Progress bar</p>	<p>Displays the percentage of new trigger CIs that have completed the discovery process for the set of jobs contained within the focus area that you have selected for discovery since the last time the activity was modified.</p> <p>Note: When you activate discovery, the trigger CIs list are prepared. During this time, discovery progress may not be reflected immediately.</p> <p>Thereafter, discovery progress is automatically refreshed every 30 seconds.</p>

Understanding the Progress/Status Matrix and the Progress Bar

Progress Status	Total			
<p>Pending Probe</p>	<p>Displays the total number of trigger CIs waiting for the Probe to pick them up for execution.</p>	<p>Displays the number of triggered CIs successfully waiting for the Probe to pick them up for execution.</p>	<p>--</p>	<p>--</p>
<p>Reached Probe</p>	<p>Displays the total number of triggered CIs that reached the Probe, and may have started running.</p>	<p>Displays the number of triggered CIs that successfully reached the Probe, and may have started running.</p>	<p>Displays the number of triggered CIs that successfully reached the Probe and have started running, but have warnings.</p>	<p>--</p>
<p>Completed</p>	<p>Displays the total number of triggered</p>	<p>Displays the number of</p>	<p>Displays the number of</p>	<p>Displays the number of triggered CIs that</p>

Progress Status	Total			
	CIs that completed running (successfully or unsuccessfully).	triggered CIs that successfully completed running.	triggered CIs that successfully completed running, but have warnings.	failed to complete running, did not reach the Probe, or were not picked up by the Probe for execution.
Total	Displays the total number of triggered CIs.	Displays the total number of successful triggered CIs.	Displays the total number of triggered CIs that were successful, but had warnings	Displays the total number of failed triggered CIs.

Note: When discovery is kicked off by schedule, as opposed to manually being started, trigger CIs that have completed at least once do not go back into **Pending Probe** and **Reached Probe** status, and are therefore not reflected in the **Pending Probe** and **Reached Probe** rows of the Progress/Status Matrix. However, when consecutive runs of the trigger CIs complete, their statuses **are** reflected in the appropriate status column of the **Completed** row of the matrix.



Similarly, since the progress bar displays the percentage of completed trigger CIs, the progress bar does not change unless new trigger CIs are dispatched or an existing trigger CI is manually rerun.





CI Count View

Clicking a link in the Triggered CIs view enables you to view the number of triggered CIs for each discovery job that have reached the selected stage of discovery and with the selected status.

Important Information	In the Discovery Modules/Jobs view, the CI Count job is displayed only when standing on a module which contains 2 or more jobs. If there is only one job in the module, clicking the triggered CI displays the CI Instances view.
------------------------------	---




User interface elements are described below (unlabeled elements are shown in angle brackets>):






UI Element (A-Z)	Description
	Up one level. Enables you to go back to the Triggered CIs view.
	Show triggered CIs. Enables you to drill down to individual triggered CIs.





UI Element (A-Z)	Description
	Refresh. Refreshes the table.
	Remove CI. Deletes the selected CI. The CI is deleted from the specific job or activity job. Available: Discovery Modules/Jobs view only, when you select a module category and select a job.
	Rerun Discovery. Enables you to rerun the selected discovery jobs. The execution complies to the defined execution policy for the relevant discovery jobs.
	Pause / Resume. Enables you to pause/resume a selected job. Note: <ul style="list-style-type: none"> • When you pause an active job: <ul style="list-style-type: none"> ◦ triggers that are currently running continue to run until they are finished ◦ all the execution information is retained, including errors • Jobs are paused based on their defined job execution policies. For details, see "Job Execution Policies" on page 36. <p>Available: Discovery Modules/Jobs view only</p>
CI Count	Displays the number of triggered CI per job that have reached the selected stage of discovery and with the selected status.
Job Name	Displays the list of jobs that have reached the selected stage of discovery and with the selected status.

CI Instances View

Clicking a job in the **CI Count** view displays the triggered CIs for that discovery job.

UI Element (A-Z)	Description
	Up one level. Enables you to move up a level of information.
	Refresh. Refreshes the list of triggered CIs.
	Add CI. Opens the Choose CIs to Add dialog box, enabling you to add a newly-discovered CI to the triggered CI list. For details, see "Choose CIs to Add Dialog Box"

UI Element (A-Z)	Description
	<p>on page 667.</p> <p>Available: Discovery Modules/Jobs view only</p>
	<p>Remove CI. Deletes the selected CI. The CI is deleted from the specific job or activity job.</p> <p>Available: Discovery Modules/Jobs view only</p>
	<p>Filter CIs. Enables you to filter the displayed CIs.</p> <ul style="list-style-type: none"> • By Status. Available only when viewing the CIs of a particular discovery job in the Discovery Module/Jobs view. <ul style="list-style-type: none"> ◦ All. Displays all the Trigger CIs. ◦ Waiting for Probe. Displays the Trigger CIs that are ready to be dispatched and are waiting for the Probe to retrieve them. ◦ In Progress. Displays the Trigger CIs that are active and are running on the Probe. ◦ In progress (being removed). Displays the Trigger CIs that are being removed from the Trigger CIs list. ◦ Success, Failed, Warning. Displays only those CIs that have the selected status. • By Probe. Displays only the CIs triggered by a selected probe/cluster. Click to open the Select Probes dialog box. • By Dispatch Type. Displays a list of CIs according to one of the following options: <ul style="list-style-type: none"> ◦ All. Displays both CIs that are used to manually activate the job and Discovery TQL queries that are used to automatically activate the job. ◦ Manually Added. Displays the CIs that are used to manually activate the job. ◦ By Discovery Query. Displays the CIs that are used to automatically activate the job. • Reset. Click to remove any filters.
	<p>Show Message. When there are warnings/errors, opens a message box containing all the warning/error messages for the triggered CI.</p>
	<p>Show additional data. Opens the Discovered CIs dialog box, enabling you to view additional information about the CI. For details, see "Discovered/Created/Last Updated CIs Dialog Box" on page 668.</p>
	<p>Show results for triggered CI. An ad hoc request is sent to the Data Flow Probe and retrieves the latest results of the job (CIT name and number of discovered CIs) that is</p>

UI Element (A-Z)	Description
	<p>running on a specific trigger CI.</p> <p>This ad hoc request does not run the job, but brings the results of the previous job run that are stored in the Probe's database. If the job has not yet run for this trigger CI, a message is displayed. See "Show Results for Triggered CI Dialog Box" on page 681.</p> <p>If no communication log exists on the Probe, a message is displayed. You can choose to always create communication logs. For details, see "Adapter Configuration Tab" on page 259.</p>
	<p>Rerun Discovery. Enables you to rerun the discovery on the selected CI.</p>
	<p>Pause / Resume. Enables you to pause/resume a selected discovery.</p> <p>Note:</p> <ul style="list-style-type: none"> • When you pause an active job: <ul style="list-style-type: none"> ◦ triggers that are currently running continue to run until they are finished ◦ all the execution information is retained, including errors • Jobs are paused based on their defined job execution policies. For details, see "Job Execution Policies" on page 36. <p>Available: Discovery Modules/Jobs view only</p>
<p>Look for</p> 	<p>To search for a specific Probe, related host, or related IP, enter part of its name in the box and click the  button.</p>
<p><CI Instances table></p>	<p>Displays all the CI instances discovered by selected job. You can drill down into any CI instance. If triggered CIs failed, or succeeded with warnings, you can drill down further to better understand the cause for the warning or failure.</p>
<p><right-click menu></p>	<p>In addition to some of the functionality described above, right-clicking a CI enables you to do the following:</p> <ul style="list-style-type: none"> • Debug. Enables you to debug a CI. You can: <ul style="list-style-type: none"> ◦ View the Communication Log ◦ Go directly to the job's adapter ◦ Go directly to the job's details (Discovery Modules/Jobs view only) ◦ Select a script to edit ◦ Rerun discovery <ul style="list-style-type: none"> • Enable Communication Log.Creates a log file for this session. The log file

UI Element (A-Z)	Description
	<p>contains information about the connection between the Probe and a remote machine.</p> <p>Note: To capture results about the connection, see the Enable Communication Log And Record Results option on this menu.</p> <ul style="list-style-type: none"> • Enable Communication Log And Record Results. Creates a log file for this session. The log file contains information about the connection between the Probe and a remote machine. Additionally, it enables capturing the discovered results; these discovered results may help in investigating various discovery problems. • Enable Scanner Debug Log. Used for most scanner debugging purposes. • Enable Scanner Trace Log. Used for more comprehensive scanner debugging purposes. <p>Note: Communication log files are created on the Probe Manager under the C:\hp\UCMDB\DataFlowProbe\runtime\communicationLog folder. For details on how the communication logs work, see "Record DFM Code" in the <i>Universal CMDB Developer Reference Guide</i>.</p> <ul style="list-style-type: none"> • Download Scanner Log. Saves the debug or trace log to a specified location. If a log for the selected CI is unavailable, enable the debug or trace log using the Rerun Discovery menu option. • Run from step. Enables you to manually run the job on the selected CI from a particular step in the job's workflow. This is useful if you do not want to rerun the whole discovery job on the CI, but only a part of it. Note: <ul style="list-style-type: none"> ◦ The workflow steps are defined in the job's adapter file. You can view or edit the workflow in the Adapter Definition tab for the relevant adapter. For details, see "Adapter Definition Tab" on page 253. ◦ You cannot run the job from particular step if the status of the CI is Waiting for probe or In Progress. <p>Available: In the Discovery Modules/Jobs view; For CIs that trigger workflow-based jobs</p> <ul style="list-style-type: none"> • Reprocess Scan File. Reprocesses the scan files of the selected CI. Available: In the Discovery Modules/Jobs view; For CIs that trigger workflow-based jobs





Discovery Status – Progress Tab

This dialog box displays the progress of running discoveries, and enables you to drill down to discovered CI instances.

To access	Select Data Flow Management > Service Discovery > a node in the tree > Discovery Status pane (on the right) > Progress tab.
Important information	The discovery progress information displayed is the last status known by the UCMDB server for each job Trigger CI within the context selected for discovery.
Relevant tasks	<ul style="list-style-type: none"> • "How to Check the Status of Application Discovery (Rediscover a View)" in the <i>Universal CMDB Modeling Guide</i> • "How to Find Discovery Errors" on page 661 • "How to Manage Discovery Errors" on page 662 • "How to Run Service Discovery" on page 712
See also	<ul style="list-style-type: none"> • "Error Messages Overview" in the <i>Universal CMDB Developer Reference Guide</i> • "Service Discovery Overview" on page 710 • "Managing Problems With Error Reporting" on page 658 • Service Discovery Errors Report in the <i>Universal CMDB Modeling Guide</i>




Triggered CIs View - Progress/Status Matrix




Displays the status of triggered CIs through the progress of discovery.

UI Element (A-Z)	Description
	Refresh. Refreshes the matrix.
	Add CI. Opens the Choose CIs to Add dialog box, enabling you to add a newly-discovered CI to the triggered CI list. For details, see "Choose CIs to Add Dialog Box" on page 667 . Available: Discovery Modules/Jobs view only, when you select a module/job.
	Rerun Discovery. Enables you to rerun the selected discovery modules/jobs.
	Pause / Resume. Enables you to pause or resume the selected discovery

UI Element (A-Z)	Description
	<p>Note:</p> <ul style="list-style-type: none"> • When you pause an active job: <ul style="list-style-type: none"> ◦ triggers that are currently running continue to run until they are finished ◦ all the execution information is retained, including errors • Jobs are paused based on their defined job execution policies. For details, see "Job Execution Policies" on page 36. <p>Available: Discovery Modules/Jobs view only</p>
Progress bar	<p>Displays the percentage of new trigger CIs that have completed the discovery process for the set of jobs contained within the focus area that you have selected for discovery since the last time the activity was modified.</p> <p>Note: When you activate discovery, the trigger CIs list are prepared. During this time, discovery progress may not be reflected immediately.</p> <p>Thereafter, discovery progress is automatically refreshed every 30 seconds.</p> <p>During the discovery process, you may receive the following message: The progress status does not reflect the latest changes, since the activity is waiting for some of its triggers to rerun.</p> <p>When you see this message, although the progress bar shows 100% completion, the discovery of the service is not yet complete. After a few seconds, some of the triggers will be rerun. These triggers require a rerun because after they were executed, new information was discovered, possibly causing them to have more results than they did before. This most often occurs for dependency search jobs. Only after the bar shows 100% and this message no longer appears is the discovery is truly finished.</p>

Understanding the Progress/Status Matrix and the Progress Bar

Progress Status	Total			
Pending Probe	Displays the total number of trigger CIs waiting for the Probe to pick them up for execution.	Displays the number of triggered CIs successfully waiting for the Probe to pick them up for execution.	--	--
Reached Probe	Displays the total number of triggered	Displays the number of	Displays the number of	--

Progress Status	Total			
	CIs that reached the Probe, and may have started running.	triggered CIs that successfully reached the Probe, and may have started running.	triggered CIs that successfully reached the Probe and have started running, but have warnings.	
Completed	Displays the total number of triggered CIs that completed running (successfully or unsuccessfully).	Displays the number of triggered CIs that successfully completed running.	Displays the number of triggered CIs that successfully completed running, but have warnings.	Displays the number of triggered CIs that failed to complete running, did not reach the Probe, or were not picked up by the Probe for execution.
Total	Displays the total number of triggered CIs.	Displays the total number of successful triggered CIs.	Displays the total number of triggered CIs that were successful, but had warnings	Displays the total number of failed triggered CIs.

Note: When discovery is kicked off by schedule, as opposed to manually being started, trigger CIs that have completed at least once do not go back into **Pending Probe** and **Reached Probe** status, and are therefore not reflected in the **Pending Probe** and **Reached Probe** rows of the Progress/Status Matrix. However, when consecutive runs of the trigger CIs complete, their statuses **are** reflected in the appropriate status column of the **Completed** row of the matrix.







Similarly, since the progress bar displays the percentage of completed trigger CIs, the progress bar does not change unless new trigger CIs are dispatched or an existing trigger CI is manually rerun.

CI Count View

Clicking a link in the Triggered CIs view enables you to view the number of triggered CIs for each discovery job that have reached the selected stage of discovery and with the selected status.


Important Information	In the Discovery Modules/Jobs view, the CI Count job is displayed only when standing on a module which contains 2 or more jobs. If there is only one job in the module, clicking the triggered CI displays the CI Instances view.
------------------------------	---







User interface elements are described below (unlabeled elements are shown in angle brackets):






UI Element (A-Z)	Description
	Up one level. Enables you to go back to the Triggered CIs view.
	Show triggered CIs. Enables you to drill down to individual triggered CIs.
	Refresh. Refreshes the table.
	<p>Remove CI. Deletes the selected CI. The CI is deleted from the specific job or activity job.</p> <p>Available: Discovery Modules/Jobs view only, when you select a module category and select a job.</p>
	Rerun Discovery. Enables you to rerun the selected discovery jobs. The execution complies to the defined execution policy for the relevant discovery jobs.
	<p>Pause / Resume. Enables you to pause/resume a selected job.</p> <p>Note:</p> <ul style="list-style-type: none"> • When you pause an active job: <ul style="list-style-type: none"> ◦ triggers that are currently running continue to run until they are finished ◦ all the execution information is retained, including errors • Jobs are paused based on their defined job execution policies. For details, see "Job Execution Policies" on page 36. <p>Available: Discovery Modules/Jobs view only</p>
CI Count	Displays the number of triggered CI per job that have reached the selected stage of discovery and with the selected status.
Job Name	Displays the list of jobs that have reached the selected stage of discovery and with the selected status.

CI Instances View

Clicking a job in the **CI Count** view displays the triggered CIs for that discovery job.

UI Element (A-Z)	Description
	Up one level. Enables you to move up a level of information.

UI Element (A-Z)	Description
	Refresh. Refreshes the list of triggered CIs.
	<p>Add CI. Opens the Choose CIs to Add dialog box, enabling you to add a newly-discovered CI to the triggered CI list. For details, see "Choose CIs to Add Dialog Box" on page 667.</p> <p>Available: Discovery Modules/Jobs view only</p>
	<p>Remove CI. Deletes the selected CI. The CI is deleted from the specific job or activity job.</p> <p>Available: Discovery Modules/Jobs view only</p>
	<p>Filter CIs. Enables you to filter the displayed CIs.</p> <ul style="list-style-type: none"> • By Status. Available only when viewing the CIs of a particular discovery job in the Discovery Module/Jobs view. <ul style="list-style-type: none"> ◦ All. Displays all the Trigger CIs. ◦ Waiting for Probe. Displays the Trigger CIs that are ready to be dispatched and are waiting for the Probe to retrieve them. ◦ In Progress. Displays the Trigger CIs that are active and are running on the Probe. ◦ In progress (being removed). Displays the Trigger CIs that are being removed from the Trigger CIs list. ◦ Success, Failed, Warning. Displays only those CIs that have the selected status. • By Probe. Displays only the CIs triggered by a selected probe/cluster. Click to open the Select Probes dialog box. • By Dispatch Type. Displays a list of CIs according to one of the following options: <ul style="list-style-type: none"> ◦ All. Displays both CIs that are used to manually activate the job and Discovery TQL queries that are used to automatically activate the job. ◦ Manually Added. Displays the CIs that are used to manually activate the job. ◦ By Discovery Query. Displays the CIs that are used to automatically activate the job. • Reset. Click to remove any filters.
	Show Message. When there are warnings/errors, opens a message box containing all the warning/error messages for the triggered CI.
	Show additional data. Opens the Discovered CIs dialog box, enabling you to view

UI Element (A-Z)	Description
	<p>additional information about the CI. For details, see "Discovered/Created/Last Updated CIs Dialog Box" on page 668.</p>
	<p>Show results for triggered CI. An ad hoc request is sent to the Data Flow Probe and retrieves the latest results of the job (CIT name and number of discovered CIs) that is running on a specific trigger CI.</p> <p>This ad hoc request does not run the job, but brings the results of the previous job run that are stored in the Probe's database. If the job has not yet run for this trigger CI, a message is displayed. See "Show Results for Triggered CI Dialog Box" on page 681.</p> <p>If no communication log exists on the Probe, a message is displayed. You can choose to always create communication logs. For details, see "Adapter Configuration Tab" on page 259.</p>
	<p>Rerun Discovery. Enables you to rerun the discovery on the selected CI.</p>
	<p>Pause / Resume. Enables you to pause/resume a selected discovery.</p> <p>Note:</p> <ul style="list-style-type: none"> • When you pause an active job: <ul style="list-style-type: none"> ◦ triggers that are currently running continue to run until they are finished ◦ all the execution information is retained, including errors • Jobs are paused based on their defined job execution policies. For details, see "Job Execution Policies" on page 36. <p>Available: Discovery Modules/Jobs view only</p>
<p>Look for</p> 	<p>To search for a specific Probe, related host, or related IP, enter part of its name in the box and click the  button.</p>
<p><CI Instances table></p>	<p>Displays all the CI instances discovered by selected job. You can drill down into any CI instance. If triggered CIs failed, or succeeded with warnings, you can drill down further to better understand the cause for the warning or failure.</p>
<p><right-click menu></p>	<p>In addition to some of the functionality described above, right-clicking a CI enables you to do the following:</p> <ul style="list-style-type: none"> • Debug. Enables you to debug a CI. You can: <ul style="list-style-type: none"> ◦ View the Communication Log ◦ Go directly to the job's adapter ◦ Go directly to the job's details (Discovery Modules/Jobs view only)

UI Element (A-Z)	Description
	<ul style="list-style-type: none"> ○ Select a script to edit ○ Rerun discovery ● Enable Communication Log. Creates a log file for this session. The log file contains information about the connection between the Probe and a remote machine. <p>Note: To capture results about the connection, see the Enable Communication Log And Record Results option in this menu.</p> ● Enable Communication Log And Record Results. Creates a log file for this session. The log file contains information about the connection between the Probe and a remote machine. Additionally, it enables capturing the discovered results; these discovered results may help in investigating various discovery problems. ● Enable Scanner Debug Log. Used for most scanner debugging purposes. ● Enable Scanner Trace Log. Used for more comprehensive scanner debugging purposes. <p>Note: Communication log files are created on the Probe Manager under the C:\hp\UCMDB\DataFlowProbe\runtime\communicationLog folder. For details on how the communication logs work, see "Record DFM Code" in the <i>Universal CMDB Developer Reference Guide</i>.</p> <ul style="list-style-type: none"> ● Download Scanner Log. Saves the debug or trace log to a specified location. If a log for the selected CI is unavailable, enable the debug or trace log using the Rerun Discovery menu option. ● Run from step. Enables you to manually run the job on the selected CI from a particular step in the job's workflow. This is useful if you do not want to rerun the whole discovery job on the CI, but only a part of it. <p>Note:</p> <ul style="list-style-type: none"> ○ The workflow steps are defined in the job's adapter file. You can view or edit the workflow in the Adapter Definition tab for the relevant adapter. For details, see "Adapter Definition Tab" on page 253. ○ You cannot run the job from particular step if the status of the CI is Waiting for probe or In Progress. <p>Available: In the Discovery Modules/Jobs view; For CIs that trigger workflow-based jobs</p>




UI Element (A-Z)	Description
	<ul style="list-style-type: none"> • Reprocess Scan File. Reprocesses the scan files of the selected CI. <p>Available: In the Discovery Modules/Jobs view; For CIs that trigger workflow-based jobs</p>


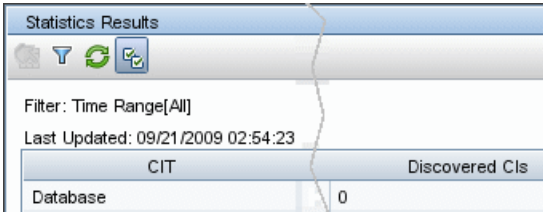
Discovery Status – Results Tab

This tab displays the discovery results from discovery job runs.

To access	Select Data Flow Management > Service Discovery > a node in the tree > Discovery Status pane (on the right) > Results tab.
Relevant tasks	<ul style="list-style-type: none"> • "How to Find Discovery Errors" on page 661 • "How to Manage Discovery Errors" on page 662 • "How to Run Service Discovery" on page 712
See also	<ul style="list-style-type: none"> • "Service Discovery Overview" on page 710 • "Managing Problems With Error Reporting" on page 658 • Service Discovery Errors Report in the <i>Universal CMDB Modeling Guide</i>

User interface elements are described below (unlabeled elements are shown in angle brackets>):



UI Element (A-Z)	Description
	Refresh. Retrieves the latest discovery results from the server (job results are not automatically updated in the Results pane).
	<p>View Instances. Displays all new and updated CIs. Select a CIT and click:</p> <ul style="list-style-type: none"> • View Created Instances to view CIs created during the discovery • View Updated Instance to view CIs updated during the discovery <p>Note: When you double-click a row, created CI instances are displayed.</p> <p>Available: When the discovery results include created or updated instances.</p>
	<p>Select the time range or Probe for which to display discovery results and statistics.</p> <ul style="list-style-type: none"> • By Time Range:

UI Element (A–Z)	Description										
	<ul style="list-style-type: none"> ○ All. Displays results for all job runs. ○ From Now/Last Minute/Last Hour/Last Day/Last Week. Choose a period of time for which to display results. ○ Custom Range. Opens the Change Timeframe dialog box where you can enter the date or choose a From and To date and time from the calendar. Click Now to enter the current date and time. Click Last Day to enter the current date and time in the To box and yesterday's date and time in the From box. Click OK to save the changes. ● By Probe: To view results by Probe, select to open the Choose Probe dialog box. Selecting All Data Flow Probes displays the results for all of the Data Flow Probes. 										
	<p>Show all declared CI Types. By default, only discovered CITs are listed in the table; the Discovered CIs column includes CITs if the number of CIs found is greater than zero. Click the button to display every CI that can be discovered by the job, even if the Discovered CIs value is zero:</p>  <table border="1" data-bbox="375 926 915 1136"> <thead> <tr> <th colspan="2">Statistics Results</th> </tr> </thead> <tbody> <tr> <td colspan="2">Filter: Time Range[All]</td> </tr> <tr> <td colspan="2">Last Updated: 09/21/2009 02:54:23</td> </tr> <tr> <th>CIT</th> <th>Discovered CIs</th> </tr> <tr> <td>Database</td> <td>0</td> </tr> </tbody> </table>	Statistics Results		Filter: Time Range[All]		Last Updated: 09/21/2009 02:54:23		CIT	Discovered CIs	Database	0
Statistics Results											
Filter: Time Range[All]											
Last Updated: 09/21/2009 02:54:23											
CIT	Discovered CIs										
Database	0										
<p><Results grid></p>	<p>Displays the discovery results and statistics.</p> <ul style="list-style-type: none"> ● CIT. The name of the discovered CIT. <p>You can configure discovery so that any object reported by the job and whose CIT is not defined in the adapter's discovered CITs list is marked in red. Objects include those added by the Probe result mechanism.</p> <p>To set this parameter:</p> <ol style="list-style-type: none"> a. Select Administration > Infrastructure Settings Manager. b. Select the General Settings category. c. Locate the Enable statistics results validation according to adapter parameter. d. Change the value to True. <ul style="list-style-type: none"> ● Created. The number of CIT instances created in the period selected or for the selected Probe. ● Deleted. The number of CIT instances deleted in the period selected or for the selected Probe 										

UI Element (A–Z)	Description
	<ul style="list-style-type: none"> • Discovered CIs. The number of CIs that were discovered for each CI type. • Total. The total number of CIs in each column. • Updated. The number of CIT instances that were updated in the period selected.
Filter	The time range set with the Set Time Range button.
Last updated	The date and time that the Results grid was last updated.

New/Edit Service Discovery Activity Dialog Box

This dialog box enables you to create or edit a Service Discovery activity.

To access	Select Data Flow Management > Service Discovery and do one of the following: <ul style="list-style-type: none"> • To create an activity: Click New Service Discovery Activity . • To edit an existing activity: Select an activity and click Edit .
Relevant tasks	<ul style="list-style-type: none"> • "How to Create Service Discovery Activities" on page 711 • "How to Edit Service Discovery Activities" on page 712

Details Area

User interface elements are described below:

UI Elements	Description
Activity Name	The name of the activity. This field is mandatory. <p>Note: Naming conventions:</p> <ul style="list-style-type: none"> • The name can contain the following characters: a-z, A-Z, 0-9, hyphen (-), underscore (_), and space (). • The name is not case sensitive. • The name must be limited to a length of 40 characters.



UI Elements	Description
Type	Select the CI type of the service that will be created and discovered by this activity.
URL	<p>Enter a valid URL for the starting point for the Service Discovery activity.</p> <p>Valid URLs have the one of the following formats:</p> <ul style="list-style-type: none"> • [<protocol>://][<name>][.<domain>][.<root-domain>][:<port>][/<site>] • [<protocol>://][<IP>][:<port>][/<site>] <p>where:</p> <ul style="list-style-type: none"> • <protocol> = http:// or https:// • <name> = The <name> can contain any Unicode letter, character, or number. The <name> may contain a dash ("-"), but not at the beginning or at the end, nor can there be two or more consecutive dashes. The <name> may not contain any other special character. • <domain> = Same as <name>. • <root-domain> = The <root-domain> must contain at least two characters, and can contain any Unicode letter, but no numbers. The <root-domain> may not contain any special characters. • <IP> = Any valid IPv4 address. • <port> = The <port> may contain only digits—at least two, and no more than 5. • <site> = Any character (including special characters), but excluding white spaces. <p>Note: Only the <name> or <IP> values are mandatory (depending on the selected format for the URL); all other values are optional.</p>
Template	<p>Select a Template resource. Parameter values in a template override those specified for a job (if any).</p> <p>A default template (with default parameter values) exists, and you can use this template if you do not want to create one. The default template can be changed. For more information, see "Service Discovery Activity Templates Dialog Box" on the next page</p>
Hop Limit	Limit the scope of the Service Discovery activity by specifying the maximum number of consumer-provider relationships to be discovered. The default value is 5.

Scheduling Area

This tab allows you to schedule jobs for the Service Discovery activity.

Caution: When creating discovery jobs, try to avoid scheduling multiple jobs to run during the

same time frame.


UI Elements	Description
Repeat Every:	Enables you to specify the interval at which the activity will run.
Allow Discovery to run at:	Enables you to constrain the time at which the activity will run. Select a predefined time from the drop-down list, or click  and then click  to open the Edit Time Template dialog box, where you can define a custom time frame.

Service Discovery Activity Templates Dialog Box





A Template resource specifies parameter overrides for selected jobs of the Service Discovery activity. These jobs must be a subset of the jobs specified in the Type resource that is selected for this Service Discovery activity. Different Service Discovery activities can use different templates, and the same template may be assigned to different Service Discovery activities.

Editing a template that is already associated with one or more activities will change the parameters for those activities. In the next scheduled run of such an activity, those new parameter values will be used.

This dialog box enables you to create or edit a Service Discovery activity template.

To access	Select Data Flow Management > Service Discovery . Select an activity and click  .
Relevant tasks	<ul style="list-style-type: none"> • "How to Create Service Discovery Activities" on page 711 • "How to Edit Service Discovery Activities" on page 712

User interface elements are described below:

UI Element	Description
	Enables you to create service discovery activity templates.
	Enables you to specify overrides for particular parameters in the activity's jobs.
	Deletes the selected template.
	Refreshes the list of templates.

Service Discovery Page







This page enables you to manage and run Service Discovery activities, and troubleshoot why expected CIs are missing after discovery.








To access	Select Data Flow Management > Service Discovery .
Relevant tasks	"How to Create Service Discovery Activities" on page 711
See also	<ul style="list-style-type: none"> • "Service Discovery Overview" on page 710 • "New/Edit Service Discovery Activity Dialog Box" on page 731

User interface elements are described below:

Service Discovery Activities Pane

The Service Discovery Activities pane displays all of the service discovery activities that have been defined.

UI Element	Description
	New Service Discovery Activity. Enables you to create service discovery activities.
	Edit. Enables you to change the following information for the selected discovery activity: <ul style="list-style-type: none"> • template • schedule • maximum number of hops
	Delete. Deletes the selected discovery activity.
	Reload Data. Refreshes the data in the Service Discovery Activities pane.
	Activate. Activates the selected discovery activity. <p>Note: If the trigger CI for the activity is missing, the activity name will be grayed out and you will not be able to activate the activity. The jobs for this activity will still run, but you will not be able to modify the activity in any way. It is recommended to delete the invalid activity and recreate it.</p>
	Deactivate. Deactivates the selected discovery activity.

UI Element	Description
	Pause. Pauses the selected discovery activity.
	Resume. Resumes the selected, paused discovery activity.
	Rerun. Runs the selected discovery activity again.
	<p>Opens the Service Discovery Activity Templates dialog box.</p> <p>Click  to create a new template, or click  to edit an existing template.</p> <p>This dialog box enables you to define specific overrides to parameters in jobs that are included in the default template.</p>
<right-click menu>	<p>In addition to some of the functionality described above, right-clicking a discovery activity enables you to do the following:</p> <ul style="list-style-type: none">  Clear Probe Results Cache. Clears the selected activity's results cache on the Probes. <p>Note: If an activity's results cache is cleared, all discovery results are sent again the next time the activity runs.</p>


Service Discovery Details Pane







The right pane of the Service Discovery view displays the following information:

- ["Activity Details Pane" below](#)
- ["Discovery Status Pane" on the next page](#)

Activity Details Pane

Displayed when you select a discovery activity in the Service Discovery Activities pane.

UI Element	Description
Overview Tab	Displays the type and status of the discovery activity, and a summary of the activity as it was defined when it was created. To edit an activity, select the activity and click the Edit Activity  button.
Activity Jobs Tab	Displays the activity jobs available for the discovery activity.

UI Element	Description
	<p>The Activity Jobs tab displays all possible jobs that can run during the execution of a service discovery activity. However, some jobs may not be executed since they are not necessary for the service being discovered. The jobs that are actually executed are listed in the "Discovery Status – Progress Tab".</p> <ul style="list-style-type: none"> • Activity Jobs Toolbar <ul style="list-style-type: none"> ◦  Go to Adapter. Redirects you to the adapter for the selected activity job. ◦  View Permission Details. Opens the Discovery Permissions dialog box, enabling you to view the permissions data for the selected activity job. ◦  View Discovered CITs in Map. Displays the selected adapter, together with its CIs and relationships, in the Discovered CITs Map window. Hold the cursor over a CIT to read a description in a tooltip. ◦  View Parameters. Opens the Activity Job Parameters dialog box, enabling you to view the parameters for the selected activity job. ◦  Edit Script. Displays a list of scripts related to the selected activity job. Select a script and edit it in the Script Editor. ◦  Edit Trigger Query. Displays the trigger query related to the selected activity job, enabling you to open and edit it in the Trigger Query Editor. • Activity Jobs Grid. Displays the information about jobs available for the discovery activity. <ul style="list-style-type: none"> ◦ Activity Job Name. The name of the activity job. ◦ Discovered CITs. The CITs discovered by the activity job. ◦ Protocols. The protocols used by the activity job. ◦ IPv6 Support. Indicates whether the activity job's adapter supports IPv6. ◦ Scheduling. Displays the details of the activity job's discovery schedule.

Discovery Status Pane

Displays the progress and results of the selected discovery activity.

UI Element	Description
Progress Tab	<ul style="list-style-type: none"> • Displays the progress of the new trigger CIs across the discovery activity. For more information, see "Discovery Status – Progress Tab" on page 722.

UI Element	Description
	<ul style="list-style-type: none">• The information is automatically refreshed every 30 seconds.• Use the information displayed in this pane to drill down to problematic trigger CIs, to uncover specific problems that Universal Discovery encountered during the discovery—for example, incorrect credentials. You can also add newly discovered CIs to the trigger CI list.• Hold the SHIFT and CTRL keys to select adjacent and non-adjacent CIs in a list.
Results Tab	Displays the results from the selected discovery activity. For more information, see "Discovery Status – Results Tab" on page 729 .

Part VII: Reconciliation

Chapter 22: Data Reconciliation

This chapter includes:

Reconciliation Overview	739
Identification Service	740
Data-In Service - Populating UCMDB	746
Merging Matched CIs Using Reconciliation Priority Rules	753
How to Create an Identification Rule	754
How to Add Reconciliation Priorities to a CI Type	756
Identification Rule Schema	757
Reconciliation Priority Window	764
How to Add Reconciliation Priority for API-based Integrations	768
How to Enable Redundant Reverse Check	769
How to Enable Attribute Name Verification during the Matching Phase of Identification	769
How to Modify the Maximum Number of Threads for the Data-In Service	770
How to Enable CI Type Tenant Owner Verification during the Matching Phase of Identification ..	771

Reconciliation Overview

Reconciliation is the process of identifying and matching entities from different data repositories (for example, UCMDB Universal Discovery, DDMI, ticketing, or BSM). This process is designed to avoid duplicate CIs in UCMDB.

Many different data collectors can send CIs to UCMDB. In actuality, each different source might be providing information about the same CI. The reconciliation process is responsible for identifying and matching entities from different data collectors and storing them, without duplicating CIs, in UCMDB.

Three main services provide support for the reconciliation process:

- **Identification service.** Responsible for comparing incoming data (input CIs), according to defined identification rules. For details, see ["Identification Service" on the next page](#).
- **Data In service.** Responsible for inserting data into UCMDB. This service decides whether to:

- merge incoming data with existing CIs in UCMDB
- ignore input CIs in the case of multiple matches

For details, see ["Data-In Service - Populating UCMDB" on page 746](#).

- **Merge.** In Federation and Data-in flows, this service is responsible for merging CIs. Merging is done in accordance with defined reconciliation priority rules. For details, see ["Merging Matched CIs Using Reconciliation Priority Rules" on page 753](#).

These services operate during the data-in process for inserting data from different sources into UCMDB, and during federation for connecting or merging information from different data repositories during TQL query calculations.

Identification Service

The Identification service uses identification rules to identify CIs. An identification rule is composed of three criterion sets:

- **Identification criteria.** A set of criteria that defines all possible conditions to find all candidate CIs for matching to a newly introduced CI. Two CIs are identical if one of the identification criteria is satisfied.
- **Match criteria.** There are two types of match criteria:
 - **Match verification criteria.** A set of criteria that are applied to all candidates left over after performing identification (in the previous step). Match verification ends successfully only when all applied verification criteria are true or missing data (NA).
 - **Match validation criteria.** An ordered set of criteria that is applied to all candidates left over after performing match verification. For each criterion, the following results are possible:
 - A true result implies a match
 - A false result implies no match
 - Missing data (NA) causes reconciliation to proceed to the next criterion. If all validation criterion are NA, then all candidates left after match verification will be implied as matched

When trying to determine whether or not two CIs are the same (according to the identification rule), each criterion is evaluated. Each criterion, in one of the above sections, contains one or more conditions. There are two types of conditions:

- **Attribute conditions.** Test whether or not two CIs have the same value (or same value while ignoring case) as the given attribute defined for the condition.
- **Connected CI conditions.** Test whether or not the two CIs share the same number of connected CIs defined for the condition.

For a criterion to evaluate to a `true` value, all of the conditions must evaluate to `true`. If one condition evaluates to `false`, the entire criterion evaluates to `false`. If one condition cannot be evaluated (its required data is missing in one of the two CIs being identified), the condition returns `unknown`, and, in turn, the entire criterion that contains it returns as `unknown`.

The identification process is as follows:

1. **At least one identification criteria must return true.** The identification process tests the identification criteria.
 - If there is at least one identification criterion that returns `true`, the identification process continues.
 - If no identification criterion returns `true`, then the CIs are not the same and the identification process ends here.
2. **Are there contradictions between the CIs?** The identification process tests the verification criteria.
 - If all of the verification data returns either `true` or `unknown`, the identification process continues.
 - Otherwise, there is a contradiction between the two CIs, and they are not the same and the identification process ends here.
3. **Evaluate the validation criteria.** The identification process tests the verification criteria one by one and according to each one's priority:
 - If the validation criterion is satisfied, the two CIs are the same.
 - If none of the validation criteria are satisfied, and a validation criterion returns `false`, the two CIs are unmatched.
 - If none of the validation criteria are satisfied or refuted:
 - i. The criteria from the next priority are evaluated.
 - ii. If there are no more criteria (the last priority was evaluated), then the two CIs are the same.

Identification Process Example

The following items are used in this example:

Input node	<ul style="list-style-type: none">• name = n1• ip_address = ip1• MAC address = m1• os_family = nt
UCMDB nodes	<ul style="list-style-type: none">• N1: name=n2• N2 :<ul style="list-style-type: none">◦ ip_address=ip1,ip2◦ MAC address=m1◦ os_family=nt• N3:<ul style="list-style-type: none">◦ name=n3◦ MAC address = m1◦ hw_id = id1◦ os_family = unix

1. For each UCMDB node, run the identification criteria:
 - Node N1 does not match any identification criteria, so it will not be added to the candidates list.
 - Node N2 matches the IP identification criterion of the input node, so it will be added to the candidates list.
 - Node N3 does not match the input node by the IP identification criterion, but does match by the MAC address identification criterion, so it will be added to the candidates list.

Therefore, the candidates list is: N2 and N3.

2. For each node in the candidates list, run OS match verification criteria. Node N3 does not satisfy this rule, since its OS is UNIX and the input node's OS is NT. Therefore, N3 will be removed from the candidates list.

The candidates list is: N2.
3. Run the match validation criteria one by one on node N2. Since node N2 has no data conflicts, the match validation criteria are approved and N2 is marked as matched.

The result of the identification process is: N2 = ip_address=ip1,ip2, MAC address=m1, os_family=nt.

To configure match criteria, see ["Identification and Match Criteria Configuration "](#) on the next page.

For examples of configuring identification rules, see ["Examples of Identification Configuration" on page 745](#).

Note: The identification process creates an identification map which is limited by default to 2,000,000 mappings. Each identification between two CIs is considered a separate mapping for each CI involved. Additionally, there is default limit of 5,000 mappings per CI. If you get an error saying that the identification map is too large, it may indicate that there is a problem with your data (for example, many nodes connected to a single IP address). Check the **cmdb.reconciliation.identification.log** for warnings. If there are none, check the **cmdb.reconciliation.log** to examine the actual identification map for unusual items.

Identification and Match Criteria Configuration

Depending on your data source, available credentials, and specific system security settings, an integration point may have access to only a limited set of attributes when identifying a CI.

For example, IP range discovery detects two IP addresses (10.12.123.101 and 16.45.77.145), and creates two nodes. However, detailed system discovery may detect that those two IP addresses are actually configured on two network interfaces in the same node.

This means that you cannot always rely on a single matching set of attributes for identification – other possible attributes that can potentially help to identify the CI should also be listed. In the previous example, the node identification attributes can be the IP address and the network interface. If you use the IP address to identify the CI, you see that all three discovered nodes are the same node.

Suppose that detailed system discovery detects a node with IP address 10.12.123.101 and network interface MAC1. At some point, that node was shut down, and the same IP address (10.12.123.101) was given to another node with network interface MAC2. These two nodes have the same IP address; however, it is obviously not the same CI. Performing match validation on the network interface data helps us to realize that it is not the same node.

The identification criteria are used to select candidates, and the match criteria are used to approve the identification result or dismiss it. For example, while handling input CI A, we may get identification candidates B and C, and the match criteria will dismiss B. In that case, we are left with C, which means that A is identified as C.

Identification Criteria

Data that the reconciliation engine receives from different data sources may contain different subsets of the attributes (topology) necessary for identifying a CI. The identification criteria should contain all

potential attributes on which CI matching can be done.

Specifications

Each identification criterion defines a potential condition for CI matching. The criterion can be an attribute such as node name, or topology such as IP address. A criterion may contain two or more conditions, to create a more complex matching rule. It may also contain different condition operators such as equals or contains, or it may contain some master value that defines a value in the CI that will always allow a match.

During the identification process, all identification criteria are running to find all candidate CIs for matching.

Possible Node Identification Criteria

- HW ID
- Network interface (containing a condition operator)
- Node name
- IP address (containing a condition operator)

Match Criteria

While identification criteria list all potential attributes for matching the data, match criteria contain the attributes that are essential for matching CIs, if any exist. This means that if two CIs are marked as candidates to be matched by the identification criteria, the match criteria will check if the data exists in both CIs in order to match the condition.

Match criteria are also used during the Data-In process in case of multiple matches, to make the decision to merge CIs from the CMDB. The CIs are merged only if the match criteria are satisfied. If one of the CIs does not satisfy the match criteria, the merge is not performed.

Specifications

A match criterion is satisfied if two candidate CIs have the same essential data (as defined in the that criterion), the data matches the condition, or if at least one of the CIs has no essential data.

Match criteria can be divided into two categories:

- Match verification criteria – if the verification criterion is not satisfied on two candidate CIs, these CIs are not matched.
- Match validation criterion – if the criterion with higher priority is satisfied (without missing data) on two candidate CIs, the validation criterion with lower priority is even not checked and the CIs are

marked as matched. Similarly, if the validation criterion with higher priority is refuted on two candidate CIs, the criterion with lower priority is even not checked and the CIs are marked as not matched.

Possible Node Match Criteria

- Match verification criteria uses the discovered OS data for verification. This means that if two nodes have discovered OS data and this data does not match, these two nodes are not matched.
- Match validation criteria (ordered from highest to lowest priority):

Priority 1. HW ID with an **equals** operator

Priority 2. Node name with an **equals** operator

Priority 3. Network interface with a **contains** operator

This means that if two nodes with the same HW ID are discovered, they are marked as matched even if they have different network interfaces or node names. On the other hand, if the discovered HW IDs on the nodes are not the same, the nodes are not marked as matched even if the network interfaces and node names are the same. The network interface rule is checked only if one of the nodes has no discovered HW ID.

Examples of Identification Configuration

Sample "vlan" CI Type Identification Configuration

```
<identification-config type="vlan">
  <identification-criteria>
    <identification-criterion>
      <attribute-condition attributeName="vlan_id"/>
      <connected-ci-condition ciType="physical_port"
linkType="membership">
        <overlap-fixed-operator number-of-matches="1"/>
      </connected-ci-condition>
    </identification-criterion>
  </identification-criteria>
</identification-config>
```

Sample "Installed Software" CI Type Identification Configuration

```
<identification-config type="installed_software" xmlns:xsi=
"http://www.w3.org/2001/XMLSchema-instance" xsi:noNamespaceSchemaLocation=
"C:\StarTeam\UCMDB\mam\ws\assets\dc\backend\reconciliation\src\main\
resources\schema\reconciliation.xsd"
  description="Installed Software is identified by a combination of their
container Node and either its Name or DML Product Name.
Two similarly identified installed software will be considered different
entities in case of mismatch of either File System Path, DML Product Name or
its Name.">
  <identification-criteria>
    <identification-criterion>
      <attribute-condition attributeName="dml_product_name"/>
      <attribute-condition attributeName="root_container"/>
    </identification-criterion>
    <identification-criterion>
      <attribute-condition attributeName="name"/>
      <attribute-condition attributeName="root_container"/>
    </identification-criterion>
  </identification-criteria>
  <match>
    <verification-criteria>
      <verification-criterion>
        <attribute-condition attributeName="file_system_path"/>
      </verification-criterion>
    </verification-criteria>
    <validation-criteria>
      <validation-criterion priority="1">
        <attribute-condition attributeName="dml_product_name"/>
      </validation-criterion>
      <validation-criterion priority="2">
        <attribute-condition attributeName="name"/>
      </validation-criterion>
    </validation-criteria>
  </match>
</identification-config>
```

Data-In Service - Populating UCMDB

After the Identification service runs, the identified data is merged and inserted into the UCMDB by the Data-In service. When the CI is created, a stable ID is generated. The stable ID remains the same when the name, attribute name, or property values (during normalization) change.

Multiple CI Matching

One of the major problems that the Data-In service solves is deciding what to do if the input CI matches multiple UCMDDB CIs.

To make this decision, the Data-In service uses match criteria.

The process is as follows:

1. Input CIs are merged with each matching UCMDDB CI.
2. For each pair of CIs resulting from this merge, match (verification and validation) criteria are run.
 - If at least one pair does not pass the match criteria check, the CIs are not merged, and the Data-In service ignores the input CI.
 - If all pairs pass the match criteria check, the CIs are merged.

Note: The CIs are merged by the Merge service.

For examples of multiple CI matching, see:

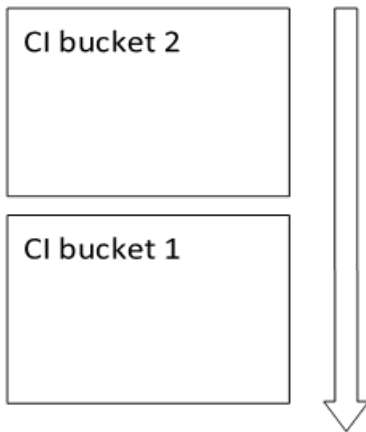
- ["Multiple CI Matching - Example 1" on page 750](#)
- ["Multiple CI Matching - Example 2" on page 751](#)

Multithreaded Data-In Service

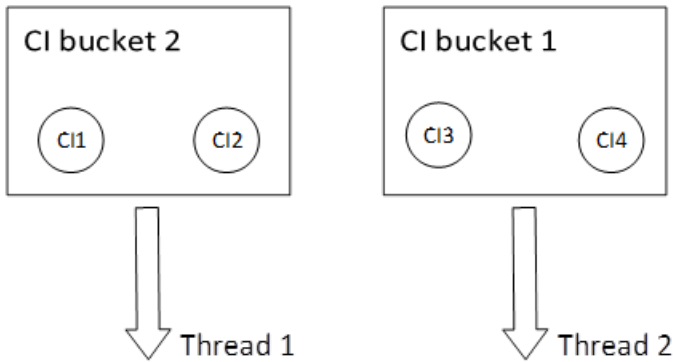
Starting from UCMDDB 10.30, the Data-In service is multithreaded and is capable to scale the speed of inserting data into UCMDDB by adjusting the number of allocated threads.

Note: By default, the Data-In service uses four allocated threads. For more information about how to adjust the allocated threads of the Data-In service, see ["How to Modify the Maximum Number of Threads for the Data-In Service" on page 770](#).

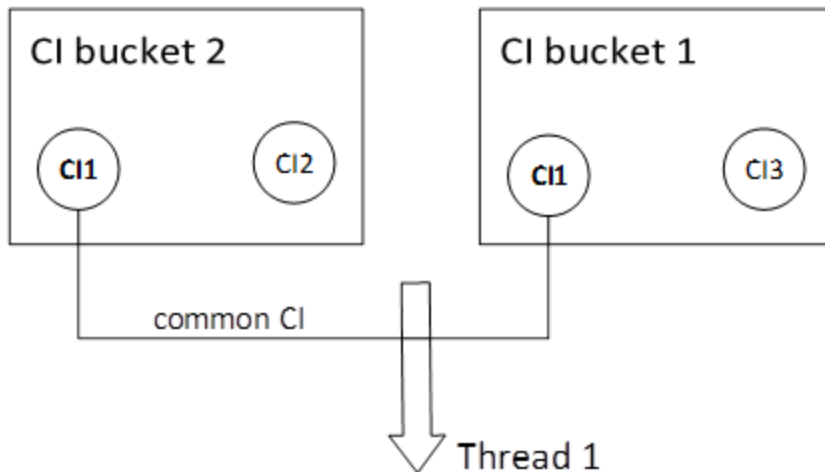
In previous versions of UCMDDB, the Data-In service uses a serial architecture and processes the arriving CIs and their updates in a controlled single-threaded approach. This architecture guarantees the data model consistency but is less efficient.



The multithreaded Data-In service concurrently processes multiple CI buckets on multiprocessor or multi-core systems if these buckets do not carry overlapping CIs.



To guarantee the data model consistency, the multithreaded Data-In service processes the CI buckets that carry the same CI information sequentially. In this situation, the multithreaded architecture does not improve the performance of the Data-In service.



With the multithreaded Data-In service, it is recommended that you consider the following approaches, which can eventually speed up the running jobs and ease the management of UCMDB Data-In:

- Break UCMDB integrations into non-overlapping CI domains
- Set up discovery on different or unrelated CI domains

Server-Side Data Normalization

Before populating the CMDB with new CIs, the server normalizes the incoming data as follows:

- When a CI of type **ip_address** is reported, if one of the **name** or the **ip_address_value** attributes contains data, the other is populated automatically.
- When a CI of type **ip_subnet** is reported, if one of the **network_netmask** or **ip_prefix_length** attributes contains data, the other is populated automatically.
- When the **REPLACE_VALUE_WITH_VALUE_FROM_SYSTEM_PROPERTY** qualifier is defined for a particular attribute, the attribute is normalized with the specified system property value.

For example, the **routing_domain** attribute, by default, contains the **REPLACE_VALUE_WITH_VALUE_FROM_SYSTEM_PROPERTY** qualifier where:

- **CONSTANT_TO_REPLACE** data item is defined as **\${DefaultDomain}**
- **SYSTEM_PROPERTY_NAME** data item is defined as **default.domain**

This means that if a CI of type **ip_address** is reported with **\${DefaultDomain}** in the **routing_domain** attribute, then the **routing_domain** attribute is populated with the value in the **default.domain** setting.

- If the CI attribute's **Discovery Auto Truncate (DDM_AUTOTRUNCATE)** qualifier is enabled, then results of type STRING are truncated according to the database encoding setting.

Note: By default, the database encoding is defined as UTF-8. This encoding can be changed in the Infrastructure Settings Manager, in the **Reconciliation Settings > Database Encoding** setting (**reconciliation.auto.truncate.db.encoding**). To access the Infrastructure Settings Manager, go to **Administration > Infrastructure Settings Manager**. For more details, see "Infrastructure Settings Manager Page" in the *Universal CMDB Administration Guide*.

- If the CI attribute has a case qualifier that is enabled, then the case of all of the results are normalized. The case qualifiers are:

Qualifier	Display Name	Description
TO_UPPER_CASE	Upper Case	Normalizes all results to upper case
TO_LOWER_CASE	Lower Case	Normalizes all results to lower case

Note: The deprecated qualifiers, **DDM_AUTOUPPERCASE** and **DDM_AUTOLOWERCASE**, can also be used to normalize results to upper case or lower case respectively, if enabled.

- If the **Discovery Auto Trim (DDM_AUTOTRIM)** qualifier for the attribute is enabled, any leading and trailing spaces and tabs are removed from the string.

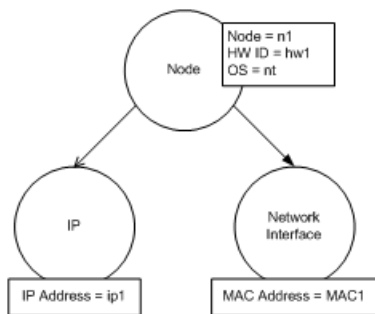
Note: This qualifier must be added only for the **String** type attributes.

For more information about attributes, see "CI Type Attributes" in the *Universal CMDB Modeling Guide*.

Multiple CI Matching - Example 1

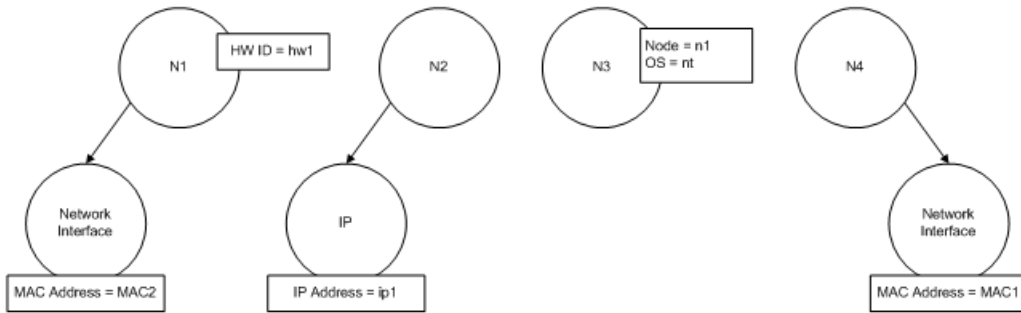
The following example demonstrates how the Data-In service matches multiple with different identification criteria where there are no conflicts.

1. The input bulk data is received.

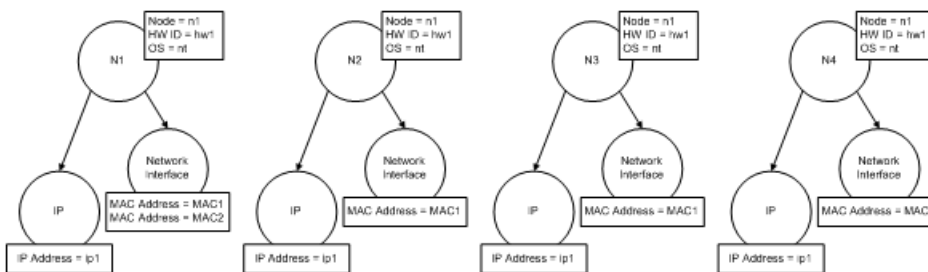


2. The service identifies matching CIs in the CMDB

In this example, the input node matches four nodes in the CMDB having different identification criteria.



3. The service merges the input CI with each matching CI in the CMDB.



4. The service checks for conflicts between the resulting merged CIs.

Nodes N2, N3, and N4 are the same CI; therefore, it is obvious that there is no conflict between them. The only difference between nodes N1 and N2 is the additional MAC address in N1. Since the MAC address match validation criterion uses the **contains** operator, there is no conflict between nodes N1 and N2 either.

Conclusion: There are no conflicts with any of the CMDB matching nodes.

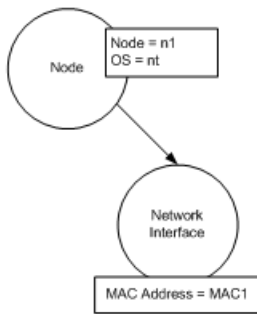
5. **Decision:** The Data-In service merges all of the CIs into one CI.

For details on how the CIs are merged into one CI, see ["Merging Matched CIs Using Reconciliation Priority Rules" on page 753](#).

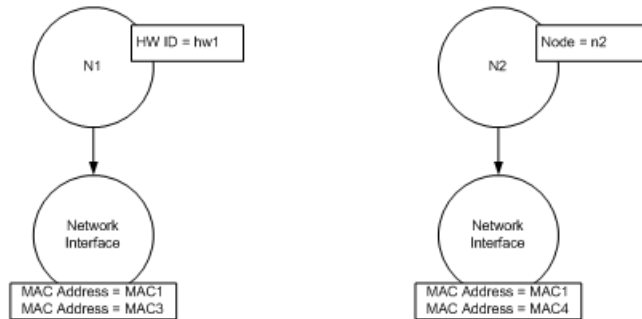
Multiple CI Matching - Example 2

The following example demonstrates how the Data-In service handles multiple CIs with different identification criteria where there are conflicts.

1. The input bulk data is received.

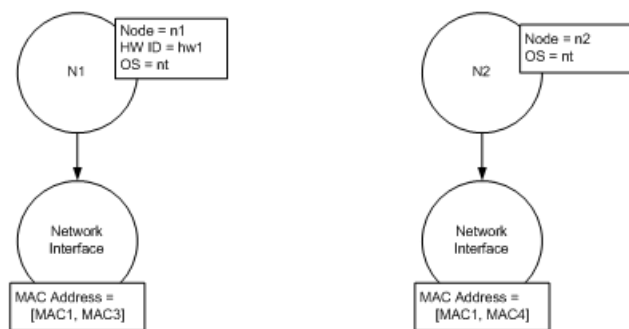


2. The service identifies matching CIs in the CMDB



3. The service merges the input CI with each matching CI in the CMDB.

In this example, the input node matches two nodes in the CMDB having different identification criteria, but there are conflicts with the matching nodes in CMDB: N1 and N2 have conflicting MAC address match criteria.



4. **Decision:** The CIs are not all merged to one CI.

How to Specify High Priority Callers for the Data-In Operations

The UCMDB Server can prioritize the Data-In operations based on the defined list of callers. To define high priority callers, follow the instructions below:

1. Go to **JMX Console > UCMDB:service=Settings Services > setSettingValue**.
2. In the name field, enter **datain.high.priority.callers**.
3. In the **value** field, enter the caller's name.

Note: To specify multiple callers, separate the callers by commas. To remove the setting, leave the value field empty.

4. Click **Invoke**.

Merging Matched CIs Using Reconciliation Priority Rules

During Data In and federation, when a CI is matched with another CI, they need to be merged. Reconciliation priorities, defined using the Reconciliation Priority Manager, are conflict resolution rules that determine how the matched CIs are merged.

This behavior becomes relevant in the following situations:

- **Data In.** The Reconciliation Priority Manager determines whether or not to insert an already existing CI into the CMDB.
- **Federation.** The Reconciliation Priority Manager determines how to handle a CI when multiple data repositories supply the same CI with different values.

To solve this problem, you can define priorities for each data repository to each CIT and attribute.

Note:

- The default value for the **datain.always.update.data.stores** setting is **UCMDB-UI,UCMDB,Enrichment**. A CI updated by any of these datastores will reset the priority to

100 (default). This means that the next merge which has priority greater than 100 will update the CI.

- For attribute type **list of strings**, the Reconciliation Priority engine does not overwrite the existing value of a string list attribute, but rather appending the incoming value(s) to the existing ones.

For details, see ["How to Add Reconciliation Priorities to a CI Type" on page 756](#).

How to Create an Identification Rule

This task describes how to prepare the XML schema for an identification rule.

The identification rule is defined in an XML file. The rule describes the required identification and match criteria for a specific CI type.

When you apply an identification rule to a CI type, it is also applied to each of the CI type's descendants, unless one of them has a identification rule of its own.

You can create an identification rule document from a blank document or use existing information as a basis.

Note: UCMDB is packaged with out-of-the-box identification rules for most usable and problematic CITs, such as node, running software, and so on.

To create an identification rule:

1. Navigate to **Modeling > CI Type Manager**.
2. Click the **Details** tab.
3. In the **Identification** area, in the **Identification** field, select **Advanced identification**, and click **Edit** at the bottom of the **Identification** area.
4. In the Edit Identification Rule dialog box that opens, define identification criteria and match (verification and validation) criteria for the identification rule. For details about the schema elements and attributes, see ["Identification Rule Schema" on page 757](#).

Example of the identification criteria section

```
<identification-criteria>
  <identification-criterion>
    <connected-ci-condition linkType="composition" ciType="interface">
      <overlap-operator match-percent="66"/>
      <attribute-condition autoExcludeThreshold="50" conditionType="approveAndContradict"
includeNullValue="false" attributeName="mac_address"/>
    </connected-ci-condition>
  </identification-criterion>
  <identification-criterion>
    <connected-ci-condition linkType="containment" ciType="ip_address">
      <overlap-operator match-percent="66"/>
      <attribute-condition conditionType="approveAndContradict" includeNullValue="false"
attributeName="ip_lease_time">
        <include-only>
          <value>0</value>
        </include-only>
      </attribute-condition>
      <attribute-condition conditionType="approveAndContradict" includeNullValue="false"
attributeName="authoritative_dns_name"/>
    </connected-ci-condition>
  </identification-criterion>
  <identification-criterion>
    <attribute-condition conditionType="approveAndContradict" includeNullValue="false"
operator="EqualIgnoreCase" attributeName="name"/>
  </identification-criterion>
  <identification-criterion>
    <attribute-condition conditionType="approveAndContradict" includeNullValue="false"
attributeName="snmp_sys_name"/>
  </identification-criterion>
  <identification-criterion>
    <attribute-condition conditionType="approveAndContradict" includeNullValue="false"
attributeName="net_bios_name"/>
  </identification-criterion>
</identification-criteria>
```

In this example:

- A 66% match of **mac_address** from the connected **interface** CI types is required.
- If the number of identification candidates vs the CMDB with the same value of **mac_address** is equal to or greater than 50, then this value is automatically excluded from further identification process.
- The **name** attribute must be the same.
- The **name** attribute is not case sensitive.
- A 66% match of the connected IP addresses is required.
- Both **name** and **routing_domain** of the connected IP address must be the same in order to match.
- The **bios_uuid** attribute must be the same.

- Only one of the identification criteria needs to be fulfilled for the reconciliation engine to find a possible match.

Example of the match criteria section


```
<match>
  <verification-criteria>
    <verification-criterion>
      <attribute-condition attributeName="os_family"/>
    </verification-criterion>
  </verification-criteria>
  <validation-criteria>
    <validation-criterion priority="1">
      <attribute-condition attributeName="bios_uuid"/>
    </validation-criterion>
    <validation-criterion priority="2">
      <connected-ci-condition ciType="interface" linkType="composition">
        <overlap-operator match-percent="66"/>
        <attribute-condition attributeName="mac_address"/>
      </connected-ci-condition>
    </validation-criterion>
    <validation-criterion priority="3">
      <attribute-condition attributeName="name"/>
    </validation-criterion>
  </validation-criteria>
</match>
```


In this example:

- The structure of the conditions is the same as those conditions in the Identification section.
- Only one priority criterion is given in this example, but there may be many criteria with the same priority.

How to Add Reconciliation Priorities to a CI Type

1. Go to the **Data Flow Management > Reconciliation Priority** module.
2. In the CI Types pane, select the CI type.

3. In the CI Type Overrides pane, select an integration and changes its priority by editing the value in the **Priority** field.
4. To set the priority for a specific attribute of that CI type:
 - a. In the Attribute Overrides pane, click **Add** .
 - b. In the Add Attribute dialog box, select the attribute from the list and click **OK**.
5. Select the attribute in the Attribute Overrides pane, and change the value in the **Priority** field.

Note: To reset the attribute to its default value, select the attribute in the Attribute Overrides pane, and click **Reset Attribute** .

6. Click the **Save**  button in the CI Types pane to save your changes.

Identification Rule Schema

Element		Attributes
Name and Path	Description	
identification-config	The parent element for the identification rule document.	<p>Name. description</p> <p>Description. A textual description of the identification rule.</p> <p>Is required. Optional</p> <p>Type. String</p> <hr/> <p>Name. type</p> <p>Description. The CI type to which the identification rule will apply.</p> <p>Is required. Required</p> <p>Type. String</p>
identification-criteria (Identification-config)	The parent element for all the possible identification criteria for the CI type. For details, see "Identification Criteria" on	

Element		Attributes
Name and Path	Description	
	<p>page 743. The identification criteria may contain many identification-criterion elements. Can appear at most once.</p>	
<p>match (Identification-config)</p>	<p>The parent element for all the possible match criteria for the CI type. For details, see "Match Criteria" on page 744. Can appear at most once.</p>	
<p>multiple-match-resolving (Identification-config)</p>	<p>When two or more CIs of the CI type are identified to one another, they may be of any descendant CI type as well. This element states that one of the descendant CI types is preferred over the others. Can appear at most once.</p>	<p>Name. preferred-type Description. Specifies the CI type of the CI that will be preferred when there are multiple matches which cannot be merged. Is required. Optional Type. String</p>
<p>preferred-property (identification-config > multiple-match-resolving)</p>	<p>This element specifies the property value of the CI that will be preferred when there are multiple matches which cannot be merged.</p>	<p>Name. name Description. The name of the property. Is required. Required Type. String</p> <p>Name. value Description. The value of the property. Is required. required Type. String</p> <p>Name. priority Description. The priority of this preferred property. Is required. Optional Type. Integer</p>

Element		Attributes
Name and Path	Description	
identification-criterion (Identification-config > identification-criteria)	This element defines a single identification criterion. The criterion may contain many conditions for identification, and for the criterion to return True , all of them must return True .	<p>Name. targetType</p> <p>Description. Indicates for which CI type this criterion is valid. If this attribute is omitted, then the criterion is applied to any derived type.</p> <p>Is required. Optional</p> <p>Type. String</p> <hr/> <p>Name. isTargetTypeDerived</p> <p>Description. Specifies whether the target type is a derived type of the current CI type.</p> <p>Is required. Optional</p> <p>Type. String</p>
key-attributes-condition (identification-config > identification-criteria > identification-criterion)	This special condition states that the CI type is identified by its key properties and CI type name, and not by any identification criteria. If this condition exists, it should be the only one in the criterion, as well the only criterion in the identification section. Can appear at most once.	
attribute-condition (identification-config > identification-criteria > identification-criterion -OR- identification-config > identification-criteria > identification-criterion > connected-ci-condition -OR- identification-config > match > validation-criteria)	Defines a condition based on an attribute.	<p>Name. attributeName</p> <p>Description. The name of the attribute.</p> <p>Is required. Required</p> <p>Type. String</p> <hr/> <p>Name. autoExcludeThreshold</p> <p>Description. If the number of identification candidates with the same attribute value exceeds this threshold, then that value is automatically</p>

Element		Attributes
Name and Path	Description	
		<p>excluded from the identification process.</p> <p>Is required. Optional</p> <p>Type:</p> <ul style="list-style-type: none"> • Positive integer. • A value of 0 disables this feature.
		<p>Name. masterValue</p> <p>Description. For the purpose of fulfilling the condition, the value defined here is considered equal to any other value.</p> <p>Is required. Optional</p> <p>Type. String</p>
		<p>Name. operator</p> <p>Description. Specifies whether the equality of attribute values should be case sensitive or not. The default is case sensitive.</p> <p>Is required. Optional</p> <p>Type. One of the values: Equals or EqualsIgnoreCase</p>
		<p>Name. includeNullValue</p> <p>Description. Specifies whether a CI should still be considered as a valid value if it has a null (empty) value in the attribute, and the condition will process normally; or is the condition ignored and the reconciliation engine moves to the next criterion. Default value is False</p>

Element		Attributes
Name and Path	Description	
		<p>Is required. Optional</p> <p>Type. Boolean</p> <p>Name. conditionType</p> <p>Type. One of the following values:</p> <p>approveAndContradict condition is used for both approving and contradicting CIs (default).</p> <p>contradictionOnly condition is used to contradict two CIs.</p> <p>approvalOnly condition is used for approving CIs only.</p>
connected-ci-condition (identification-config identification-criteria > identification-criterion -OR- identification-config > match > verification-criteria -OR- identification-config > match)	Defines a condition based on connected CIs. The connected condition may contain attribute conditions. If no attribute conditions exist, the condition matches the connected CI type using its own identification rule.	<p>Name. ciType</p> <p>Description. The type of CI that is assumed to be connected to the CI type to which this rule belongs using the linkType attribute.</p> <p>Is required. Required</p> <p>Type. String</p> <p>Name. linkType</p> <p>Description. The type of link that the ciType attribute uses to connect to the CI type to which this rule belongs</p> <p>Is required. Required</p> <p>Type. String</p> <p>Name. isDirectionForward</p> <p>Description. The direction of the link. Default value is True (from the rule's CI type to ciType).</p> <p>Is required. Optional</p>

Element		Attributes
Name and Path	Description	
		Type. Boolean
overlap-fixed-operator (Identification-config > identification-criteria > identification-criterion > connected-ci-condition)	Defines the fixed number of matches to connected CIs that are needed to fulfill the condition for the connected-ci-condition element to return True. Either this or overlap-operator must exist.	Name. number-of-matches Description. The number of matches. Is required. Required Type. Integer
overlap-operator (Identification-config > identification-criteria > identification-criterion > connected-ci-condition)	Defines the percent of connected CIs (from the total input number of connected CIs) that are needed to fulfill the condition for the connected-ci-condition element to return True. Either this or overlap-fixed-operator must exist.	Name. match-percent Description. The percent of matches. Is required. Required Type. Integer between 1 and 100
verification-criteria (Identification-config > match)	The parent element for all the possible verification criteria for the CI type. For details, see " Match Criteria " on page 744. The verification criteria must contain at least one verification-criterion element. Can appear at most once.	
verification-criterion (Identification-config > match > verification-criteria)	This element defines a single verification criterion. The criterion may contain many conditions for verification.	Name. targetType Description. The derived CI type for which this criterion is valid. If this attribute is omitted, then the criterion is applied to any derived type. Is required. Optional Type. String
		Name. isTargetTypeDerived Description. Specifies whether the target type is a derived type of the current CI type. Is required. Optional

Element		Attributes
Name and Path	Description	
		<p>Type. Boolean</p> <p>Name. numberOfConflictsToFail Identification</p> <p>Description. The number of conflicting conditions that will cause the current criterion to fail. Default Value: 1.</p> <p>Is required. Optional</p> <p>Type. Integer</p>
validation-criteria (Identification-config > match)	The parent element for all possible validation criteria for the CI type. For details, see " Match Criteria " on page 744. The validation criteria must contain at least one validation-criterion element. Can appear at most once.	
validation-criterion (Identification-config > match > validation-criteria)	This element defines a single validation criterion. The criterion may contain many conditions for validation.	<p>Name. priority</p> <p>Description. The criterion's priority.</p> <p>Is required. Required</p> <p>Type. Integer</p> <p>Name. targetType</p> <p>Description. The derived CI type for which this criterion is valid. If this attribute is omitted, then the criterion is applied to any derived type.</p> <p>Is required. Optional</p> <p>Type. String</p> <p>Name. isTargetTypeDerived</p> <p>Description. Specifies whether the target type is a derived type of the current CI</p>

Element		Attributes
Name and Path	Description	
		type. Is required. Optional Type. Boolean
		Name. numberOfConflictsToFail Identification Description. The number of conflicting conditions that will cause the current criterion to fail. Default Value: 1. Is required. Optional Type. Integer

Reconciliation Priority Window

This window enables you to specify the reconciliation priority for a particular integration point, CIT, or attribute.

The Reconciliation Priority Manager provides a centralized location where you can view and change the reconciliation priority for all integration points.

Note: In the Integration Point Pane, you can modify the reconciliation priority for the selected integration point only. For details, see ["Integration Point Pane" on page 346](#).

For details about the reconciliation engine, see ["Data Reconciliation" on page 739](#).

To access	Do one of the following: <ul style="list-style-type: none"> • Select Data Flow Management > Reconciliation Priority. • Select Data Flow Management > Integration Studio, right-click an Integration point and select Reconciliation Priority Manager.
Relevant tasks	<ul style="list-style-type: none"> • "How to Work with Federated Data" on page 317 • "How to Work with Population Jobs" on page 318 • "How to Work with Data Push Jobs" on page 320






User interface elements are described below:

UI Element (A-Z)	Description
Integration	Enables you to select a specific integration point for which to specify the reconciliation priority. Alternatively, you can set priorities for all integration points.
CI Types pane	Lists the CI types and attributes that are supported by the selected integration point. See below for more details.
Reconciliation Priority Overrides pane	Lists all integration points that contain the selected CI Type , and the priority overrides for the selected CI types, if any. See below for more details.

CI Types pane


This pane lists the CI types and attributes that are supported by the selected integration point.

Note: If there is a manual override on an item in the tree, that item and all its parent items are displayed with an asterisk next to the CI type.


UI Element (A-Z)	Description
	Expands/collapses the entire hierarchical tree structure.
Tree View 	Click Tree View to select the display format of the CI types tree. The following options are available: <ul style="list-style-type: none"> • Display label • Class name • Legacy class name
	Toggles the display of the legend at the bottom of the CI Types pane.
	Saves the changes to the priority override settings.
	Filters the tree to display only those CI types that have reconciliation priority overrides, and their parents.

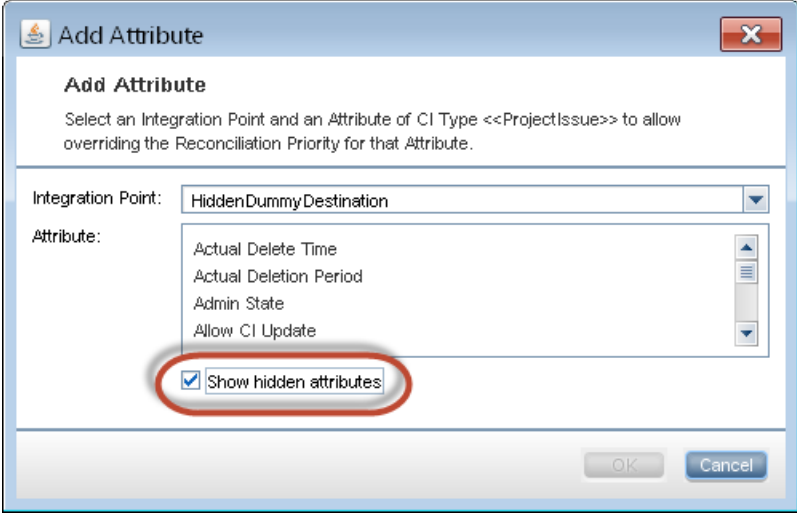


Reconciliation Priority Overrides Pane

CI Type Overrides Area

UI Element (A-Z)	Description
Inherited From	The name of the CI type from which the priority level is inherited.
Integration Name	The name of the integration point for which the override is defined.
Priority	<p>Displays the priority that is assigned to a particular CI Type. This value can range from -1,000,000 to 1,000,000. The default priority level for all items is 100. If you change the priority of an entry, the new value propagates downwards to all descendants of that particular CI type.</p> <p>To change the priority of a CI type, do the following:</p> <ul style="list-style-type: none"> • Click the Priority field and enter a new value. • Press Enter. • Click  in the CI Types pane.

Attribute Overrides Area

UI Element (A-Z)	Description
	<p>Opens the Add Attribute dialog box, enabling you to select attributes for which you want to set overrides.</p> <ul style="list-style-type: none"> • Integration Point. Displays a list of all defined integration points. Select the integration point for which you want to change an attribute's priority. If an integration point is selected, only attributes for this integration point can be added to the list. • Attribute. Enables you to select an attribute for which you want to specify a priority override. To view the hidden attributes among this list, select the Show hidden attributes check box.

UI Element (A-Z)	Description
	 <p>Note: Hidden attributes are not marked as Visible in the Attributes pane of the CI Type Manager. For details, see Attributes Page in the <i>Universal CMDB Modeling Guide</i>.</p>
	<p>Resets the value of the selected attribute to its default value.</p> <p>Note: If you reset the priority for an attribute, and this priority is not overridden in any parent of this CIT, the attribute override row is removed from the list, and the value is restored to 100. If a parent of this CIT does have an attribute override for this attribute, the value is set to the parent's value.</p>
Attribute	The name of the attribute for which you are specifying a priority override.
Inherited From	The name of the CI type from which the priority level is inherited.
Integration Name	The name of the integration point for which the override is defined.
Priority	<p>Displays the priority that is assigned to a particular attribute. This value can range from -1,000,000 to 1,000,000. The default priority level for all items is 100. If you change the priority of an entry, the new value propagates downwards to all descendants of that particular CI type.</p> <p>Note: When you change the priority, you must click  in the CI Types pane to save your changes.</p>

How to Add Reconciliation Priority for API-based Integrations

1. Add **dataStoreOrigin** parameter for the UCMDB user used by the API integration.
 - a. 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. (Default user name: **sysadmin**)
 - b. Locate **UCMDB:service=URM Services** and click the link to jump to the Operations table.
 - c. Locate and invoke the **listResources** operation with the following parameter values:
customerID: Enter your customer ID (default: **1**)
resourceType: Auth_USER
 - d. On the returned result page, select the user (for example, **admin**) used by the API integration.
 - e. In the Resource XML window, add the following to the `xmlAuthUser` definition tag:

```
dataStoreOrigin="AnyValue"
```
 - f. Click **Save resource**.
2. Go to **UCMDB UI > Data Flow Management > Integration Studio**, and create an integration point based on the UCMDB API Population adapter. Set the same integration name to the user **dataStoreOrigin**.
3. In the Integration Studio module, right-click the integration point you just created, select **Reconciliation Priority Manager** and define the priorities.

For detailed instructions, see ["How to Add Reconciliation Priorities to a CI Type" on page 756](#) and ["Reconciliation Priority Window" on page 764](#).

Note: In `cmdb.reconciliation.audit.log`, the API bulks will be logged with the new context:

```
INFO [qtp1666398047-387] - [ID=1556106913] [Customer ID=1] [Changer=AnyValue:
User:admin,LoggedInUser:admin] [total= 0.267]
```


How to Enable Redundant Reverse Check

During Reconciliation DataIn, when sending a CI with valid link information from Probe to UCMDB Server, the identification required link is redundant. If there is no other valid identification data, the CI would fail to identify itself and could not be reconciled to the server.

The redundant reverse check is introduced so that you can reverse the action of making identification required link redundant for such CIs, and then have them sent to the UCMDB server when the CIs have no enough data to identify themselves.

To enable redundant reverse check, simply add `isReverseCheck="true"` in the discovery job adapter source (default value: **false**). To do so,

1. In UCMDB UI, from the **Data Flow Management > Universal Discovery** module, locate the desired discovery job, right-click the job and select **Go to Adapter**.
2. Right-click the adapter in the Resources pane and select **Edit adapter source**.

The Adapter Source Editor opens.

3. In the Adapter Source Editor, locate the `resultMechanism` tag.
4. Add `isReverseCheck="true"` to the `resultMechanism` tag as follows:

```
<resultMechanism isEnabled="true" isReverseCheck="true">
```

5. Click **Save**.

How to Enable Attribute Name Verification during the Matching Phase of Identification

The **reconciliation.match.attributes** JMX setting verifies names of attributes during the matching phase of the identification process. If, compared to the other CI, there is a different value among the CI attribute values defined in this setting, the verification process stops and the match is rejected.

Only the attributes that are inherited from the Managed Object should be used in this setting (for example, **global_id** and **name**). Names of the attributes specified in the setting should be separated by comma.

This setting applies only to CIs that are identified based on the Identification Rule.

The following example explains how this setting works:

- If you have two node CIs:
 - Node1 with **global_id=g1** and **name=n**
 - Node2 with **global_id=g2** and **name=n**
 - **reconciliation.match.attributes** set to **global_id**

This scenario will result in the two nodes not matching.

- If Node1 does not have **global_id** set, the two CIs will match.

To enable this setting, do the following:

1. Go to **JMX Console > UCMDB:service=Settings Services > setSettingValue**.
2. In the **name** field, enter **reconciliation.match.attributes**.
3. In the **value** field, enter names of the CI attributes, separated by comma.

Note: To disable this setting, leave the **value** field empty.

4. Click **Invoke**.

How to Modify the Maximum Number of Threads for the Data-In Service

Since UCMDB 10.30, the Data-In service can process multiple CI buckets concurrently if they do not intersect based on their identification. If two CIs from two buckets are identified with each other, then the Data-In service processes the two buckets sequentially.

By default, the Data-In service can process four CI buckets concurrently. You can modify this number according to the server's capability: increase the number if the server is powerful and decrease the number if otherwise.

To modify the maximum number of threads for the Data-In service, follow these steps:

1. Extract the **<UCMDB_Server_Home>\lib\reconciliation.jar\services\reconciliation\service-config.xml** file to the following folder:

<UCMDB_Server_Home>\conf\service-config\services\reconciliation

2. Locate the following section in the extracted **service-config.xml** file:

```
<task-config total-threads-num="4" max-queue-size="30">  
  <manager-creation>  
    <manager-factory-class-name>com.hp.ucmdb.reconciliation.datain.manager.DataInManagerFactory</manager-factory-class-name>  
  </manager-creation>  
</task-config>
```

3. Modify the value of `total-threads-num` from 4 to your desired value, and then save the file.

Note: The recommended values are from 1 to 8.

4. Restart the UCMDB server.

How to Enable CI Type Tenant Owner Verification during the Matching Phase of Identification

You can dynamically add a verification criterion based on the **TenantOwner** attribute during the matching phase of the identification process for CIs by using the new JMX setting **reconciliation.tenantaware.citypes**. If, compared to the other CI, there is a different value among the CI attribute values defined in this setting, the verification process stops and the match is rejected.

The following example explains how this setting works:

- If you have two node CIs:
 - Node1 with **TenantOwner**=t1 and **name**=n
 - Node2 with **TenantOwner**=t2 and **name**=n
 - **reconciliation.tenantaware.citypes** set to **node**

This scenario will result in the two nodes not matching.

- If Node1 does not have **TenantOwner** set, the default Tenant will be provided.

Note: If you add a node CIT, UNIX for example, you do not have to add it since it is inherited by identification rule. Only if you change the UNIX CIT identification rule, you need to add it explicitly.

To enable TenantOwner attribute verification for CITs that are identified by key attributes,

1. Add the **ID_ATTRIBUTE** qualifier for the **TenantOwner** attribute of the **managed_object** CIT.

Note: The **TenantOwner** attribute will be inherited to all the child classes. Make sure that a child class does not override it.

- a. Go to the **JMX console > UCMDB:service=URM Services**.
- b. Invoke the **listResourceTypes** method.
- c. On the returned page, click **CM_CLASS**, then click **managed_object**.
- d. In the Resource XML box, add the following attribute qualifier to the **TenantOwner** attribute:

```
<Attribute-Qualifier name="ID_ATTRIBUTE" is-factory="true" is-user-  
modified="true" version="15" >  
  <Data-Items/>  
</Attribute-Qualifier>
```

- e. Click **Save resource**.
2. Invoke the JMX method **updateClassModel** to update the class model (go to the **JMX console > UCMDB:service=Class Model Services**, and invoke the **updateClassModel** method with **1** in the **Value** field for customerID).
 3. Reload the class model from persistency (go to the **JMX console > UCMDB:service=Class Model Services**, and invoke the **reloadClassModelFromPersistency** method).
 4. Go to **JMX console > UCMDB:service=Model Services**, invoke the **recalculateID** method with **classname** field empty.

This may take a while as it updates the calculated IDs for all instances of the classes with key attributes identification.

To enable the reconciliation.tenantaware.citypes setting for specific CITs (separated by comma) that are identified based on identification rules,

1. Go to **JMX Console > UCMDB:service=Settings Services > setSettingValue**.
2. In the **name** field, enter **reconciliation.tenantaware.citypes**.
3. In the **value** field, enter names of the CITs, separated by comma.

Note: To disable this setting, leave the **value** field empty.

4. Click **Invoke**.

To enable the `reconciliation.tenantaware.citypes` setting for all the CITs that are identified based on identification rules,

1. Go to **JMX Console > UCMDB:service=Settings Services > setSettingValue**.
2. In the **name** field, enter **`reconciliation.tenantaware.citypes`**.
3. In the **value** field, enter *****.
4. Click **Invoke**.

Note:

- If you changed the Tenant ID on the Data Flow Probe, make sure you clear the probe cache as well by performing either of the following:
 - Log in to the probe server, run the following script:
Windows: `hp\UCMDB\DataFlowProbe\tools\clearProbeData.bat`
Linux: `hp\UCMDB\DataFlowProbe\tools\clearProbeData.sh`
 - Log in to the UCMDB server UI, go to **Data Flow Management > Universal Discovery > Discovery Modules/Jobs**. For each of the jobs that run on the probe, right-click the job and select **Clear Probe Results Cache**.
- In a multi-tenant aware environment, a tenant must be specified for the Data Flow Probe.

Tenant Owner Related Known Issues, Problems, and Workaround

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

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

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

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

1. Remove the **ID_ATTRIBUTE** qualifier for the **TenantOwner** attribute on the **managed_object** CIT.
2. Remove the value of the **reconciliation.tenantaware.citypes** setting.
3. Reload the class model from persistency (go to the **JMX console > UCMDB:service=Class Model Services**, and invoke the **reloadClassModelFromPersistency** method).
4. Go to **JMX console > UCMDB:service=Model Services**, invoke the **recalculateID** method with **classname** field empty.
5. Go to **JMX console > UCMDB:service=Model Services**, invoke the **updateClasModel** method.

LIMITATION: Enrichment is not invoking the Reconciliation on Update **OwnerTenant** via **Associate Tenant Rule**. As a result, you may have duplicated data in the system in case if you update the **OwnerTenant**'s CI to a tenant that already has this CI.

Workaround: None.

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

Workaround: None.

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

Workaround: None.

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

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

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

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

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

Appendix A: Troubleshooting and Limitations – Data Flow Management

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

- ["Troubleshooting – Universal Discovery" below](#)
- ["Limitations – Universal Discovery" on page 782](#)

Note:

- For details on using log files to perform basic troubleshooting, see:
 - ["Data Flow Probe Log Files" on page 99](#)
 - Log Files in the *Universal CMDB Administration Guide*

Troubleshooting – Universal Discovery

- ["Discovery Results Do Not Appear in the Topology Map" below](#)
- ["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 778](#)
- ["TCP Ports" on page 778](#)
- ["Discover Resources on a Windows XP Machine" on page 778](#)
- ["Trigger CIs for jobs in a management zone are in continuous "Progress" status" on page 778](#)
- ["Device attributes are not populating or contain unexpected or null values" on page 779](#)
- ["Inventory Discovery by Scanner job fails" on page 779](#)

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:\hp\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 *Universal CMDB Modeling Guide*.

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.

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:
 - o **forceRefreshAll**. This method loads the log files for both AM and SM integration jobs.
 - o **listAMIntegrationJobByName**. This method loads the log files for AM integration jobs.
 - o **listSMIntegrationJobByAdapterName**. This method loads the log files for SM integration jobs.

Note:

- o 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.
- o 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.
- o 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
getSMIntegrationJobDetails	This method displays the detailed information of the SM integration job that has the specified index. You must invoke listSMIntegrationJobByAdapterName or forceRefreshAll in the previous step.
getAMIntegrationJobDetailsByName	This method displays the detailed information of the AM integration job that has the specified query name and index. You must invoke listSMIntegrationJobByAdapterName or forceRefreshAll in the previous step.
getAMIntegrationJobDetails	This method displays the detailed information of the AM integration job that has the specified index. You must invoke listSMIntegrationJobByAdapterName or forceRefreshAll 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 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).

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 Data Flow Management Guide (Universal CMDB 10.33)

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.

We appreciate your feedback!