HP Business Service Management

for the Windows and Linux operating systems

Software Version: 9.13

RTSM Data Flow Management

Legal Notices

Documentation Updates

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

• Software Version number, which indicates the software version.

• Document Release Date, which changes each time the document is updated.

• Software Release Date, which indicates the release date of this version of the software.

To check for recent updates, or to verify that you are using the most recent edition of a document, go to:

http://h20230.www2.hp.com/selfsolve/manuals

This site requires that you register for an HP Passport and sign-in. To register for an HP Passport ID, go to:

http://h20229.www2.hp.com/passport-registration.html

Or click the **New users - please register** link on the HP Passport login page.

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

Support

Visit the HP Software Support web site at:

http://www.hp.com/go/hpsoftwaresupport

This web site provides contact information and details about the products, services, and support that HP Software offers.

HP Software online support provides customer self-solve capabilities. It provides a fast and efficient way to access interactive technical support tools needed to manage your business. As a valued support customer, you can benefit by using the support web site to:

- Search for knowledge documents of interest
- Submit and track support cases and enhancement requests
- Download software patches
- Manage support contracts
- Look up HP support contacts
- Review information about available services
- Enter into discussions with other software customers
- Research and register for software training

Most of the support areas require that you register as an HP Passport user and sign in. Many also require a support contract. To register for an HP Passport ID, go to:

http://h20229.www2.hp.com/passport-registration.html

To find more information about access levels, go to:

http://h20230.www2.hp.com/new_access_levels.jsp

Table of Contents

PART II: DATA FLOW MANAGEMENT SETUP

PART III: INTEGRATION

PART IV: DISCOVERY

PART V: RECONCILIATION

PART VI: HARDENING

Table of Contents

Welcome to This Guide

This guide describes the applications that enable data flow management. These applications include the Integration Studio and Discovery.

For details on working with DFM content, see the *HP Universal CMDB Discovery and Integration Content Guide* PDF. This book is available on the HP Software Product Manuals Web site (http://h20230.www2.hp.com/selfsolve/manuals) under the Universal CMDB (Application Mapping) product.

This chapter includes:

➤ How This Guide Is Organized on page 13

➤ Who Should Read This Guide on page 14

➤ How Do I Find the Information That I Need? on page 15

➤ Additional Online Resources on page 17

➤ Documentation Updates on page 18

How This Guide Is Organized

The guide contains the following parts:

Part I   Introduction

Describes the components of Data Flow Management, including the Integration Studio and discovery. Describes RTSM licensing policies and Data Flow Probe installation.

Part II   Data Flow Management Setup

Describes how to set up HP Business Service Management to discover components running in your environment.

Part III   Integration

Explains how to define adapters to include data in the RTSM from other sources.

Part IV   Discovery

Describes how to activate jobs that discover the components of your system

Part V   Reconciliation

Explains how to match and identify entities from different data repositories.

Part VI   Hardening

Explains how to harden Data Flow Management and the Data Flow Probe and how to configure SSL with your BSM platform and Data Flow Probe.

Who Should Read This Guide

This guide is intended for the following users of HP Business Service Management:

➤ HP Business Service Management administrators

➤ HP Business Service Management platform administrators

➤ HP Business Service Management application administrators

➤ HP Business Service Management data collector administrators

Readers of this guide should be knowledgeable about enterprise system administration, have familiarity with ITIL concepts, and be knowledgeable about BSM in general and the Operational Database technology specifically.

How Do I Find the Information That I Need?

This guide is part of the HP BSM Documentation Library. This Documentation Library provides a single-point of access for all BSM documentation.

You can access the Documentation Library by doing the following:

➤ In BSM, select **Help** > **Documentation Library**.

➤ From a BSM Gateway Server machine, select **Start** > **Programs** > **HP Business Service Management** > **Documentation**.

Topic Types

Within this guide, each subject area is organized into topics. A topic contains a distinct module of information for a subject. The topics are generally classified according to the type of information they contain.

This structure is designed to create easier access to specific information by dividing the documentation into the different types of information you may need at different times.

Three main topic types are in use: **Concepts**, **Tasks**, and **Reference**. The topic types are differentiated visually using icons.

Topic Type	Description	Usage
Concepts	Background, descriptive, or conceptual information.	Learn general information about what a feature does.
Tasks	**Instructional Tasks.** Step-by-step guidance to help you work with the application and accomplish your goals. Some task steps include examples, using sample data. Task steps can be with or without numbering: ➤ **Numbered steps.** Tasks that are performed by following each step in consecutive order. ➤ **Non-numbered steps.** A list of self-contained operations that you can perform in any order.	➤ Learn about the overall workflow of a task. ➤ Follow the steps listed in a numbered task to complete a task. ➤ Perform independent operations by completing steps in a non-numbered task.
	Use-case Scenario Tasks. Examples of how to perform a task for a specific situation.	Learn how a task could be performed in a realistic scenario.

Topic Type	Description	Usage
Reference	**General Reference**. Detailed lists and explanations of reference-oriented material.	Look up a specific piece of reference information relevant to a particular context.
	User Interface Reference. Specialized reference topics that describe a particular user interface in detail. Selecting **Help on this page** from the Help menu in the product generally open the user interface topics.	Look up specific information about what to enter or how to use one or more specific user interface elements, such as a window, dialog box, or wizard.
Troubleshooting and Limitations	**Troubleshooting and Limitations**. Specialized reference topics that describe commonly encountered problems and their solutions, and list limitations of a feature or product area.	Increase your awareness of important issues before working with a feature, or if you encounter usability problems in the software.

Additional Online Resources

Troubleshooting & Knowledge Base accesses the Troubleshooting page on the HP Software Support Web site where you can search the Self-solve knowledge base. Choose **Help** > **Troubleshooting & Knowledge Base**. The URL for this Web site is http://h20230.www2.hp.com/troubleshooting.jsp.

HP Software Support accesses the HP Software Support Web site. This site enables you to browse the Self-solve knowledge base. You can also post to and search user discussion forums, submit support requests, download patches and updated documentation, and more. Choose **Help** > **HP Software Support**. The URL for this Web site is www.hp.com/go/hpsoftwaresupport.

Most of the support areas require that you register as an HP Passport user and sign in. Many also require a support contract.

To find more information about access levels, go to:

http://h20230.www2.hp.com/new_access_levels.jsp

To register for an HP Passport user ID, go to:

http://h20229.www2.hp.com/passport-registration.html

HP Software Web site accesses the HP Software Web site. This site provides you with the most up-to-date information on HP Software products. This includes new software releases, seminars and trade shows, customer support, and more. Choose **Help** > **HP Software Web site**. The URL for this Web site is www.hp.com/go/software.

Documentation Updates

HP Software is continually updating its product documentation with new information.

To check for recent updates, or to verify that you are using the most recent edition of a document, go to the HP Software Product Manuals Web site (http://h20230.www2.hp.com/selfsolve/manuals).

Part I

Introduction

1

Introduction to Data Flow Management

This chapter includes:

Concepts

➤ Data Flow Management Overview on page 22

➤ Data Flow Management Architecture on page 27

➤ Data Flow Management Concepts on page 28

Tasks

➤ How to Receive Bulk Data from SiteScope on page 34

Reference

➤ Naming Conventions on page 35

Troubleshooting and Limitations on page 35

Concepts

🔵 Data Flow Management Overview

This section includes the following topics:

➤ "RTSM Integrations" on page 22

➤ "Discovery" on page 23

➤ "Data Flow Management Modules" on page 24

➤ "Reconciliation" on page 26

RTSM Integrations

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

An integration type can be:

➤ **Population.** Integration that populates the RTSM 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 RTSM 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.

For details, see "Integration Studio" on page 249.

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 applications, databases, 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 do not need to install any agents on the devices to be discovered.

Following installation, the network on which the RTSM Data Flow Probe is located, the host on which the Probe resides, and the host's IP address are automatically discovered and a CI is created for each of these objects. These discovered CIs populate the CMDB. They act as triggers that activate a Discovery job. 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.

Once you configure Discovery and activate the required discovery jobs, Discovery runs on the system, discovers system components, and saves them as CIs in the CMDB. You can discover new objects manually or automatically. Objects that are outside the Probe's network require additional, manual configuration.

For details on discovering and integrating components on your system, see the *HP Universal CMDB Discovery and Integration Content Guide* PDF. This book is available on the HP Software Product Manuals Web site (http://h20230.www2.hp.com/selfsolve/manuals) under the Universal CMDB (Application Mapping) product.

Note: This guide assumes that the RTSM Data Flow Probe is installed in the default location, **C:\hp\UCMDB\DataFlowProbe**.

Data Flow Management Modules

Note for HP Universal CMDB Configuration Manager users: The Data Flow Management modules are available only when you are logged into UCMDB in **Actual** state.

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

➤ "Integration Studio" on page 24
➤ "Discovery Control Panel" on page 25
➤ "Data Flow Probe Setup" on page 25
➤ "Reconciliation Priority" on page 25
➤ "Adapter Management" on page 25
➤ "DDM Community" on page 25
➤ "Data Flow Probe Status" on page 26

Integration Studio

The Integration Studio module enables you to set up BSM integrations to define and control data flows from external data repositories to the RTSM, or from the RTSM to external data repositories.

For details, see "Integration Studio" on page 249.

Discovery Control Panel

The Discovery Control Panel application module enables you to manage the Discovery process to discover the CIs and relationships of your IT infrastructure. You control the process by 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 details, see "Discovery Control Panel" on page 323.

Data Flow Probe Setup

The Data Flow Probe Setup module enables you to add Probes to the system and to edit existing Probes. You define the network range that each Probe covers. From the Data Flow Probe Setup you also manage credentials. The credentials are used for both Discovery and Integrations purposes.

For details, see "Data Flow Probe Setup" on page 93.

Reconciliation Priority

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

For details, see "Reconciliation Priority" on page 455.

Adapter Management

The Adapter Management module enables you to edit adapters, scripts, and configuration files. You can also replace or remove external resources needed in Discovery or Integration.

For details, see "Adapter Management" on page 169.

DDM Community

The DDM Community Web site provides you with a convenient way to obtain the latest Discovery and Integration Content Pack. You need an HP Passport user name and password to log in. The URL for this Web site is: https://h20090.www2.hp.com/.

For details, see "DDM Community" on page 245.

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. You can also view the report results in a MyBSM portlet.

For details, see "Data Flow Probe Status" on page 235.

Reconciliation

The Reconciliation process consists of two important steps:

➤ **Identification**. The process by which CIs and relationships within the RTSM are identified against existing CIs within the RTSM, other CIs within the same bulk, or CIs coming from various federated data sources.

➤ **Reconciliation Priority**. The process by which the RTSM reconciliation engine decides how to deal with conflicting data. When conflicting values are given for the same CI attribute by different integrations, the RTSM 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 RTSM reconciliation engine uses the last reported value as the most accurate; all integrations have exactly the same priority.

For details about reconciliation, see "Reconciliation" on page 429.

For details about the Reconciliation Priority Manager, see "Reconciliation Priority Window" on page 465.

🍀 Data Flow Management Architecture

Data Flow Management architecture is deployed as follows:
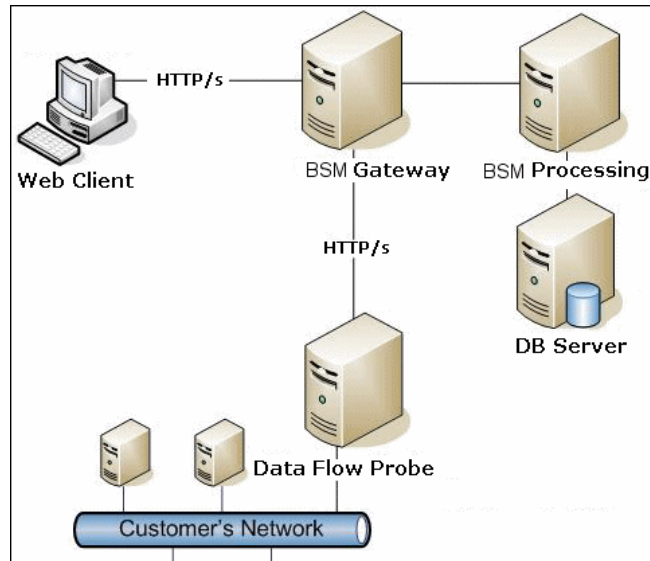
➤ The Data Flow Probe is responsible for the data flow to and from external data repositories (data push or population) and for performing discovery. Federation is always run directly from the RTSM Server and does not leverage the Probe infrastructure. Generally, data push runs from the RTSM Server, but uses the Probe in cases where the adapter is based on the Data Push Adapter platform.

➤ The Data Flow Probe initiates communication with the RTSM Server using http or https traffic, enabling the product to bypass possible firewalls.

➤ If Data Flow Probe is used only for data synchronization between BSM and CMS or between two BSMs and not for Discovery, it can reside on the BSM gateway machine. If there are several gateway machines, one of the gateways can be chosen to run the Data Flow Probe.

🎲 **Data Flow Management Concepts**

This section describes the main topics of Data Flow Management:

➤ "Data Flow Probe" on page 28

➤ "Communication Protocols" on page 28

➤ "Discovery and Integration Adapters" on page 29

➤ "Discovery Modules" on page 31

➤ "Discovery and Integration Content Packs" on page 31

➤ "Integration Points" on page 31

➤ "Discovery Jobs" on page 32

➤ "Discovery Wizards" on page 32

➤ "Agentless Discovery" on page 32

➤ "Trigger CIs and Trigger Queries" on page 33

Data Flow Probe

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

Communication Protocols

Discovery of the IT infrastructure components uses protocols such as SNMP, WMI, JMX, Telnet, and so on. For details, see "Domain Credential References" on page 103.

Discovery and Integration Adapters

An adapter can be of one of the following types:

➤ **Jython Adapter**. An adapter based on a set of Jython scripts that are executed sequentially. For details, see "How to Create Jython Code" in the *RTSM Developer Reference Guide*.

➤ **Java Adapter**. An adapter based on Java code that implements the various DFM interfaces and is wrapped in a JAR file. For details, see "Developing Java Adapters" in the *RTSM Developer Reference Guide*.

➤ **Generic DB Adapter**. An adapter that uses SQL queries and maps database tables to CIs and relationships by using an ORM file. For details, see "Developing Generic Database Adapters" in the *RTSM Developer Reference Guide*.

➤ **Generic Push Adapter.** An adapter that uses a mapping file and Jython scripts to push data to an external data repository. For details, see "Developing Push Adapters" in the *RTSM Developer Reference Guide*.

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 and set up 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 attached to the Discovery Jobs; for integration adapters, the information is being 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 206. For details on creating adapters, see "Adapter Development and Writing" in the *RTSM Developer Reference Guide*.

Input Queries

Note: Input queries refer only to Discovery-based integrations.

Each adapter is assigned an Input query that is used for two functions:

➤ **The Input query defines a minimal set of requirements** for every Trigger CI included in a job or integration 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. 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 RTSM.** 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, in the Triggered CI Data pane. For details, see "Input Pane" on page 192.

For details on using input queries when writing adapters, see "Step 1: Create an Adapter" in the *RTSM 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 choose a module for it 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.

Discovery and Integration Content Packs

The latest Discovery and Integration content for RTSM is delivered as a Content Pack available for download via the HP Live Network. For details on downloading and installing Content Packs, see "DDM Community" on page 245.

By downloading the latest Content Pack, you ensure that your system is up to date with the latest defect fixes and content functionality. Content Packs are released in a separate release train and are installed on top of the current product platform.

Integration Points

Integration points are entities used to set up RTSM 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 249.

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 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.

For details, see "Discovery Control Panel" on page 323.

Discovery Wizards

You use one of the Discovery wizards (to discover the infrastructure, databases, and J2EE applications) when you need to use the default values set for IP ranges, network credentials, and so on. For details on using a wizard, see "Basic Mode Window" on page 354.

Agentless Discovery

Discovery is an agentless technology that discovers IT environment components through a dedicated RTSM Data Flow Probe residing on the customer's site.

Although Discovery is agentless, it does not require the installation of dedicated agents on the servers that are to be discovered, but it depends on 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, see "Domain Credential References" on page 103.

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.

For details on adding Trigger CIs to a job, see "Discovery Status Pane" on page 372.

A Trigger query associated with a job is a subset of the Input query, and defines which specific CIs should automatically trigger a job. 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.

Tasks

🔧 How to Receive Bulk Data from SiteScope

SiteScope results can be sent to BSM zipped or unzipped. The request includes a parameter that indicates to BSM whether the results being sent are in zipped or unzipped format.

To send SiteScope results in a zipped format:

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

2 Locate the line beginning **appilog.agent.probe.send.results.zipped**.

3 Change the value to **true**.

4 Restart the Probe so that it is updated with the changes.

   SiteScope results are zipped before being sent to BSM.

Reference

🔖 Naming Conventions

When naming entities in Data Flow Management, you can use the following characters: a-z, A-Z, 0-9. When entering IP addresses, use only digits and asterisks (*).

🔍 Troubleshooting and Limitations

For details on using the log files to perform basic troubleshooting, see:

➤ "Data Flow Probe Log Files" on page 132

➤ "Data Flow Management Log Files" in the *RTSM Administration Guide*

This section includes the following topics:

➤ "Discovery Results Do Not Appear in the Topology Map" on page 35

➤ "Networks and IPs" on page 36

➤ "TCP Ports" on page 36

➤ "Discover Resources on a Windows XP Machine" on page 36

➤ "Limitations" on page 37

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 RTSM cannot retrieve the data or build the query results. Check the Statistics 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**.

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.

Limitations

➤ When Discovery is installed on a non-English operating system, job and module names are still limited to English characters.

➤ 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).

In general, you should refrain from making changes to out-of-the-box resources. If you must do so, be sure to track your changes so that they can be re-applied after you install a Content Pack. Important general fixes (not specific to your environment) should be sent to CSO so that they can be analyzed and included as part of one of the next Content Packs.

2

Licensing Models for Run-time Service Model

This chapter includes:

Concepts

➤ Licensing Model – Overview on page 40

➤ UCMDB Foundation License on page 42

➤ UCMDB Integration Only License on page 45

➤ DDM Advanced Edition License on page 46

Tasks

➤ How to Upgrade to the Integration Only or DDM Advanced Edition License on page 48

Reference

Troubleshooting and Limitations on page 49

Concepts

Licensing Model – Overview

HP Universal CMDB's licensing model is based on three complementary types of license, or licensing levels. The first one, known as the UCMDB Foundation License, is granted free of charge to eligible customers. The other two levels (the UCMDB Integration Only License and the DDM Advanced Edition License) are fee based.

This section includes the following topics:

➤ "Licensing Levels" on page 40

➤ "Units of Measure" on page 41

Licensing Levels

➤ **UCMDB Foundation License**

This license grants the rights to use UCMDB as the backbone component of select BTO products.

➤ **UCMDB Integration Only License**

This license grants the right to integrate third-party (non-HP) products with UCMDB using various types of integrations.

➤ **DDM Advanced Edition License**

This license grants the rights to:

➤ Use all Discovery and Dependency Mapping (DDM) capabilities to populate UCMDB

➤ Integrate BTO and third-party (non-HP) products with UCMDB, using any type of integration

The following table provides an overview of what is permitted with the various licenses:

License/Integration	Integrations with other BTO products	Integrations with third-party products	Custom Discovery-like integrations	All Discovery capabilities
UCMDB Foundation	Permitted	No	No	No
UCMDB Integration Only	Permitted	Permitted	No	No
DDM Advanced Edition	Permitted	Permitted	Permitted	Permitted

Units of Measure

➤ **OS Instance**

Each implementation of the bootable program that can be installed onto a physical system or a partition within the physical system. A physical system can contain multiple Operating System instances.

➤ **Managed Server**

A computer system or computer system partition where a bootable program is installed, but not including personal computers or computers primarily serving a single individual.

Note: Printers and network devices are not counted as Managed Servers.

UCMDB Foundation License

This is a no charge entitlement license for the UCMDB product, which is automatically granted to any HP customer who purchases HP Discovery and Dependency Mapping (DDM), HP Service Manager (SM), or HP Asset Manager (AM).

This section also includes:

Standard BTO Integrations

With this license, you are entitled to integrate the following BTO products with UCMDB:

➤ HP Business Service Management

➤ HP Universal CMDB

➤ HP Asset Manager

➤ HP Service Manager

➤ HP DDM Inventory

➤ HP Network Node Manager

➤ HP Storage Essentials

➤ HP Systems Insight Manager

Data flows between these products are implemented by means of adapters provided out-of-the-box with HP Universal CMDB or bundled under the SACM solution. Most adapters can leverage the Data Flow Probe infrastructure of HP Universal CMDB - except those supporting a federation data flow or the push data flow from UCMDB to SM, due to a technical restriction.

Note: The data flow from UCMDB to Asset Manager relies on a Connect-It connector, which is licensed free of charge to AM customers.

The right granted by the UCMDB Foundation license to integrate BTO products with UCMDB does not remove the need for customers to properly license these products in the first place.

Other Integrations

With this license, you are also entitled to integrate BTO products with UCMDB using:

➤ Standard integrations provided by HP partners (additional charges may apply)

➤ Custom data exchange integrations (the Generic DB Adapter, the Generic Push Adapter and customer-developed Java adapters)

➤ The HP Universal CMDB Web Service API and the HP Universal CMDB API (Java)

Number of CIs and Relationships

The UCMDB Foundation License does not restrict the number of CIs and relationships that can be stored in UCMDB or exchanged between UCMDB and other BTO products. The only limitation is physical capacity and performance.

Number of UCMDB Instances

The UCMDB Foundation License does not restrict the number of UCMDB instances that can be deployed in a customer environment for the purpose of implementing development, test, production, HA and/or DR platforms. However, technical limitations may apply regarding how data can be managed and exchanged in a multi-instance installation. Servers that are discovered with DDM or sourced from a third-party product only need to be counted once under the DDM Advanced Edition license or the UCMDB Integration Only license, even if they appear in several UCMDB instances for the purpose of operational management.

Number of Data Flow Probe instances

The UCMDB Foundation License does not restrict the number of Data Flow Probe instances that can be deployed in a customer environment for the purpose of hosting discovery or integration adapters. However, technical limitations may apply regarding the maximum number of probes that can be used with UCMDB. Also, as mentioned above, some adapters cannot be hosted by a probe.

Particular Case of BSM

Customers who purchase HP Application Performance Manager (APM) version 9.0x or later are automatically granted a no-charge license to use the embedded UCMDB component labeled as Run-time Service Model (RTSM) and to integrate BTO products with RTSM. As a result, APM customers do not have and do not need a UCMDB Foundation license.

Note: APM was formerly known as HP Business Availability Center version 8.0x (BAC) and RTSM as the Operational Database (ODB).

UCMDB Integration Only License

This license is based on the Managed Server unit of measure (for details, see "Units of Measure" on page 41). An appropriate quantity of that license must be acquired by customers who need to integrate third-party products with UCMDB.

This section also includes:

➤ "Licensing Rule" on page 46
➤ "Valid Types of Integrations" on page 45

Licensing Rule

One License To Use (LTU) must be purchased for each Managed Server that is defined in a third-party product and whose definition then gets copied to UCMDB to be recorded in the form of CIs. The UCMDB Integration Only license requires an initial minimum purchase of 100 LTUs.

Valid Types of Integrations

With this license, you can integrate third-party products with UCMDB using:

➤ Standard integrations provided by HP
➤ Standard integrations provided by HP partners (additional charges may apply)
➤ Custom data exchange integrations (the Generic DB Adapter, the Generic Push Adapter and customer-developed Java adapters)
➤ The HP Universal CMDB Web Service API and the HP Universal CMDB API (Java)
➤ But not Discovery-like integrations (those created using Jython adapters)

Note: HP Universal CMDB provides out-of-the-box adapters for third-party products such as Microsoft SCCM and BMC Atrium CMDB.

🎲 DDM Advanced Edition License

This license is based on the OS Instance unit of measure (for details, see "Units of Measure" on page 41). An appropriate quantity of that license must be acquired by customers who need access to all the Discovery and Dependency Mapping capabilities of DDM.

This section also includes:

➤ "Licensing Rule" on page 46

➤ "Discovery and Dependency Mapping" on page 46

➤ "Integrations" on page 47

➤ "DDM Inventory No Charge Entitlement with DDM Advanced Edition" on page 47

Licensing Rule

One License To Use (LTU) must be purchased for each OS Instance that is discovered by DDM and gets recorded in UCMDB in the form of CIs. The DDM Advanced Edition license requires an initial minimum purchase of 100 LTUs.

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

Servers that are both discovered by DDM and sourced from a third-party product (to collect additional data) do not need to be counted under the UCMDB Integration Only license. The DDM Advanced Edition license covers that usage scenario.

Discovery and Dependency Mapping

With this license, you can use the Discovery Control Panel and other related functions to take advantage of all the discovery content available out of the box. In addition, you can create new Jython adapters to discover other resources.

Integrations

With this license, you can use the Integration Studio to create integration points with BTO and third-party products using Discovery-like integrations (custom Jython adapters).

DDM Inventory No Charge Entitlement with DDM Advanced Edition

For each LTU purchased under the DDM Advanced Edition license for a given server, you are granted a free DDM Inventory license to collect inventory data on the same server.

Tasks

🔧 How to Upgrade to the Integration Only or DDM Advanced Edition License

When you install BSM, you receive the Universal CMDB Foundation license. To obtain the file needed to upgrade to the Integration Only or DDM Advanced Edition license, contact HP Software Support, then perform the following procedure:

To upgrade your license:

1 Obtain the appropriate file from HP Software Support.

2 Replace the **ucmdb_license.xml** file in the **<BSM root directory>\odb\conf** folder on the Data Processing server machine.

If BSM is installed in a distributed deployment, replace the file on the Gateway Server machine.

3 Use the JMX console to force a license change:

    a Launch the Web browser and enter the server address, as follows: **http://<BSM Server Host Name or IP>:21212/jmx-console**.

    b When prompted, enter the JMX Console authentication credentials (if you do not have these credentials, contact your system administrator). The default user name and password are **admin**/**admin**.

    c Under **UCMDB**, click **service=Server Services** to open the Operations page.

    d Locate **getLicense** and enter the following information:

    In the Value box for the **customerID** parameter, enter **1**.

    Click **Invoke**.

    Information about the license type, customer name, permitted packages, and whether any applications are blocked is displayed.

Reference

🔍 Troubleshooting and Limitations

This section describes troubleshooting and limitations for RTSM licensing.

➤ **Problem**: When integrating RTSM with HP Storage Essentials, unable to run the **SE Integration by SQL** job with the Foundation license.

Solution: Perform the SE Oracle Database discovery described in the *HP Universal CMDB Discovery and Integration Content Guide* PDF.

➤ **Problem**: When integrating RTSM with HP Network Node Manager (NNMi), unable to run the **Layer2 by NNM** job with the Foundation license.

Solution: For details, see "Network Node Manager (NNMi) Integration" in the *HP Universal CMDB Discovery and Integration Content Guide* PDF.

3

Data Flow Probe Installation on the Windows Platform

This chapter includes:

Tasks

➤ How to Install the Data Flow Probe — Windows on page 52

➤ How to Upgrade the Data Flow Probe from Versions Earlier than 9.03 to 9.04 on page 64

➤ How to Upgrade the Probe from Version 9.03 to 9.04 on page 65

➤ How to Detect Probe Version on page 67

➤ How to Run Probe Manager and Probe Gateway on Separate Machines on page 67

➤ How to Configure the Probe Manager and Probe Gateway Components on page 68

➤ How to Connect a Data Flow Probe to a Non-Default Customer on page 70

Reference

➤ Data Flow Probe Installation Requirements on page 71

Troubleshooting and Limitations on page 73

Tasks

❧ How to Install the Data Flow Probe — Windows

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

Note: To deploy a CUP upgrade for a Probe, see "How to Upgrade the Data Flow Probe from Versions Earlier than 9.03 to 9.04" on page 64.

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

The Probe can be installed before or after you install the BSM Gateway server. However, during Probe installation, you must provide the Server name, so it is preferable to install the Server before installing the Probe.

Verify that you have enough hard disk space available before beginning installation. For details, see "Data Flow Probe Installation Requirements" on page 71.

It is recommended to install the Probe on a separate server from the BSM servers, to distribute the overall system load.

Important:

➤ After installing the Probe, we recommend that you disable virus scanning on the main directory that is used to store your MySQL table data. The default directory is **C:\hp\UCMDB\DataFlowProbe\MySQL\data**.

➤ Before installing the Probe on a Windows 2008 machine, a user must have full control permissions on the file system. In addition, after installing the Probe, verify that the user who will run the Probe has full administration permissions on the file system where the Probe is installed.

To install the RTSM Data Flow Probe:

1 Select **Admin** > **Platform** > **Setup and Maintenance** > **Downloads**.

Note: The RTSM Data Flow Probe link in the Downloads page is displayed only if you have purchased a license for Data Flow Management, and if the administrator has added the Probe link to the Downloads page. For details, see "Installing Component Setup Files" in the *HP Business Service Management Deployment Guide* PDF.

---

 2 Click the **HPUCMDB_DataFlowProbe_904.exe** link. You can open the
 Setup file or save it to your computer:

 ➤ If you choose to open the file, it is not saved to your computer, and the
 setup program starts immediately. In this case, depending on your
 browser security settings, a security warning dialog box may open.
 Confirm that you want to proceed.

 ➤ If you choose to save the file to your computer, double-click the
 downloaded file to begin installation.
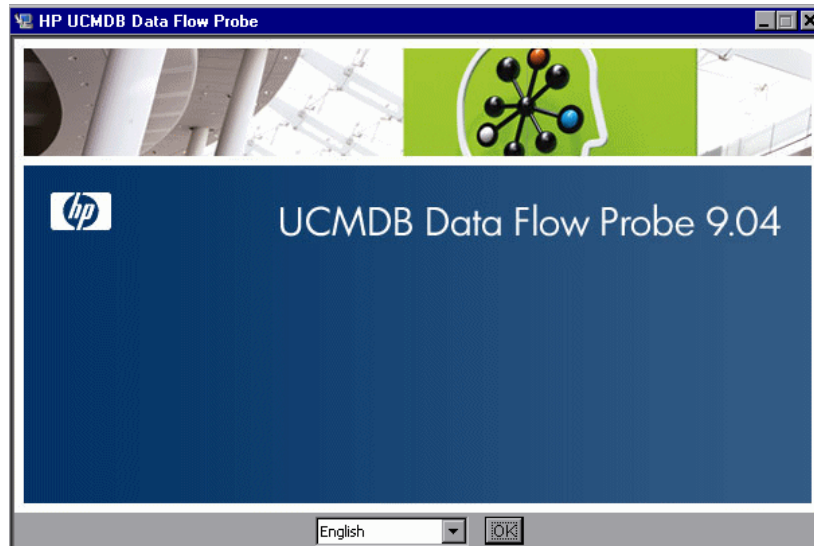
3 Choose the locale language and click **OK** to open the Introduction dialog box.
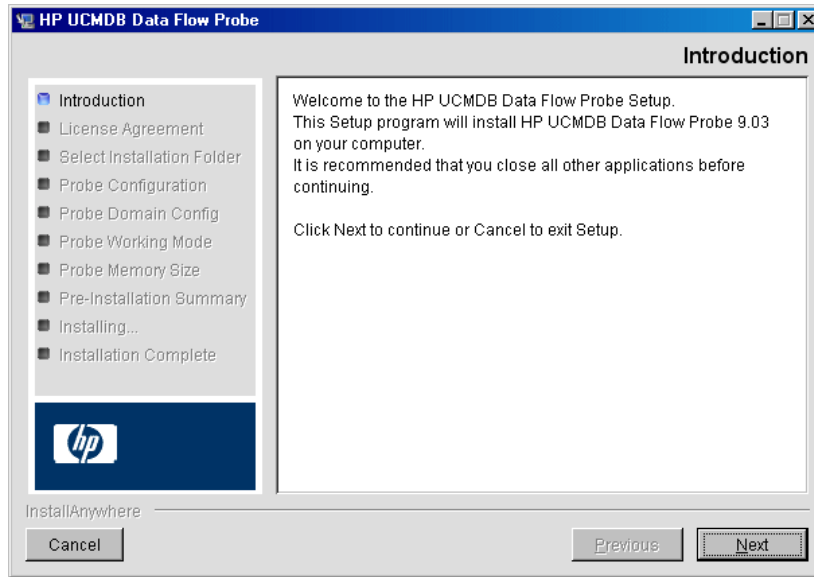
4 Click **Next** to continue to the License Agreement.
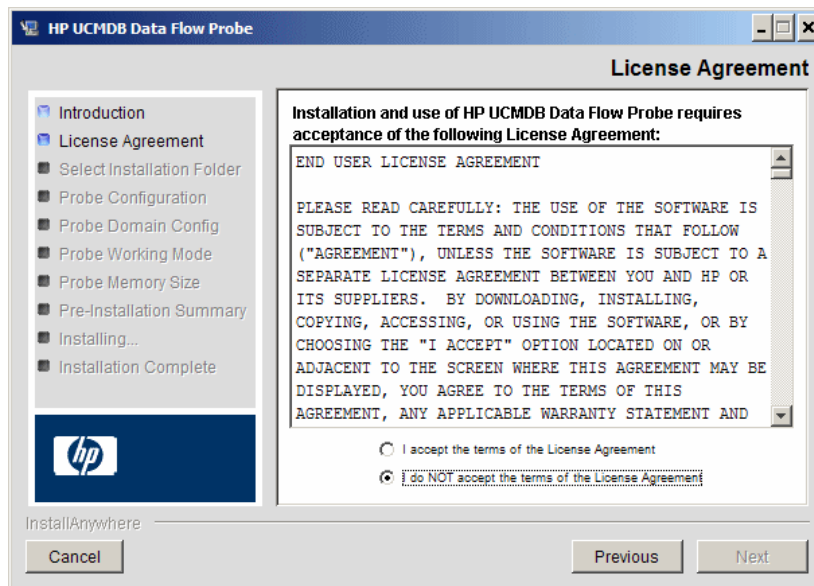
5 Accept the terms of the agreement and click **Next** to open the Select Installation Folder dialog box.
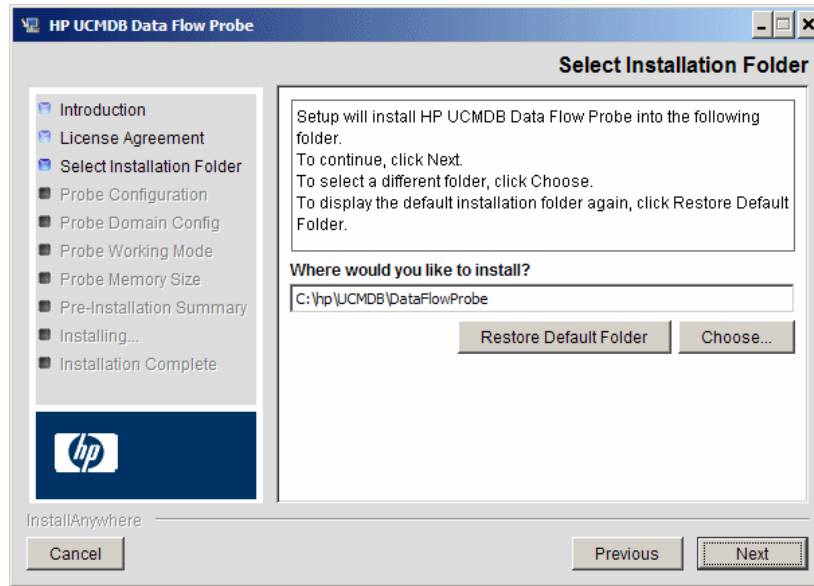
6 Accept the default entry or click **Choose** to display a standard Browse dialog box. To install to a different directory, browse to and select the installation folder.

Note:

➤ The installation folder that you select must be empty.

➤ To restore the default installation directory, after selecting a directory in the Browse dialog box, click **Restore Default Folder**.

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

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

   ➤ If you select **HP Universal CMDB**, in the **Application Server address** box, enter the name or the IP address of the HP Universal CMDB server to which the Probe is to be connected.

   ➤ If you select HP BSM, in the **Application Server address** box, enter the IP or the DNS name of the Gateway Server.

➤ In the **Data Flow Probe address** box, enter the IP address or the DNS name of the machine on which you are currently installing the Probe, or accept the default.

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

---

 8 If you do not enter the address of the application server, a message is displayed. You can choose to continue to install the Probe without entering the address, or to return to the previous page and add the address.
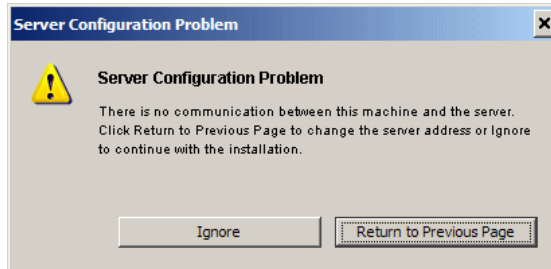
 9 Click **Next** to open the HP UCMDB Data Flow Probe Configuration dialog box.
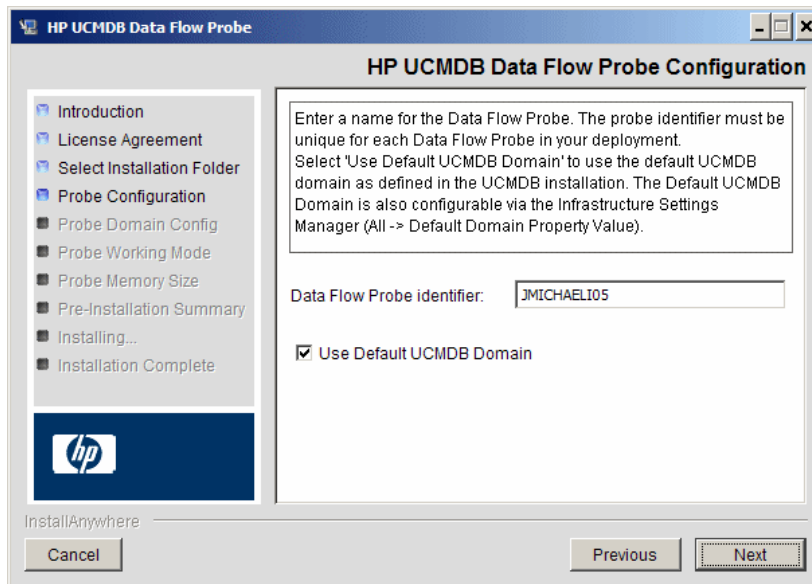
 ➤ In the **Data Flow Probe Identifier** box, enter a name for the Probe that is used to identify it in your environment.

Important:

➤ The RTSM Probe identifier, which is case sensitive, must be unique for each Probe in your deployment.

➤ When installing the Probe in separate mode (with the Probe Gateway and Probe Manager are installed on separate machines), you must give the same name (case-sensitive) to the Probe Gateway and all its Managers. This name appears in RTSM as a single Probe node. Failure to give the same name may prevent jobs from running.

➤ Select **Use Default CMDB Domain** to use the default BSM IP address or machine name, as defined in the BSM Server installation.

The Default UCMDB Domain is also configurable via Infrastructure Settings, available after installing BSM (**Admin** > **Platform** > **Setup and Maintenance** > **Infrastructure Settings** > **Foundations** > **RTSM** > **Class Model Settings** > **Default Domain Property Value**).

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

➤ **Data Flow Probe domain type**. Choose between **Customer** and **External**, depending on the type of domain on which the Probe is to be running:

➤ **Customer.** Select if you are installing one or more Probes in your deployment.

➤ **External.** Select if you are upgrading from version 6.x systems.

 Important: For new installations, always select **Customer**.

➤ **Data Flow Probe domain**: If you are not using the default domain defined in RTSM, enter the name of the domain here.

11 Click **Next** to open the HP UCMDB Data Flow Probe Working Mode dialog box.
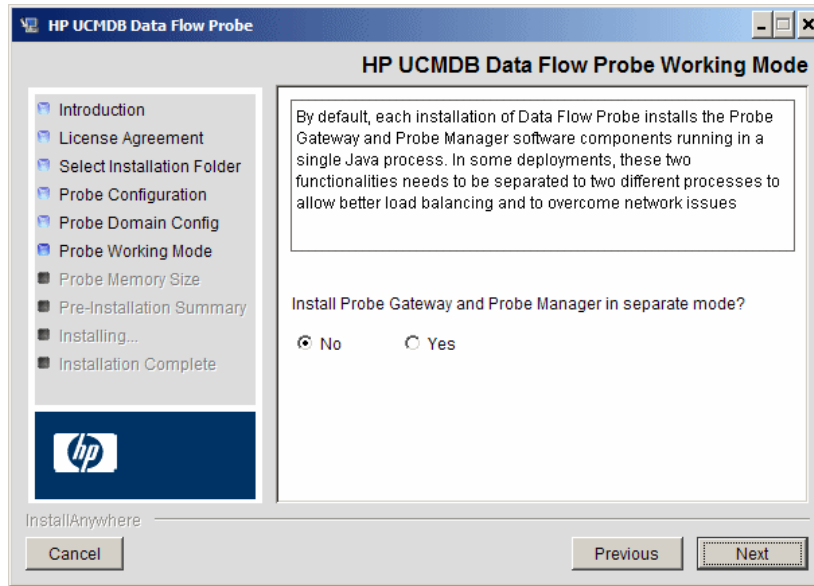
You can run the Probe Gateway and Manager as one Java process or as separate processes. You would probably run them as separate processes in deployments that need better load balancing and to overcome network issues.

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

Click **Yes** to run Probe Gateway and Probe Manager as two processes. For details on the procedure, see "How to Run Probe Manager and Probe Gateway on Separate Machines" on page 67.

12 Click **Next** to open the HP UCMDB Data Flow Probe Memory Size dialog box.
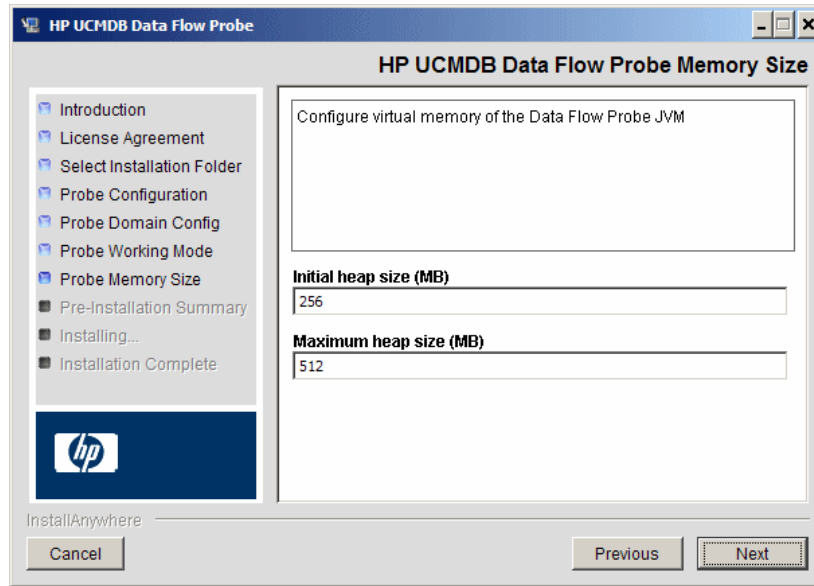
Define the minimum and maximum memory to be allocated to the Probe. The values are measured in megabytes.

Note: To change the maximum heap size value at a later point in time, update the following parameters in the file **WrapperEnv.conf**, located at **C:\hp\UCMDB\DataFlowProbe\bin\WrapperEnv.conf**:

➤ **set.GATEWAY_MAX_MEM**

➤ **set.MANAGER_MAX_MEM**

The maximum heap size allowed in 32-bit JVM is 1536 MB. If the Data Flow probe is installed in separate mode, each parameter will affect the corresponding process.

---

13 Click **Next** to open the Pre-Installation Summary dialog box and review the selections you have made.
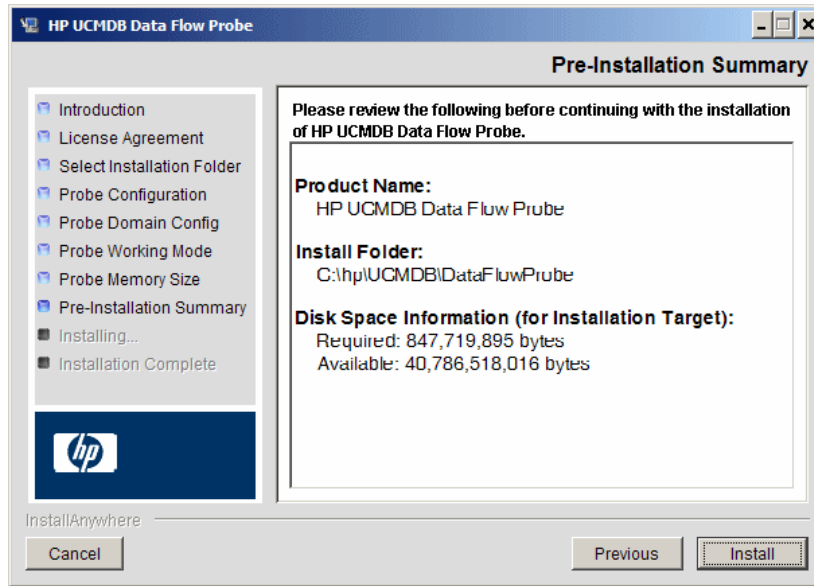
14 Click **Install** to complete the installation of the Probe. When the installation is complete the Install Complete page is displayed.

Any errors occurring during installation are written to the following file: **C:\hp\UCMDB\DataFlowProbe\HP_UCMDB_Data_Flow_Probe_Install Log.log**.

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

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

16 Activate the Probe by selecting the shortcut.

You can run the Probe in a console. For details, see "Launch the Probe in a Console".

The Probe is displayed in BSM: access **Admin** > **RTSM Administration** > **Data Flow Management** > **Data Flow Probe Setup.** For details see "Data Flow Probe Installation Requirements" on page 71.

Important: HP Software recommends that you disable virus scanning on the main directory that is used to store your MySQL table data. The default directory is **C:\hp\UCMDB\DataFlowProbe\MySQL\data**.

✌ How to Upgrade the Data Flow Probe from Versions Earlier than 9.03 to 9.04

This task describes how to upgrade the RTSM Data Flow Probe from a version earlier than 9.03 to 9.04.

Note: If you are upgrading from UCMDB 9.03 to 9.04, follow the procedure described in "How to Upgrade the Probe from Version 9.03 to 9.04" on page 65.

---

1 Uninstall the old Probe

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

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

2 Install the new Probe

You should install the new Probe with the same configuration, using the same Probe ID, domain name, and server name as for the previous Probe installation. Remember that the Probe ID is case sensitive. For details, see "How to Install the Data Flow Probe — Windows" on page 52.

Note: After performing an upgrade and installing the new Data Flow Probe, all the Discovery jobs that were active before the upgrade are automatically run.

🪛 How to Upgrade the Probe from Version 9.03 to 9.04

Use the following procedure to upgrade the Data Flow Probe when upgrading from UCMDB 9.03 to 9.04:

Note: If an integration is running on the Probe, during the upgrade the integration stops running, and starts over when the Probe is restarted after the upgrade. 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, upgrading the Probe.

---

 1 Upgrade the UCMDB server to version 9.04. For details, see "Upgrade from UCMDB 9.0x to 9.04" on page 83.

 2 Stop the Data Flow Probe.

 3 Delete the following folder: **C:\hp\UCMDB\DataFlowProbe\bin\jre**.

 4 Create backup versions of the following files:

 ➤ **C:\hp\UCMDB\DataFlowProbe\bin\WrapperGateway.conf**

 ➤ **C:\hp\UCMDB\DataFlowProbe\bin\WrapperManager.conf**

> **Note:** : These files should contain default configurations only and should not be modified. However, if these files were changed as a result of an HP Support request, you need to update the newly created files with the same changes.

 5 Extract the zip file to the Probe folder: **C:\hp\UCMDB\DataFlowProbe**.

 6 Verify that the Probe version is updated to 9.04 in the following file **C:\hp\UCMDB\DataFlowProbe\version.dat**.

 7 Start the Probe.

 8 In the Data Flow Probe Setup module, verify that the Probe is connected and that the Probe version is updated. For details, see "Details Pane" on page 155.

 9 If this process fails, you can uninstall the Probe and reinstall the new one. For details, see "How to Upgrade the Data Flow Probe from Versions Earlier than 9.03 to 9.04" on page 64.

ꙮ How to Detect Probe Version

Beginning in UCMDB 9.04, the Probe reports its version when connecting to the server. The Probe version is displayed in the Details pane of the Data Flow Probe Setup module. If the PROBE version is not compatible with the server version (and there is no supported upgrade) an error is generated and the Probe is forced to shut down.

When you apply a new Cumulative Update Patch (CUP) to the UCMDB 9.04 server, the Probes do not shut down automatically, and are able to report new data to the server. However, this is not recommended. Therefore, when you apply a CUP to the server, you must also apply it to the Probes—either manually or automatically.

ꙮ How to Run Probe Manager and Probe Gateway on Separate Machines

During installation, you can choose to separate the Probe Manager and Probe Gateway processes so that they run on separate machines. You must:

 1 Install the Probe on both machines according to the procedure in "How to Install the Data Flow Probe — Windows" on page 52.

 2 Choose **Yes** in step 11 on page 61.

 3 Perform the configuration in "How to Configure the Probe Manager and Probe Gateway Components" on page 68.

Note:

➤ At least one Probe Gateway component must be installed. Gateway is connected to the UCMDB Server, receives tasks from the Server, and communicates with the collectors (Probe Manager).

➤ Several Probe Managers can be installed. Managers run jobs and gather information from networks.

➤ The Probe Gateway should contain a list of attached Managers.

➤ The Probe Managers must know to which Gateway they are attached.

🔧 How to Configure the Probe Manager and Probe Gateway Components

This task describes how to set up the Data Flow Probe when the Probe Manager and Probe Gateway run as separate processes on two machines.

Important: The Probe Manager name in both the probeMgrList.xml and DiscoveryProbe.properties files must be identical. The name is case sensitive.

This section includes the following topics:

➤ "Set Up the Probe Gateway Machine" on page 68

➤ "Set Up the Probe Manager Machine" on page 69

➤ "Start the Services" on page 69

1 Set Up the Probe Gateway Machine

   a Open the following file:

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

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

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

   c Open the following file:

     C:\hp\UCMDB\DataFlowProbe\conf\DiscoveryProbe.properties

   d Locate the lines beginning **appilog.collectors.local.ip =** and **appilog.collectors.probe.ip =** and enter the Gateway machine name or IP address, for example:

```
appilog.collectors.local.ip = STARS01
appilog.collectors.probe.ip = STARS01
```

2 Set Up the Probe Manager Machine

   a In **C:\hp\UCMDB\DataFlowProbe\conf\DiscoveryProbe.properties**, locate the line beginning **appilog.collectors.local.ip =** and enter the Manager machine name or IP address, for example:

```
appilog.collectors.local.ip = OLYMPICS08
```

   b Locate the line beginning **appilog.collectors.probe.ip =** and enter the Gateway machine name in uppercase, for example:

```
appilog.collectors.probe.ip = STARS01
```

3 Start the Services

   a On the Probe Manager machine, start the Manager service: **Start > All Programs > UCMDB > Start Data Flow Probe Manager**.

   b On the Probe Gateway machine, start the Gateway service: **Start > All Programs > HP UCMDB > Start Data Flow Probe Gateway**.

🔧 How to Connect a Data Flow Probe to a Non-Default Customer

You can connect a Data Flow Probe to a customer that is not the default. The default customer ID is **1**.

1 Open the following file in a text editor:

   C:\hp\UCMDB\DataFlowProbe\conf\DiscoveryProbe.properties.

2 Locate the **customerID** entry.

3 Update the value with the customer ID, for example, **customerId = 2**.

4 Restart the Probe so that it is updated with your changes.

Reference

🔍 Data Flow Probe Installation Requirements

This section includes the following topics:

➤ "Hardware Requirements" on page 71

➤ "Software Requirements" on page 71

➤ "Supported Databases" on page 72

➤ "Virtual Environment Requirements" on page 72

Hardware Requirements

Computer/processor	**Windows:** Pentium IV 2.4 GHz or later processor
Memory	**Windows:** Minimum 1 GB RAM (Recommended: 2 GB RAM)
Virtual memory (for Windows deployment)	Minimum 2 GB **Note:** The virtual memory size should always be at least twice the physical memory size.
Free hard disk space	**Windows:** Minimum 4 GB (at least 4 GB for database software and data files) (Recommended: 20 GB hard disk)
Display	**Windows:** Color palette setting of at least 256 colors (32,000 colors recommended)

Software Requirements

Hardware Platform	OS Type	OS Version and Edition	Supported	Recommended
x86	Windows 2008	SP2, Standard/Enterprise editions, 32-bit	Yes	
x86-64	Windows 2008	SP2, Standard/Enterprise editions, 64-bit	Yes	Yes

Hardware Platform	OS Type	OS Version and Edition	Supported	Recommended
x86-64	Windows 2008	R2 and R2 SP1, Standard/Enterprise editions, 64-bit	Yes	
x86	Windows 2003	SP2 and R2 SP2, Standard/Enterprise editions, 32-bit	Yes	
x86-64	Windows 2003	SP2 and R2 SP2, Standard/Enterprise editions, 64-bit	Yes	
	Windows 7	Professional/Enterprise	No	
	Windows 2000		No	

Supported Databases

Database	Version and Edition	Recommended	Comments
MySQL	5.1.46	Yes	This database comes bundled with the Probe installation.

Virtual Environment Requirements

Platform	OS Version and Edition	Supported	Recommended
VMware ESX 3.x	➤ Windows 2003 Standard/Enterprise editions SP2 and R2 SP2, 32/64-bit ➤ Windows 2008 Standard/ Enterprise SP2, 32/64-bit and R2, 64-bit	Yes	
VMware ESX 4.0	➤ Windows 2003 Standard/Enterprise editions SP2 and R2 SP2, 32/64-bit ➤ Windows 2008 Standard/ Enterprise SP2, 32/64-bit and R2, 64-bit	Yes	Yes

Platform	OS Version and Edition	Supported	Recommended
Pre ESX 3.5 (like 3.0.x versions)	➤ May not provide adequate performance ➤ Does not support Windows 2008 or Windows 7	No	
ESXi VMware	All platforms	No	
MS Hyper-V	Server 2008 v1 and R2	No	
Xen Hypervisor 3.x	All platforms	No	

🔍 Troubleshooting and Limitations

Repairing Corrupted Databases

The Data Flow Probe MySQL database may become corrupt without the possibility of recovery, for example, because the machine was shut down but the MySQL service was not stopped.

To repair the corruption:

1 Stop the Probe.

2 Run the **repair_mysql.bat** tool from the following folder: **C:\hp\UCMDB\DataFlowProbe\tools**

3 Start the Probe.

If this procedure does not fix the corruption, contact HP Software Support.

Probe Downgrade or Rollback

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

Probe Restart

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

4

Data Flow Probe Installation on the Linux Platform

This chapter includes:

Tasks

➤ How to Install the Data Flow Probe — Linux on page 76

➤ How to Stop the Data Flow Probe on page 85

➤ How to Upgrade the Probe from UCMDB 9.03 to 9.04 on page 86

➤ How to Upgrade the Data Flow Probe from Versions Earlier than 9.03 to 9.04 on page 88

➤ How to Connect a Data Flow Probe to a Non-Default Customer on page 89

Reference

➤ Data Flow Probe Support Requirements on page 90

Troubleshooting and Limitations on page 90

Tasks

❧ How to Install the Data Flow Probe — Linux

Important:

➤ This Probe is intended for integration use only, and cannot be used for discovery. This Probe does not appear in the Data Flow Setup window.

➤ Only integration with BSM version 9.01 and later is supported on the Probe on Linux.

➤ An instance of Microsoft My SQL database must not be running on the machine on which you are installing the Data Flow Probe. If an instance exists, you must disable it.

➤ To install the Data Flow Probe, you must have root permissions to the Linux machine.

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

The Probe can be installed before or after you install the BSM Gateway server. However, during Probe installation you must provide the Server name, so it is preferable to install the Server before installing the Probe.

Verify that you have enough hard disk space available before beginning installation. For details, see "Data Flow Probe Support Requirements" on page 90.

It is recommended to install the Probe on a separate server from the BSM servers, to distribute the overall system load.

Important: After installing the Probe, HP Software recommends that you disable virus scanning on the main directory that is used to store your MySQL table data. The default directory is **/opt/hp/UCMDB/DataFlowProbe/MySQL/data**.

To install the RTSM Data Flow Probe:

1 Select **Admin** > **Platform** > **Setup and Maintenance** > **Downloads**.

Note: The RTSM Data Flow Probe link in the Downloads page is displayed only if you have purchased a license for Data Flow Management, and if the administrator has added the Probe link to the Downloads page. For details, see "Installing Component Setup Files" in the *HP Business Service Management Deployment Guide* PDF.
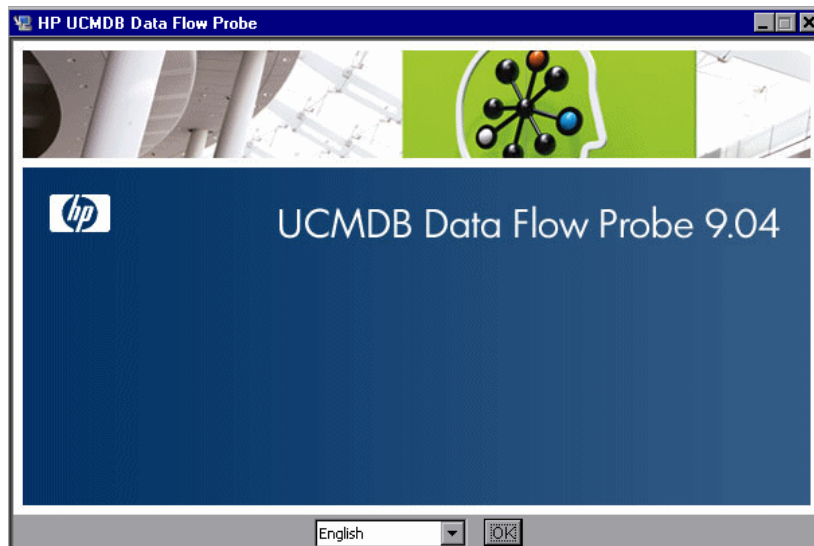
2 Choose the locale language and click **OK** to open the Introduction dialog box.
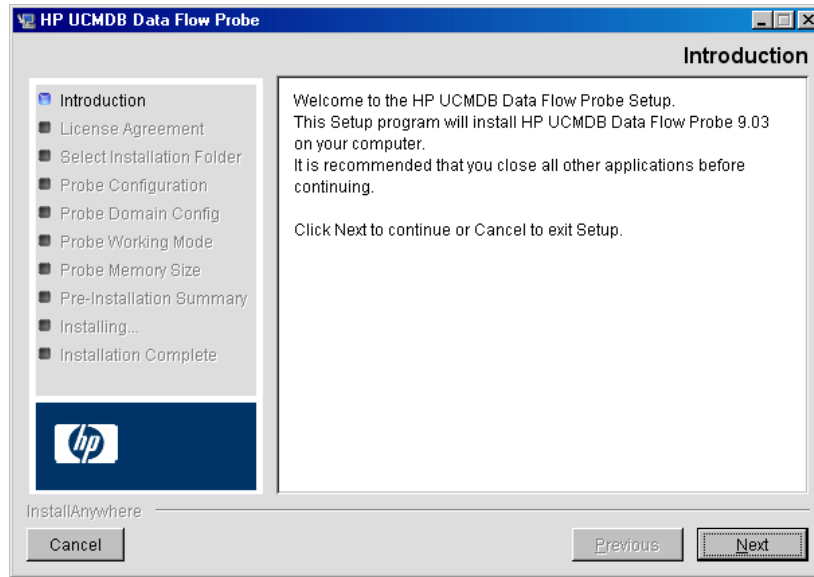
3 Click **Next** to continue to the License Agreement.
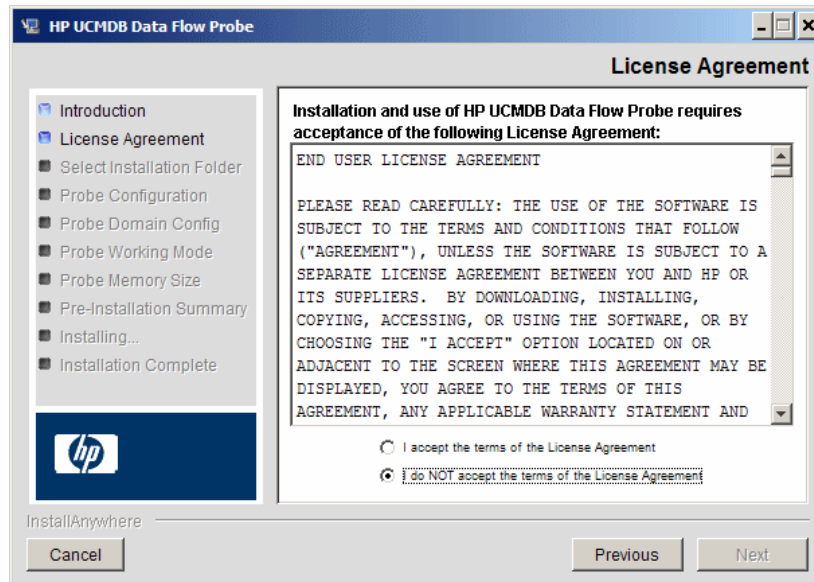
4 Accept the terms of the agreement and click **Next** to open the Select Installation Folder dialog box.
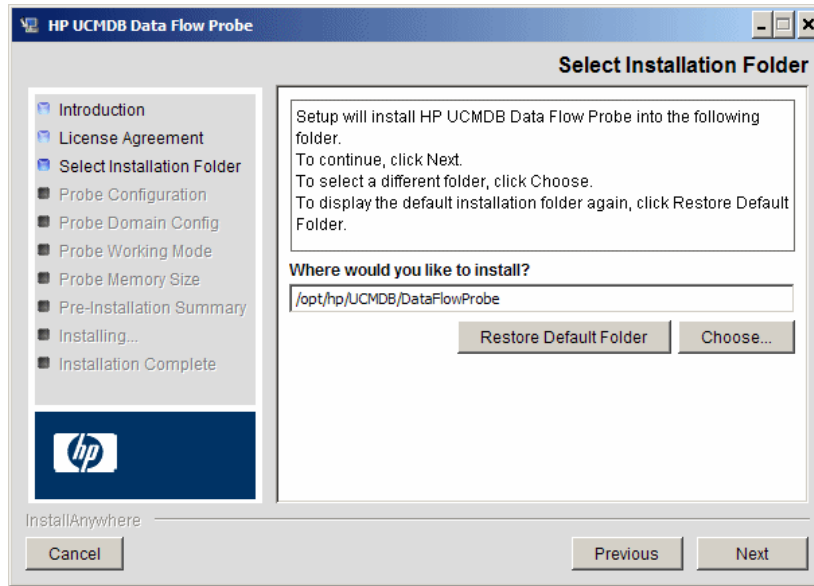
5 Accept the default entry or click **Choose** to display a standard Browse dialog box. To install to a different directory, browse to and select the installation folder.

Note:

➤ You can change the location of the installation, but the directory must be located under **/opt/**.

➤ To restore the default installation directory, after selecting a directory in the Browse dialog box, click **Restore Default Folder**.

---

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

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

   ➤ If you select **HP Universal CMDB**, in the **Application Server address** box, enter the name or the IP address of the HP Universal CMDB server to which the Probe is to be connected.

   ➤ If you select HP BSM, in the **Application Server address** box, enter the IP or the DNS name of the Gateway Server.

➤ In the **Data Flow Probe address** box, enter the IP address or the DNS name of the machine on which you are currently installing the Probe, or accept the default.

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

---

7 If you do not enter the address of the application server, a message is displayed. You can choose to continue to install the Probe without entering the address, or to return to the previous page and add the address.
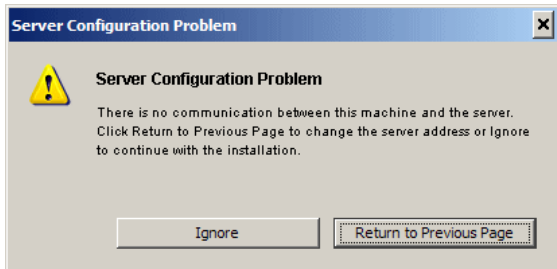
8 Click **Next** to open the HP UCMDB Data Flow Probe Configuration dialog box.
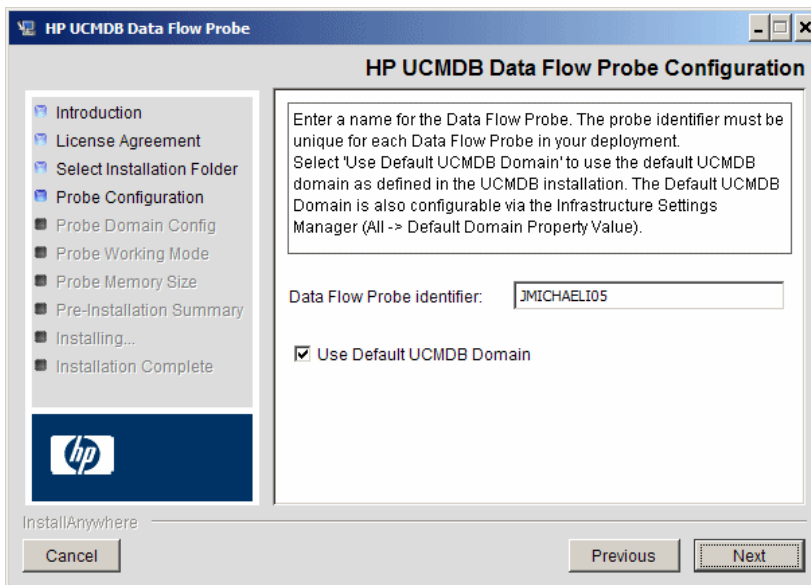
➤ In the **Data Flow Probe Identifier** box, enter a name for the Probe that is used to identify it in your environment. This is the name that appears in the Integration Point dialog box. For details, see "New Integration Point/Edit Integration Point Dialog Box" in *RTSM Data Flow Management Guide*.

> **Important:** The RTSM Probe identifier, which is case sensitive, must be unique for each Probe in your deployment.

➤ Select **Use Default CMDB Domain** to use the default BSM IP address or machine name, as defined in the BSM Server installation.

The Default UCMDB Domain is also configurable via Infrastructure Settings, available after installing BSM (**Admin** > **Platform** > **Setup and Maintenance** > **Infrastructure Settings** > **Foundations** > **RTSM** > **Class Model Settings** > **Default Domain Property Value**).

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

➤ **Data Flow Probe domain type**. Choose between **Customer** and **External**, depending on the type of domain on which the Probe is to be running:

➤ **Customer.** Select if you are installing one or more Probes in your deployment.

➤ **External.** Select if you are upgrading from version 6.x systems.

Important: For new installations, always select **Customer**.

➤ **Data Flow Probe domain**: If you are not using the default domain defined in RTSM, enter the name of the domain here.

Note: The installation procedure skips the HP UCMDB Data Flow Probe Working Mode dialog box. This is because the Probe Gateway and Probe Manager must be run as one Java process.

---

10 Click **Next** to open the HP UCMDB Data Flow Probe Memory Size dialog box.
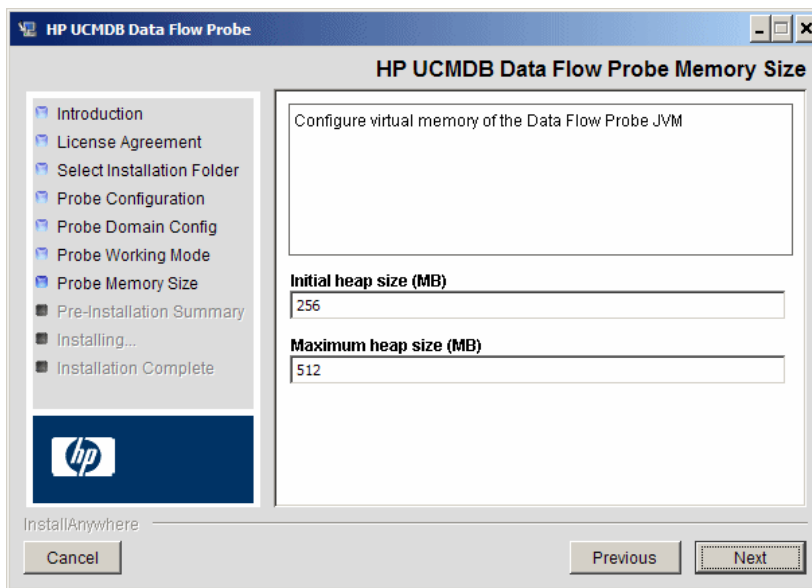
Define the minimum and maximum memory to be allocated to the Probe. The values are measured in megabytes.

Note: To change the maximum heap size value at a later point in time, update the following parameters in the file **WrapperEnv.conf**, located at: **/opt/hp/UCMDB/DataFlowProbe/bin/WrapperEnv.conf**:

➤ **set.GATEWAY_MAX_MEM**

➤ **set.MANAGER_MAX_MEM**

The maximum heap size allowed in 32-bit JVM is 1536 MB. If the Data Flow probe is installed in separate mode, each parameter will affect the corresponding process.

11 Click **Next** to open the Pre-Installation Summary dialog box and review the selections you have made.
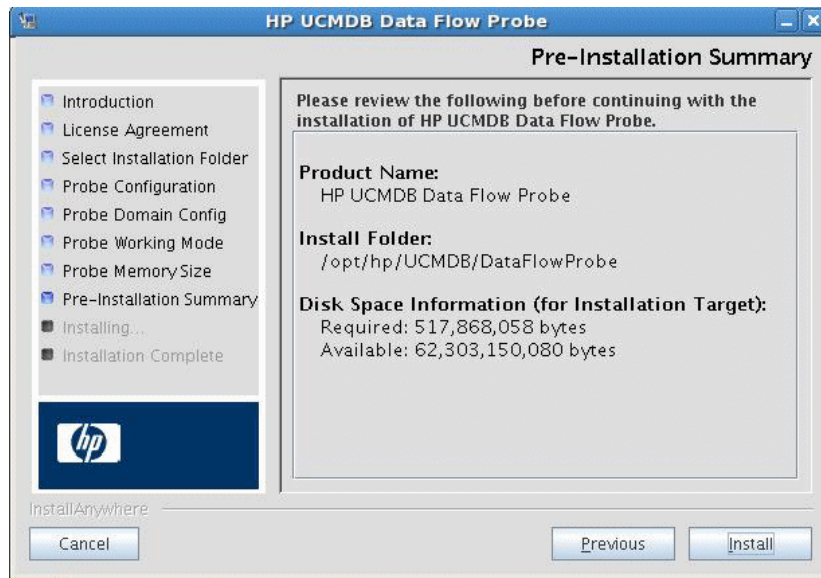
12 Click **Install** to complete the installation of the Probe. When installation is complete the Install Complete page is displayed.

Any errors occurring during installation are written to the following file: **/opt/hp/UCMDB/DataFlowProbe/HP_UCMDB_Data_Flow_Probe_ InstallLog.log**. If you installed the Probe to another directory under **/opt/**, the log file is located there.

13 Click **Done**.

14 Activate the Probe by executing the following command: **/opt/hp/UCMDB/DataFlowProbe/bin/ProbeGateway.sh start**

To activate the Probe in a console, execute the following command: **/opt/hp/UCMDB/DataFlowProbe/bin/ProbeGateway.sh console**

The installed Probe is displayed in the New Integration Point dialog box, in the list of Probes. For details, see "New Integration Point/Edit Integration Point Dialog Box".

Note: The user running the Probe service must be a member of the Administrators group.

How to Stop the Data Flow Probe

To stop the Probe server, execute the following command:

/opt/hp/UCMDB/DataFlowProbe/bin/ProbeGateway.sh stop

🔧 How to Upgrade the Probe from UCMDB 9.03 to 9.04

Use the following procedure to updgrade the Data Flow probe when upgrading from UCMDB 9.03 to 9.04:

Note: If an integration is running on the Probe, during the upgrade the integration stops running, and starts over when the Probe is restarted after the upgrade. 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, upgrading the Probe.

---

1 Upgrade the UCMDB server to version 9.04. For details, see "Upgrade from UCMDB 9.0x to 9.04" on page 83.

2 Stop the Data Flow probe.

3 Delete the following folder: **/opt/hp/UCMDB/DataFlowProbe/bin/jre**.

4 Create backup versions of the following files:

➤ **/opt/hp/UCMDB/DataFlowProbe/bin/WrapperGateway.conf**

➤ **/opt/hp/UCMDB/DataFlowProbe/bin/WrapperManager.conf**

Note: : These files should contain default configurations only and should not be modified. However, if these files were changed as a result of an HP Support request, you need to update the newly created files with the same changes.

---

5 Extract the zip file to the probe folder: **/opt/hp/UCMDB/DataFlowProbe**.

6 Verify that the probe version is updated to 9.04 in the following file: **/opt/hp/UCMDB/DataFlowProbe/version.dat**.

7 Start the probe.

 8 If this process fails, you can uninstall the probe and reinstall the new one.
   For details, see "How to Upgrade the Data Flow Probe from Versions
   Earlier than 9.03 to 9.04" on page 88.

🔨 How to Upgrade the Data Flow Probe from Versions Earlier than 9.03 to 9.04

This task describes how to upgrade the RTSM Data Flow Probe from a version earlier than 9.03 to 9.04.

Note: If you are upgrading from UCMDB 9.03 to 9.04, follow the procedure described in "How to Upgrade the Probe from UCMDB 9.03 to 9.04" on page 86.

---

1 Uninstall the old Probe

Uninstall all existing Probes. If a Probe is running, stop it before you uninstall it. For details, see "How to Stop the Data Flow Probe" on page 85.

Either:

➤ In shell, execute:

```
sh /opt/hp/UCMDB/DataFlowProbe/UninstallerData/Uninstall_Discovery_Probe
```

Or:

➤ Double-click on the Uninstall_Discovery_Probe file in the file system.

2 Install the new Probe

You should install the new Probe with the same configuration, using the same Probe ID, domain name, and server name as for the previous Probe installation. Remember that the Probe ID is case sensitive.

Note: After performing an upgrade and installing the new Data Flow probe, all the Discovery jobs that were active before the upgrade are automatically run.

🐾 How to Connect a Data Flow Probe to a Non-Default Customer

You can connect a Data Flow Probe to a customer that is not the default. The default customer ID is **1**.

1 Open the following file in a text editor:

../DataFlowProbe/conf/DiscoveryProbe.properties

2 Locate the **customerID** entry.

3 Update the value with the customer ID, for example, **customerId = 2**.

4 Restart the Probe so that it is updated with your changes.

Reference

🔖 Data Flow Probe Support Requirements

For details on support requirements, see "HP Universal CMDB Support Matrix" in the *HP Universal CMDB Deployment Guide* PDF.

🔍 Troubleshooting and Limitations

The Data Flow Probe MySQL database may become corrupt without the possibility of recovery, for example, because the machine was shut down but the MySQL service was not stopped.

To repair the corruption:

1 Stop the Probe.

2 Run the **repair_mysql.sh** tool from the following folder: **/opt/hp/UCMDB/DataFlowProbe/tools**.

3 Start the Probe.

If this procedure does not fix the corruption, contact HP Software Support.

Probe Downgrade or Rollback

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

Probe Restart

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

Part II

Data Flow Management Setup

5

Data Flow Probe Setup

This chapter includes:

Concepts

➤ Job Execution Policies on page 94

➤ Data Validation on the Data Flow Probe on page 97

➤ Filtering Results on page 98

Tasks

➤ How to Get Started with the RTSM Data Flow Probe on page 99

➤ How to Add a Data Flow Probe on page 100

➤ How to Delete Unsent Probe Results on page 102

Reference

➤ Domain Credential References on page 103

➤ Data Flow Probe Log Files on page 132

➤ The DiscoveryProbe.properties File on page 137

➤ Data Flow Probe Setup User Interface on page 148

Troubleshooting and Limitations on page 166

Concepts

🔹 Job Execution Policies

You can define periods of time when a Probe must not run. You can choose to disable specific jobs running on any Probe or all jobs running on a specific Probe. 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 "Add/Edit Policy Dialog Box" on page 152.

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:

Job Execution Policy		
⬆ ⬇ ➕ ✖ ✏		
Time	**Probes**	**Jobs**
Total TCP Blackout	All	[IP Traffic by Network Data, Col
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:
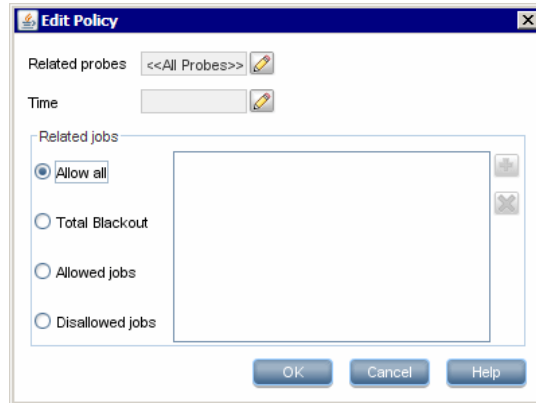
The next job (Software Element CF by Shell) starts running. It checks the policies in the policy list from top to bottom. It starts by checking **Total TCP Blackout**. The job appears in this policy (**Disallowed Jobs** is selected in the Edit Policy dialog box), so the job does not run:
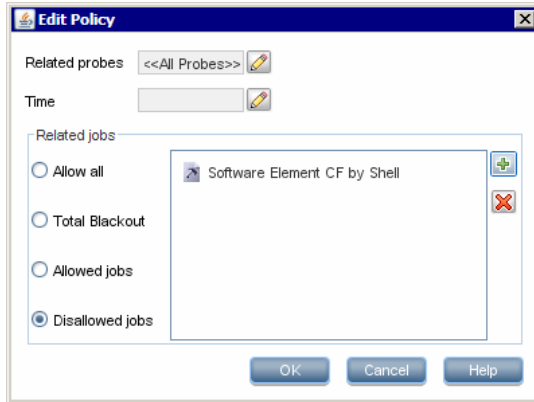
Caution: If a job is not connected to any policy, it does not run. To run these jobs, set the last policy in the list to **Allow All**.

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 Validation on the Data Flow Probe

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.

➤ The CI's attributes of type STRING are checked to verify that they do not exceed the size limit. If an attribute is longer than the limit, DFM checks whether an AUTO_TRUNCATE qualifier is defined for the attribute. If there is a qualifier, the value is truncated and a warning message is written to the Probe error.log file.

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.

For details on attributes, see "CI Type Attributes" in the *RTSM Modeling Guide*.

97

🔵 Filtering Results

You can filter results sent by the Probe to the BSM Gateway 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 and global filtering:

➤ **Adapter filtering.** The Data Flow 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 199.

➤ **Global filtering.** DFM filters the results of all jobs running on a Probe. You define global filters in the globalFiltering.xml file. For details, see "Configure a Filter" on page 187.

The order of filtering is as follows: during a run, the Data Flow Probe first searches for an adapter filter and applies the filter to the results of the run. If there are no adapter filters, DFM searches for a global filter and applies that filter to the results. If DFM finds no filters, all results are sent to the server.

Tasks

🔧 How to Get Started with the RTSM Data Flow Probe

This task describes how to install and launch the Data Flow Probe running on a Windows platform. (The Data Flow Probe that runs on a Linux platform is intended only for integrations.)

Note:

➤ The Probe link in the Downloads page is displayed only if you have purchased a license for the DFM application.

➤ The managed environment is defined by the IP 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.

This task includes the following steps:

➤ "Install the Probe" on page 99

➤ "Launch the Probe from the Start Menu" on page 99

➤ "Launch the Probe in a Console" on page 100

➤ "Run Discovery" on page 100

➤ "Stop the Probe" on page 100

Install the Probe

For details, see "Data Flow Probe Installation on the Windows Platform" on page 51.

Launch the Probe from the Start Menu

On the machine on which the Probe is installed, select **Start** > **Programs** > **HP UCMDB** > **Start Data Flow Probe**. The Probe is started as a service.

To verify that the Probe has been launched successfully, in BSM select **Admin > RTSM Administration** > **Data Flow Management** > **Data Flow Probe Setup**. Select the Probe and, in the Details pane, verify that the status is **connected**.

Launch the Probe in a Console

You can configure the Probe so that it opens in a console. In this case, the command prompt window is displayed. Execute the following script: **C:\hp\UCMDB\DataFlowProbe\bin\gateway.bat console**.

Note: The user running the Probe service must be a member of the Administrators group.

Run Discovery

For details, see "Discovery Control Panel Overview" on page 324.

Stop the Probe

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

➤ To stop the Probe when it is running as a service, select **Start** > **Programs** > **HP UCMDB** > **Stop Data Flow Probe**.

🪁 How to Add a Data Flow Probe

This task describes how to add a Probe to BSM.

This task includes the following steps:

➤ "Prerequisites" on page 101

➤ "Add a Domain to RTSM" on page 101

➤ "Add a Data Flow Probe to the new domain" on page 101

➤ "Add more Probes to the domain – optional" on page 101

➤ "Define credentials" on page 102

1 Prerequisites

Verify that the Probe is installed and make a note of its IP address.

2 Add a Domain to RTSM

In this step, you create the domain for the new Probe. When you start the Probe, it connects to RTSM automatically. To verify, select **Admin** > **RTSM Administration** > **Data Flow Management** > **Data Flow Probe Setup**. Select the Probe and, in the Details pane, verify that the status is **connected**.

To define Probe ranges before the Probe has connected for the first time, you must define them manually. For details, see "Add/Edit IP Range Dialog Box" on page 149.

  a Access the Probe configuration window: **Admin** > **RTSM Administration** > **Data Flow Management** > **Data Flow Probe Setup**.

  b Select **Domains and Probes** and click the **Add Domain or Probe** button to open the **Add New Domain** dialog box. For details, see "Add New Domain Dialog Box" on page 153.

3 Add a Data Flow Probe to the new domain

In this step, you define the Probe and its range.

  a Double-click the new domain and select the **Probes** folder.

  b Click the **Add Domain or Probe** button to open the Add New Probe dialog box. For details, see "Add New Probe Dialog Box" on page 154.

  c Select the new Probe and define its IP range. For details, see "Add/Edit IP Range Dialog Box" on page 149.

  d Repeat for any additional probes you want to add.

4 Add more Probes to the domain – optional

To add more Probes to this domain, repeat step 3.

5 **Define credentials**

Configure credentials depending on what must be discovered and which protocols are supported on your site's network.

For details, see "Details Pane (Protocol)" on page 157. For a list of protocols, see "Domain Credential References" on page 103.

🔧 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 RTSM Server.

1 Access the Data Flow Probe JMX console: Launch a Web browser and enter the following address: **http://<Probe Gateway machine name or IP address>:1977**. If you are running the Data Flow Probe locally, enter **http://localhost:1977**.

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

Note: If you have not created a user, use the default user name **admin** and the password **admin** to log in.

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.

Reference

🔍 Domain Credential References

This section explains protocol credentials. You can edit credential attributes. For details, see "Protocol Parameter Dialog Box" on page 165.

Note: The following information can change from version to version: Changes in content implementation can cause protocol attributes to be updated.

This section includes the following topics:

➤ "Domains and Probes Pane UI Elements" on page 103

➤ "Supported Agents" on page 107

➤ "Supported Protocols" on page 108

Domains and Probes Pane UI Elements

When a protocol is selected in the Domains and Probes Pane, the following elements are included (unlabeled UI elements are shown in angle brackets):

UI Element (A-Z)	Description
➕	Opens the Protocol Parameter dialog box, to add new connection details.
❌	Select a protocol, select connection details, and click the button to remove the connection details.
✏️	Select a protocol and click to open the Edit Protocol Parameter dialog box.

UI Element (A-Z)	Description
⬆ ⬇	Select a protocol and click an arrow to move the protocol instance up or down.
	The order of the policies in the list defines which policy is checked first: a job starts running and checks the policy list from top to bottom. If the job name exists in a policy, the job runs. For details on adding jobs to a protocol, see "Add/Edit Policy Dialog Box" on page 152. For details on job execution policies, see "Example of Policy Ordering" on page 94.

UI Element (A-Z)	Description

<right-click menu>	Choose from the following options:
	
	➤ **Edit.** Choose this option to enter protocol parameters, such as user name and password, that enable DFM to connect to an application on a remote machine.
	
	➤ **Edit using previous interface.** Choose this option if:
	
	   ➤ In a previous version of RTSM, 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 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.
	
	➤ **Check credentials.** In the box that opens, enter the IP address of the remote machine on which the protocol must run. The Probe attempts to connect to this IP and returns an answer as to whether the connection succeeded or not.

<right-click a column name>	Choose from the following options: ➤ **Hide Column.** Displayed when a column is shown. ➤ **Show All Columns.** Displayed when a column is hidden. ➤ **Customize.** Select to change the display order of the columns. ➤ **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.

All protocol credentials include the following parameters:

Parameter	Description
Index	Indicates the order in which protocol instances are used 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, click **Edit**. For details, see "Scope Definition Dialog Box" on page 165. **Default: ALL**.
User Label	Enter a label to help you identify a specific protocol credential, when you use it later. Enter a maximum of 50 characters.

Supported Agents

➤ **SNMP Agent.** Provides information about the operating systems, device types, installed software, and other system resources information. SNMP agents can usually be extended to support new MIBs, exposing more data for managerial purposes.

➤ **WMI Agent.** Microsoft's remote management agent, which is usually available for access by a remote administrator. The WMI agent is also extensible by adding WMI providers to the generic agent.

➤ **Telnet/SSH Agent (or daemon).** Used mostly on UNIX systems to connect remotely to a machine and to launch various commands to obtain data.

➤ **xCmd.** A remote administration technology similar in functionality to Telnet/SSH that enables launching any console command over Windows machines. xCmd relies on Administrative Shares & Remove Service Administration APIs to function correctly.

The **xCmd.exe** file is signed by an HP digital certificate. To validate that **xCmd.exe** is provided by HP, right-click the **xCmd.exe** file (or **xCmdSvc.exe** on a remote machine), select **Properties** and view the digital signatures.

➤ **Application specific.** This agent depends on the remote application to function as an agent and respond appropriately to the Probe's remote queries, for example, database discoveries, Web server discoveries, and SAP and Siebel discoveries.

Supported Protocols

This section includes the following topics:

Tip: If you use the SSH or Telnet credentials for discovery, we recommend that you add the following folders to the system path:

/sbin

/usr/sbin

/usr/local/sbin

Default Ports for Supported Protocols

The following table lists the default ports for each supported protocol.

Protocol	Default Port
HP SIM	50001, 280
HTTP	80
JBoss	1099
LDAP	389
NNM	80
NTCMD	135, 137, 138, 139
PowerShell	80, 443, 5985, 5986 **Note:** The ports depend on the Microsoft Windows operating system configuration
SAP	➤ 3200 ➤ 3300-3303 ➤ 33xx, where xx is the SAP server instance number **Note:** To enable UCMDB to identify other port numbers mapped to SAP instances, you must configure the **portNumberToPortName.xml** file. For more details, see "How to Define a New Port" on page 180.

Protocol	Default Port
SAP JMX	➤ 50004, 50104, 50204, 50304, 50404 ➤ 5xx04, where xx is the SAP J2EE server instance number **Note:** To enable UCMDB to identify other port numbers mapped to SAP instances, you must configure the **portNumberToPortName.xml** file. For more details, see "How to Define a New Port" on page 180.
Siebel Gateway	2320
SNMP	161
SQL	1521, 1433, 6789, 3306, 2048
SSH	22
Telnet	23
UDDI	80, 443
VMWare VIM	80, 443
WebLogic	7001, 7002
WebSphere	8880
WMI	135, 137, 138, 139

Tip: If you use the SSH or Telnet credentials for discovery, we recommend that you add the following folders to the system path:

/sbin

/usr/sbin

/usr/local/sbin

⚒ Generic Protocol

This protocol is intended for integrations that do not need a specific protocol. It is recommended to use this protocol for all out-of-the-box integrations, as they require a user name and password only.

Parameter	Description
Description	Description of the credentials.
User Name	The name of the user needed for authentication.
User Password	The password of the user needed for authentication.

⚒ HP SIM Protocol

Parameter	Description
Port Number	The port at which the SIM MXPartner WebService API listens for SOAP requests. The defaults are **280** for HTTP and **50001** for HTTPS.
SIM Database Instance	➤ **Microsoft SQL Server**: Enter the instance name only for non-default instances of Microsoft SQL Server. ➤ **Oracle**: Enter the SID.
SIM Database Name	(Microsoft SQL Server only) Enter the name of the database.
SIM Database Password	The password of the database user (Microsoft SQL Server) or schema name (Oracle) for the SIM database.
SIM Database Port	The listener port for the database.
SIM Database Type	Choose between: ➤ MSSQL ➤ MSSQL_NTLM ➤ Oracle
SIM Database User Name	The database user (Microsoft SQL Server) or schema name (Oracle) with permissions to access the database.
SIM Webservice Protocol	Choose between **HTTP** or **HTTPS**.

Parameter	Description
User Name	The name of the user needed to connect to the application.
User Password	The password of the user needed to connect to the application.

🔍 JBoss Protocol

Parameter	Description
Port Number	The port number.
Connection Timeout	Time-out in milliseconds after which the Probe stops trying to connect to the JBoss application server.
User Name	The name of the user needed to connect to the application.
Password	The password of the user needed to connect to the application.

🔍 LDAP Protocol

Parameter	Description
Port Number	The port number.
Connection Timeout	Time-out in milliseconds after which the Probe stops trying to connect to the LDAP application server.
User Name	The name of the user needed to connect to the application.
Password	The password of the user needed to connect to the application.
Protocol	Choose which security model to use to access the service: ➤ **LDAP**. Discovery uses an unprotected connection. ➤ **LDAPS**. Discovery uses an SSL connection.
LDAP Authentication Method	**Simple**. The supported authentication method.

Parameter	Description
Trust Store File Path	The file containing trusted certificates. To import certificates into the Trust Store file: ➤ Create a new Trust Store or use the default Java Trust Store: <java-home>/lib/security/cacerts ➤ Enter the full path to the LDAP Trust Store file.
Trust Store Password	The LDAP Trust Store password used to access the Trust Store file. This password is set during the creation of a new Trust Store. If the password has not been changed from the default, use **changeit** to access the default Java Trust Store.

NetApp Protocol

Parameter	Description
Port Number	The port number. The default is **8088**.
User Name	The name of the user needed to connect to the application.
User Password	The password of the user needed to connect to the application.

NNM Protocol

Parameter	Description
Connection Timeout	Time-out in milliseconds after which the Data Flow Probe stops trying to connect to the NNMi server.
NNM Password	The password for the specified NNMi Web service (for example, Openview).
NNM User name	The user name for connecting to the NNMi console. This user must have the NNMi Administrator or Web Service Client role.

Parameter	Description
NNM Webservice Port	The port for connecting to the NNMi console. This field is pre-filled with the port that the JBoss application server uses for communicating with the NNMi console, as specified in the following file: ➤ Windows: %NnmDataDir%\shared\nnm\conf\nnm.ports.properties ➤ UNIX: $NnmDataDir/shared/nnm/conf/nnm.ports.properties For non-SSL connections, use the value of jboss.http.port, which is 80 or 8004 by default (depending on the presence of another Web server when NNMi was installed). For SSL connections, use the value of **jboss.https.port**, which is 443 by default.
NNM Webservice Protocol	The protocol for the NNMi Web service (the default is **http**).
UMCBD Password	The password for the Web service (the default is **admin**).
UCMDB Username	A valid UCMDB Web service account name with the UCMDB Administrator role (the default is **admin**).
UCMDB Webservice Port	The port for connecting to the UCMDB Web service. If you are using the default UCMDB configuration, use port **8080** (for non-SSL connections to UCMDB).
UCMDB Webservice Protocol	The protocol for the RTSM Web service (the default is **http**).

🔍 NTCMD Protocol

Parameter	Description
Connection Timeout	Time-out in milliseconds after which the Probe stops trying to connect to the NTCMD server.
User Name	The name of the user needed to connect to the host as administrator.
Password	The password of the user needed to connect to the host as administrator.
Windows Domain	The Windows domain in which the credentials are defined. If this field is left empty or is not a valid domain, the NTCMD protocol assumes the user is defined locally on the host.

Note: This protocol uses the DCOM protocol for connecting to remote machines. The DCOM protocol requires that the following ports are open: 135, 137, 138, and 139. In addition the DCOM protocol uses arbitrary ports between 1024 and 65535, but there are ways to restrict the port range used by WMI/DCOM/RPC. In addition, for information about for configuring DCOM to work with firewalls, see http://support.microsoft.com/kb/154596/en-us.

🔍 PowerShell Protocol

Field	Description
Connection Timeout	Time-out in milliseconds after which the Probe stops trying to connect to the destination machine.
User Name	The name of the user that can connect to the remote machine by PowerShell.
User Password	The password of the user that can connect to the remote machine by PowerShell.
Windows Domain	The Windows domain on which the credentials are defined. If this field is empty, PowerShell assumes that the user is defined locally on the host.

🔍 Remedy Protocol

Field	Description
Connection Timeout	Time-out in milliseconds after which the Data Flow Probe stops trying to connect to the Remedy application server.
Remedy Password	Enter the password of the user account that enables access to Remedy/Atrium through the Java API.
Remedy Username	Enter the user name that enables access to Remedy/Atrium through the Java API.

🔍 SAP JMX Protocol

Parameter	Description
Port Number	The SAP JMX port number. The SAP JMX Port structure is usually 5<System Number>04. For example, if the system number is 00, the port is 50004. Leave this field empty to try to connect to the discovered SAP JMX port; SAP JMX port numbers are defined in the **portNumberToPortName.xml** configuration file.
Connection Timeout	Time-out in milliseconds after which the Probe stops trying to connect to the SAP JMX console.
User Name	The name of the user needed to connect to the application as administrator.
Password	The password of the user needed to connect to the application as administrator.

🔍 SAP Protocol

Parameter	Description	
Connection Timeout	Time-out in milliseconds after which the Probe stops trying to connect to the SAP console.	
User Name	The name of the user needed to log in to the SAP system. The user should have the following permissions:	
	Authorization Object	**Authorization**
	S_RFC	For the **S_RFC** object, obtain privileges: RFC1, SALX, SBDC, SDIF, SDIFRUNTIME, SDTX, SLST, SRFC, STUB, STUD, SUTL, SXMB, SXMI, SYST, SYSU, SEU_COMPONENT.
	S_XMI_PROD	EXTCOMPANY=MERCURY;EXTPRODUCT=DARM;INTERFACE=XAL
	S_TABU_DIS	DICBERCLS=SS; DICBERCLS=SC
Password	The password of the user needed to log in to the SAP system.	

Parameter	Description
SAP Client Number	It is recommended to use the default value (**800**).
SAP Instance Number	By default, set to **00**.
SAP Router String	A route string describes the connection required between two hosts using one or more SAProuter programs. Each of these SAProuter programs checks its Route Permission Table (http://help.sap.com/saphelp_nw04/helpdata/en/4f/992dfe446d11d189700000e8322d00/content.htm) to see whether the connection between its predecessor and successor is allowed. If it is, SAProuter sets it up.

Siebel Gateway Protocol

Parameter	Description
Connection Timeout	Time-out in milliseconds after which the Probe stops trying to connect to the Siebel Gateway console.
User Name	The name of the user needed to log on to the Siebel enterprise.
Password	The password of the user needed to log on to the Siebel enterprise.

Parameter	Description
Siebel Site Name	The name of the Siebel Enterprise.
Path to Siebel Client	The location on the Probe machine of the Siebel driver folder, where you copied srvrmgr. For details, see "Prerequisites - Other" in the *HP Universal CMDB Discovery and Integration Content Guide* PDF.
	Note:
	➤ If there are several protocol entries with different srvrmgr versions, the entry with the newer version should appear before the entry with the older version. For example, to discover Siebel 7.5.3. and Siebel 7.7, define the protocol parameters for Siebel 7.7 and then the protocol parameters for Siebel 7.5.3.
	➤ **Siebel discovery.** If the Data Flow Probe is installed on a 64-bit machine on a Windows platform, place the **ntdll.dll**, **MSVCR70.DLL**, and **msvcp70.dll** drivers together with the Siebel drivers in the Siebel driver folder on the Probe machine.
	These drivers usually exist on a 32-bit machine and can be copied to the 64-bit machine.

🔍 SNMP Protocol

Parameter	Description
Port Number	(For SNMP versions v1, v2, and v3) The port number on which the SNMP agent listens.
Connection Timeout	Time-out in milliseconds after which the Probe stops trying to connect to the SNMP agent.
Retry Count	The number of times the Probe tries to connect to the SNMP agent. If the number is exceeded, the Probe stops attempting to make the connection.
Versions 1, 2	**Community.** Enter the authentication password you used when connecting to the SNMP service community (which you defined when configuring the SNMP service—for example, a community for read-only or read/write).

Parameter	Description
Version 3	**Authentication Method**: Select one of the following options for securing the access to management information:
	➤ **noAuthNoPriv.** Using this option provides no security, confidentiality, or privacy at all. It can be useful for certain applications, such as development and debugging, to turn security off. This option requires only a user name for authentication (similar to requirements for v1 and v2).
	➤ **authNoPriv.** The user logging on to the management application is authenticated by the SNMP v3 entity before the entity allows the user to access any of the values in the MIB objects on the agent. Using this option requires a user name, password, and the authentication algorithm (HMAC-MD5 or HMAC-SHA algorithms).
	➤ **authPriv.** The user logging on to the management application is authenticated by the SNMP v3 entity before the entity allows the user to access any of the values in the MIB objects on the agent. In addition, all of the requests and responses from the management application to the SNMP v3 entity are encrypted, so that all the data is completely secure. This option requires a user name, password, and an authentication algorithm (HMAC-MD5 or HMAC-SHA).
	User Name: The name of the user authorized to log on to the management application.
	Password: The password used to log on to the management application.
	Authentication Algorithm: The MD5 and SHA algorithms are supported.
	Privacy Key: The secret key used to encrypt the scoped PDU portion in an SNMP v3 message.
	Privacy Algorithm: The DES, 3DES, AES-128, AES-192 and AES-256 algorithms are supported.

Troubleshooting and Limitations

Problem. Failure to collect information from SNMP devices.

➤ **Solution 1**. Verify that you can actually access information from your Network Management station by using a utility that can verify the connectivity with the SNMP agent. An example of such a utility is **GetIf**.

➤ **Solution 2**. Verify that the connection data to the SNMP protocol has been defined correctly in the Add Protocol Parameter dialog box. For details, see "Protocol Parameter Dialog Box" on page 165.

➤ **Solution 3**. Verify that you have the necessary access rights to retrieve data from the MIB objects on the SNMP agent.

SQL Protocol

Parameter	Description
Database Type	The database type. Select the appropriate type from the box.
Port Number	The port number on which the database server listens. ➤ If you enter a port number, DFM tries to connect to a SQL database using this port number. ➤ **For an Oracle database**: If there are many Oracle databases in the environment and you do not want to have to create a new credential for each separate database port, you leave the Port Number field empty. When accessing an Oracle database, DFM refers to the portNumberToPortName.xml file and retrieves the correct port number for each specific Oracle database port. **Note**: You can leave the port number empty on condition that: ➤ All Oracle database instances are added to the portNumberToPortName.xml file. For details, see "portNumberToPortName.xml File" on page 174. ➤ The same user name and password is needed to access all Oracle database instances.
Connection Timeout	Time-out in milliseconds after which the Probe stops trying to connect to the database.
User Name	The name of the user needed to connect to the database.

Parameter	Description
Password	The password of the user needed to connect to the database.
Instance Name	The name of the database instance — the Oracle system identification or the DB2 database name. When connecting to any database, you can leave this field empty. In this case, DFM takes the SID from the Triggered CI data value: **${DB.name:NA}**. For details, see "Trigger CIs and Trigger Queries" on page 33.
Encryption method	**None**. **SSL**. For Oracle only.
Trust Store File Path	Enter the full path to the SSL trust store file. To use the trust store file, do one of the following: ➤ Enter the name (including the extension) and place the file in the following resources folder: **C:\hp\UCMDB\DataFlowProbe\runtime\ probeManager\discoveryResources**. ➤ Insert the trust store file full path.
Trust Store Password	The SSL trust store password.

SSH Protocol

For details on configuring F-Secure when discovering Windows machines on which the F-Secure application is running on an SSH server, see the *HP Universal CMDB Discovery and Integration Content Guide* PDF.

Parameter	Description
Port Number	By default an SSH agent uses port 22. If you are using a different port for SSH, enter that port number.
Connection Timeout	Time-out in milliseconds after which the Probe stops trying to connect to the remote machine. For the UNIX platform: If your server is slow, it is recommended to change Timeout to 40000.

Parameter	Description
Version	**SSH2**. Connect through SSH-2 only. **SSH1**. Connect through SSH-1 only. **SSH2 or SSH1**. Connect through SSH-2 and in case of error (if SSH-2 is not supported by the server), try to connect through SSH-1.
Shell Command Separator	The character that separates different commands in a shell (to enable the execution of several commands in the same line). For example, in UNIX, the default shell command separator is a semicolon (**;**). In Windows, the shell command separator is an ampersand (**&**).
Authentication Method	Choose one of the following authentication options to access SSH: ➤ **password**. Enter a user name and password. ➤ **publickey**. Enter the user name and path to the key file that authenticates the client. ➤ **keyboard-interactive**. Enter questions and answers. For details, see "Prompts and Responses" on page 124.
User Name	The name of the user needed to connect to the host through the SSH network protocol.
Password	The password of the user needed to connect to the host.
Key File Path	(Enabled when the publickey authentication method is selected.) Location of the authentication key. (In certain environments, the full key path is required to connect to an SSH agent.) **Note**: Enter the full path to the key file on the Probe machine.

Parameter	Description
Prompts and Responses	(Enabled when the keyboard-interactive authentication method is selected.) A method whereby the server sends one or more prompts to enter information and the client displays them and sends back responses keyed-in by the user. The following is an example of prompts and expected responses: **Prompt**: Please enter your user name. **Response**: Shelly-Ann **Prompt**: What is your age? **Response**: 21 **Prompt**: This computer is HP property. Press y to enter. **Response**: y To create these prompts and responses, enter the following strings in the fields, separated by commas: **Prompts**: user,age,enter **Response**: Shelly-Ann,21,y You can enter the full string as it appears in the SSH prompt, for example: or you can enter a key word, for example, **user**. DFM maps this word to the correct prompt.

Parameter	Description
Sudo paths	The full paths to the sudo command. Paths are separated by commas.
Sudo commands	A list of commands that can be executed with the sudo command. Commands are separated by commas. For all commands to be executed with sudo, add an asterisk (*****) to this field. This field accepts a sudo command that prompts for the user's password.

Troubleshooting

Problem. Failure to connect to the TTY (SSH/Telnet) agent.

Solution. To troubleshoot connectivity problems with the TTY (SSH/Telnet) agent, use a utility that can verify the connectivity with the TTY (SSH/Telnet) agent. An example of such a utility is the client tool PuTTY.

🔍 Telnet Protocol

Parameter	Description
Port Number	The port number. By default a Telnet agent uses port 23. If you are using a different port for Telnet in your environment, enter the required port number.
Connection Timeout	Time-out in milliseconds after which the Probe stops trying to connect to the remote machine. **For UNIX platforms**: If your server is slow, it is recommended to change Connection Timeout to 40000.
Authentication Method	Choose one of the following authentication options to access Telnet: ➤ **password**. Enter a user name and password. ➤ **keyboard-interactive**. Enter questions and answers. For details, see "Prompts and Responses" on page 124.
User Name	The name of the user needed to connect to the host.
Password	The password of the user needed to connect to the host.

Parameter	Description
Prompts and Responses	(Enabled when the keyboard-interactive authentication method is selected.) A method whereby the server sends one or more prompts to enter information and the client displays them and sends back responses keyed-in by the user.
	The following is an example of prompts and expected responses:
	Prompt: Please enter your user name.
	Response: Shelly-Ann
	Prompt: What is your age?
	Response: 21
	Prompt: This computer is HP property. Press y to enter.
	Response: y
	To create these prompts and responses, enter the following strings in the fields, separated by commas:
	Prompts: user,age,enter
	Response: Shelly-Ann,21,y
	You can enter the full string as it appears in the Telnet prompt, for example:
	or you can enter a key word, for example, **user**. DFM maps this word to the correct prompt.

Parameter	Description
Sudo paths	The full paths to the sudo command. Paths are separated by commas.
Sudo commands	A list of commands that can be executed with the sudo command. Commands are separated by commas. For all commands to be executed with sudo, add an asterisk (*****) to this field.

Troubleshooting and Limitations

Problem. Failure to connect to the TTY (SSH/Telnet) agent.

Solution. To troubleshoot connectivity problems with the TTY (SSH/Telnet) agent, use a utility that can verify the connectivity with the TTY (SSH/Telnet) agent. An example of such a utility is the client tool PuTTY.

Limitation. The Telnet protocol does not support discovery of Windows Telnet servers.

UDDI Registry Protocol

Parameter	Description
Connection Timeout	Time-out in milliseconds after which the Probe stops trying to connect to the UDDI Registry.
UDDI Registry URL	The URL where the UDDI Registry is located.

🔍 VMware Infrastructure Management (VIM) Protocol

Parameter	Description
Connection Timeout	Time-out in milliseconds after which the Probe stops trying to connect to VMware Infrastructure.
Port Number	DFM uses the number defined here when processing one of the Network – VMware jobs: If the port number is left empty, DFM performs a WMI query to extract the port number from the registry. DFM queries **HKLM\SOFTWARE\VMware, Inc.\VMware VirtualCenter** and searches for the **HttpsProxyPort** or **HttpProxyPort** attributes: ➤ If the **HttpsProxyPort** attribute is found, DFM uses its value for the port and sets the prefix to **HTTPS**. ➤ If the **HttpProxyPort** attribute is found, DFM uses its value for the port and sets the prefix to **HTTP**.
Use SSL	**true**: DFM uses a Secure Sockets Layer (SSL) protocol to access VMware Infrastructure, and the prefix is set to **HTTPS**. **false**: DFM uses the http protocol.
User Name	The name of the user needed to connect to VMware Infrastructure.
Password	The password of the user needed to connect to VMware Infrastructure.

🔍 WebLogic Protocol

Parameter	Description
Port Number	If you enter a port number, DFM tries to connect to WebLogic using this port number.
	However, say you know that there are many WebLogic machines in the environment and do not want to have to create a new credential for each machine. You leave the Port Number field empty. When accessing a WebLogic machine, DFM refers to the WebLogic port (defined in portNumberToPortName.xml) already found on this machine (by TCP scanning, using the **Network Connection – Active Discovery** module).
	Note: You can leave the port number empty on condition that:
	➤ All WebLogic ports are added to the portNumberToPortName.xml file. For details, see "portNumberToPortName.xml File" on page 174.
	➤ The same user name and password is needed to access all WebLogic instances.
Connection Timeout	Time-out in milliseconds after which the Probe stops trying to connect to the WebLogic application server.
User Name	The name of the user needed to connect to the application.
Password	The password of the user needed to connect to the application.
Protocol	An application-level protocol that determines whether DFM should connect to the server securely. Enter **http** or **https**.
Trust Store File Path	Enter the full path to the SSL trust store file.
	To use the trust store file, do one of the following:
	➤ Enter the name (including the extension) and place the file in the following resources folder: **C:\hp\UCMDB\DataFlowProbe\runtime\ probeManager\discoveryResources\j2ee\weblogic\ \<WebLogic version>**
	➤ Insert the trust store file full path.

Parameter	Description
Trust Store Password	The SSL trust store password.
Key Store File Path	Enter the full path to the SSL keystore file. To use the keystore file, do one of the following: ➤ Enter the name (including the extension) and place the file in the following resources folder: **C:\hp\UCMDB\DataFlowProbe\runtime\ probeManager\discoveryResources\j2ee\weblogic\ <WebLogic version>** ➤ Insert the keystore file full path.
Key Store Password	The password for the keystore file.

🔍 WebSphere Protocol

Parameter	Description
Port Number	The protocol port number as provided by the WebSphere system administrator. You can also retrieve the protocol port number by connecting to the Administrative Console using the user name and password provided by the WebSphere system administrator. In your browser, enter the following URL: **http:/ <host>:9060/admin**, where: ➤ **<host>** is the IP address of the host running the WebSphere protocol ➤ **9060** is the port used to connect to the WebSphere console Access **Servers** > **Application Servers** > **Ports** > **SOAP_CONNECTOR_ADDRESS** to retrieve the required port number.
Connection Timeout	Time-out in milliseconds after which the Probe stops trying to connect to the WebSphere server.

Parameter	Description
User Name	The name of the user needed to connect to the application.
Password	The password of the user needed to connect to the application.
Trust Store File Path	The name of the SSL trust store file. To use the trust store file, do one of the following: ➤ Enter the name (including the extension) and place the file in the following resources folder: **C:\hp\UCMDB\DataFlowProbe\runtime\ probeManager\discoveryResources\j2ee\websphere** ➤ Insert the trust store file full path.
Trust Store Password	The SSL trust store password.
Key Store File Path	The name of the SSL keystore file. To use the keystore file, do one of the following: ➤ Enter the name (including the extension) and place the file in the following resources folder: **C:\hp\UCMDB\DataFlowProbe\runtime\ probeManager\discoveryResources\j2ee\websphere** ➤ Insert the keystore file full path.
Key Store Password	The password for the keystore file.

🔍 WMI Protocol

Parameter	Description
User Name	The name of the user needed to connect to the host.
Password	The password of the user needed to connect to the host.
Windows Domain	The Windows domain in which the credentials are defined. If this field is left empty or is not a valid domain, the WMI protocol assumes the user is defined locally on the host.

Note: This protocol uses the DCOM protocol for connecting to remote machines. The DCOM protocol requires that the following ports are open: 135, 137, 138, and 139. In addition the DCOM protocol uses arbitrary ports between 1024 and 65535, but there are ways to restrict the port range used by WMI/DCOM/RPC. In addition, for information about for configuring DCOM to work with firewalls, see http://support.microsoft.com/kb/154596/en-us.

🔍 Data Flow Probe Log Files

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 Probe's log files, log in to the JMX console (http://<probe_machine>:8090/jmx-console/) and, from the main page, select the **GeneralUtils** mbean. Activating the **executeLogGrabber** function zips all the Probe's log files. Save the .zip file locally on your client machine.

General Logs

WrapperProbeGw.log

Records all the Probe's console output in a single log file.

Level	Description
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.

Level	Description
Error	All errors in the Probe components.
Information	N/A
Debug	N/A

Basic Troubleshooting. Check this log to verify if errors occurred in the Probe components.

probe-infra.log

List of all infrastructure messages.

Level	Description
Error	All infrastructure errors.
Information	Information about infrastructure actions.
Debug	Messages mainly for debug purposes.

Basic Troubleshooting. Messages from the Probe's infrastructure only.

wrapperLocal.log

When running the Probe in separate mode (with the Probe Manager and Probe Gateway installed on separate machines), a log file is also saved to the Probe Manager.

Level	Description
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.

Probe Gateway Logs

probeGW-taskResults.log

This log records all the task results sent from the Probe Gateway to the server.

Level	Description
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

➤ 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.

probeGW-tasks.log

This log records all the tasks received by the Probe Gateway.

Level	Description
Error	N/A
Information	N/A
Debug	The task's XML.

Basic Troubleshooting

➤ 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

Performance statistics dump, collected every predefined period of time, which includes memory information and thread pool statuses.

Level	Description
Error	N/A
Information	N/A
Debug	N/A

Basic Troubleshooting

➤ Check this log to investigate memory issues over time.

➤ The statistics are logged every 1 minute, by default.

probeMgr-adaptersDebug.log

This log contains messages that are created following a job execution.

🔍 The DiscoveryProbe.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 **DiscoveryProbe.properties** file. To edit the parameters, open **DiscoveryProbe.properties** in a text editor.

The **DiscoveryProbe.properties** file is located in the following folder: **C:\hp\UCMDB\DataFlowProbe\conf**.

Caution: If you update the parameters in the **DiscoveryProbe.properties** file, you must restart the Probe so that it is updated with the changes.

The **DiscoveryProbe.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.

➤ **Discovery 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, 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.)

DiscoveryProbe.properties Parameters

Server Connection Definitions

Parameter Name (A-Z)	Purpose	Type	Value Description
appilog.agent.Probe .BasicAuth.Realm	Used only when the Probe should be connected to the UCMDB server using proxy server	string	Default: None
appilog.agent.Probe .DownloadingTime out	Timeout in ms. for download configuration files and userExt files (serverData files).	long	Default: 300000
appilog.agent.probe .protocol	Defines the protocol used to communicate between the Probe Gateway and the Server.	string	**HTTP** or **HTTPS** (SSL) Default: **HTTP**
appilog.agent.Probe .ServerTimeout	Timeout in ms. for Probe requests going to the server.	long	Default: 180000
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.

Parameter Name (A-Z)	Purpose	Type	Value Description
appilog.agent.Probe .JMX.BasicAuth. User appilog.agent.Probe .JMX.BasicAuth. Pwd	Authentication data for the Probe JMX.	string bytes	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 (the **getEncryptedKey Password** operation in the **MainProbe** MBean).
appilog.collectors. domain	The domain which the Probe Gateway belongs to (formerly known as the **Domain** of the Probe).	string	Default: **DefaultProbe**
appilog.collectors. domain.type	The type of the domain.	string	**customer**; **external** Default: **customer**
appilog.collectors.p robe.name	The Probe name used for identification on UCMDB server	string	Uses the value defined during installation
appilog.collectors. probe.name	The Probe ID attribute. Used to identify the Probe Gateway by the UCMDB server. The server uses this ID to transfer tasks to the appropriate Probe Gateway.	string	Default: the machine name
http.proxyHost	Used only when the Probe should be connected to the UCMDB server using proxy server	string	DNS names
http.proxyPass	Used only when the Probe should be connected to the UCMDB server using proxy server	string	Default: None

Parameter Name (A-Z)	Purpose	Type	Value Description
http.proxyPort	Used only when the Probe should be connected to the UCMDB server using proxy server	int	Default: None
http.proxyRealm	Used only when the Probe should be connected to the UCMDB server using proxy server	string	Default: None
http.proxyUser	Used only when the Probe should be connected to the UCMDB server using proxy server	string	Default: None
jettyHttpPort	The port of the jetty server used by Probe.	int	Default: **8090**
jettyHttpsPort	The https port of the jetty server used by Probe	int	Default: **8453**
server.webApp. name	Name of the server Web application (.war file) responsible for the Probe.	string	Default: **mam-collectors**
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

Discovery Probe Definitions

Parameter Name	Purpose	Type	Value Description
appilog.agent. local.jdbc.user appilog.agent. local.jdbc.pwd	My SQL authentication info	string bytes	To change the DB password: **1** The OOTB script set_dbuser_password.cmd can be used in order to change the password of the default MySQL user. **2** The password value in the properties file should be encrypted. Encrypt the password using the Probe JMX (getEncryptedKey Password operation in MainProbe MBean).
appilog.agent. probe.jdbc.driver appilog.agent. probe.jdbc.uri	Probe GW database info	string string	Default: **com.mysql.jdbc.Driver** Default: **jdbc:mysql://localhost/ probeMgr?autoReconnect=true**
appilog.agent. probe.jdbc.user appilog.agent. probe.jdbc.pwd	Probe GW authentication info	string bytes	Password has to be encrypted. Encrypt password using the Probe JMX (**getEncryptedKey Password** operation in **MainProbe** MBean).
appilog.agent.loc al.jdbc.driver appilog.agent.loc al.jdbc.uri	Probe Manager database info	string string	Default: **com.mysql.jdbc.Driver** Default: **jdbc:mysql://localhost/ probeMgr?autoReconnect=true**
appilog.agent.net flow.jdbc.uri	Netflow database info	boolean	jdbc:mysql://localhost/ netflow?autoReconnect=true&jd bcCompliantTruncation=false

Parameter Name	Purpose	Type	Value Description
appilog.collectors .probeLocal Union	true: Probe GW process should also run a Probe Manager on same JVM. false: Probe manager runs separately	boolean	Default: **true**
appilog.collectors .ProbeUseSpecific RMIPortFrom	Internal communication port	int	Default: **1199** **0**: Ports are allocated automatically
appilog.collectors .rmi.gw.port	Communication port between Probe GW and Probe Managers in case they are installed on seperate processes	int	Default: **1742**. 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**. Note: This value should be the same for all installed Probe Managers belonging to this Probe Gateway.
appilog.collectors .storeDomain ScopeDocument	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 appilog.collectors .probe.ip	The Probe Manager & Gateway IP addresses or DNS names	string string	DNS Names
appilog.collectors .probe.html.port appilog.collectors .local.html.port	Probe JMX console ports. Used to manage the Probe components.	int int	Default: **1977** Default: **1978**

Probe Gateway Configurations

Parameter Name	Purpose	Type	Value Description
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.retrieve tasksFromServer. interval	The interval in ms. between task requests from the server by the Probe Gateway.	long	Default: **15000**
appilog.agent. probe.saveResultsI nBKPTable	**true**: Results sent to the Server are stored in the database in a backup table. **false**: Results are not stored in a backup table.	boolean	Default: **false**

Probe Manager Configurations

Parameter Name	Purpose	Type	Value Description
appilog.agent. local.max.worker. runtime appilog.agent. local.max.stuck appilog.agent. local.check.stuck Threads	Maximal time (in msec) which a worker thread is allowed to run. After this period it is considered as stuck. 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.	long int boolean	Default: **900000** Default: **10** 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.process.result.dataValidation.content	Defines whether to validate data reported to the UCMDB server by content. Deals mainly with reported values (i.e. attribute value), rather than metadata of objects.	boolean	Default: true
appilog.agent.local.process.result.checkMultiUpdate	Defines whether to check data consistency on objects.	boolean	Default: true

Parameter Name	Purpose	Type	Value Description
appilog.agent.local.process.result.filterRedundant.filterIgnoredCIs	➤ **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.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.process.result.dataValidation.validLinks	true - validate links are legal. false - do not validate links.	boolean	Default: true
appilog.agent.local.process.result.filterRedundant	true - filter results which have been already sent to server. false - disable filter.	boolean boolean	Default: **true** Default: **true**

Parameter Name	Purpose	Type	Value Description
appilog.agent. local.discovery AnalyzerFrom Eclipse	True: DiscoveryAnalyzer is executed from Eclipse. False: DiscoveryAnalyzer is not executed from Eclipse.	boolean	Default: **false**
appilog.agent .local.maxTask ResultSize	Chunk maximal size of results being sent to the server.	int	Default: **20000**
appilog.agent. local.probe.restart .interval	Interval (in msec) before auto-restarts of the Probe Manager.	long	Default: **900000**
appilog.agent. local.process. result.autoDelete	true - send autodelete 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. result. filter Redundant is enabled.	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.fixLinks Direction	true - fix direction of illegal links. false - otherwise.	boolean	Default: **true**
appilog.agent .local.process .result.warnOnM ultiUpdate	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 absent by default, but gets its value from the global parameter.	boolean	Default: **true**
appilog.agent. local.serverdata. sync.timeout	Timeout (in msec) for the Probe to sync with Server data before starting executing tasks.	long	Default: **60000**

Parameter Name	Purpose	Type	Value Description
appilog.agent. local.special Characters 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.Default ResultGroupMax Objs	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: **5000**
appilog.collectors. probemgr.Default ResultGroupMin Time		long	Default: **30000** (in ms.) Relation between two keys: **OR**

I18N Parameters

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

🔍 Data Flow Probe Setup User Interface

This section includes (in alphabetical order):

Add/Edit IP Range Dialog Box

Enables you to set the network range for discovery. 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	Select the required Probe in the Domains and Probes pane and then click the **Add IP range** button in the Ranges pane (**Admin** > **RTSM Administration** > **Data Flow Management** > **Data Flow Probe Setup** > *<Domain>* > **Probes** > *<Probe>* > **Ranges pane**)
Important information	If you define a range that is out of the scope of the network on which the Probe is installed, a warning message informs you that the Probe is not included in the range. Answer **Yes** to save the current range without including the Probe in the range. Answer **No** to continue editing without saving the current range.
Relevant tasks	"How to Use Discovery Control Panel – Advanced Mode Workflow" on page 331

User interface elements are described below:

UI Element (A–Z)	Description
	To exclude an IP range from discovery, click the **Add IP range** button.
	To delete the excluded part of an IP range, select the excluded range and click the **Remove IP range** button.
	To edit the excluded part of an IP range, click the **Edit IP range** button. For details, see **Exclude Ranges** below.

UI Element (A–Z)	Description
Exclude Ranges	Click the **Add IP range** button to open the Add IP Range dialog box (to add a new IP range) or the **Edit IP range** button to open the Edit IP Range Dialog box (to change an existing IP range), and then click **Advanced** to exclude part of a range. In the Exclude IP Range dialog box, enter the range to exclude.

<div style="margin-left:2em">

Note:

➤ You must enter a range (in the Add/Edit IP Range dialog box) before you can enter the excluded range.

➤ The rules for entering an excluded range are the same as for entering a range. For details, see **Range** below.

➤ Use this feature to divide a network range into several subranges.

For example, if the range is
10.0.64.0 – 10.0.64.255

and you define three excluded ranges:
10.0.64.45 – 10.0.64.50
10.0.64.65 – 10.0.64.70
10.0.64.89 – 10.0.64.95

the ranges to be discovered are:
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

</div>

UI Element (A–Z)	Description
Range	The rules for defining an IP address range are as follows: ➤ 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 start IP and end IP must belong to the same A class network. For example, 1.1.1.1 - 1.2.2.2. ➤ The range can include an asterisk (*), representing any number in the range of 0-255. ➤ 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.*. ➤ Two Probes in the same domain cannot have the same IP address in their range.

Add/Edit Policy Dialog Box

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

To access	Admin > RTSM Administration > Data Flow Management > Data Flow Probe Setup > Domains and Probes > Details pane > Job Execution Policy section. Select an existing policy and click Edit Policy, or click the Add Policy button.
See also	➤ "Job Execution Policies" on page 94 ➤ "Job Execution Policy Pane" on page 159 ➤ "Domain Credential References" on page 103

User interface elements are described below:

UI Element (A–Z)	Description
Related jobs	➤ **Allow all.** Run the job execution policy on all jobs. ➤ **Total blackout.** The policy does not run on any jobs. ➤ **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. For allowed and disallowed jobs, click the **Add job** or **Remove job** button to choose specific jobs to be included in, or excluded from, the policy. If you click the **Add job** button, the Choose Discovery Jobs dialog box opens.
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	The date and time during which the policy is active. Click the button to open the Edit Timetable dialog box.

🔍 Add New Domain Dialog Box

Enables you to add a domain.

To access	Click the **Add Domain or Probe** button in the Domains and Probes pane.
Important information	In a version 8.01 or later environment that has been upgraded from version 6.x, to enable data to be modelled similarly as in the previous version, you must define the Probes as belonging to the **External** domain and not to the **Customer** domain.

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	➤ **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.

✸ Add New Probe Dialog Box

Enables you to add a Probe.

To access	Click the **Add Domain or Probe** button in the Domains and Probes pane.
Important information	➤ To add a Probe to an existing domain, select **Probes** in the Domains and Probes pane and click the **Add Domain or Probe** button.
	➤ To add a Probe to a new domain, create a domain, then add the Probe to the domain.
	➤ Two Probes in the same domain cannot have the same IP address in their range.
	➤ When a Probe is activated, it is added automatically and its status changes to **connected.** For details, see "Launch the Probe from the Start Menu" on page 99 or "Launch the Probe in a Console" on page 100.

✸ Choose Discovery Jobs Dialog Box

Enables you to choose the jobs that are to be added to, or excluded from, the job execution policy.

To access	Select **Allowed Jobs** or **Disallowed jobs** in the Edit Policy dialog box and click the ➕ button.

User interface elements are described below:

UI Element (A–Z)	Description
<Installed packages>	Locate the job to be included in, or excluded from, the policy. (Use the SHIFT or CTRL key to select several packages.)

🔩 Data Flow Probe Setup Window

Enables you to define a new domain or to define a new Probe for an existing domain. Also enables you to define the connection data for each protocol.
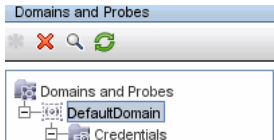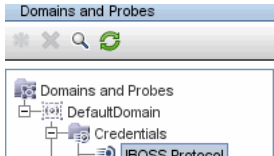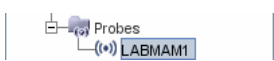
To access	**Admin** > **RTSM Administration** > **Data Flow Management** > **Data Flow Probe Setup**
Important information	➤ For details on the Domains and Probes pane, see "Domains and Probes Pane" on page 162. ➤ For details on the Details pane, see "Details Pane" on page 155.
See also	"Domain Credential References" on page 103

🔩 Details Pane

Enables you to view the Probes running under all domains and to add an execution policy to jobs (to schedule time periods when jobs should not run).

To access	Click an object in the Domains and Probes pane.
Important information	Depending on what you select in the Domains and Probes pane, different information is displayed in the Details pane.

Displayed Information

If You Select...	The Information Displayed Is...
	Domains and Probes. You can view details on all Probes and you can define and edit job execution policies. For details, see "Details Pane (Probe)" on page 157 and "Job Execution Policy Pane" on page 159.
	A specific domain. You can add a description and view a list of Probes running in that domain. For details, see "Details Pane (Probe)" on page 157 and "Description Pane" on page 158.
	A specific protocol. You can add protocol parameters and you can view details on the protocol, including user credentials. For details, see "Details Pane (Protocol)" on page 157 and "Domain Credential References" on page 103.
	A specific Probe. You can view details on the Probe, including range information. You can also add ranges to, or exclude ranges from, the Probe, and you can remove a Probe from RTSM. For details, see "Ranges Pane" on page 160, "Details Pane (Probe)" on page 157, and "Data Flow Probes Pane" on page 158.

Details Pane (Probe)

User interface elements are described below:

UI Element (A–Z)	Description
Last time probe accessed	The last time that the Probe was accessed on the server machine.
Probe IPs	The IP of the Probe machine.
Status	➤ **Connected.** The Probe has successfully connected to the server (the Probe connects every few seconds). ➤ **Connected (suspended).** The Probe is suspended such that no jobs can be run on the Probe. ➤ **Disconnected.** The Probe is not connected to the server.
Version	The version of the Probe. **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 Probe. To ensure compatibility, you must upgrade the Probe manually. For details, see the section about manually upgrading the Probe in the *HP Universal CMDB Deployment Guide* PDF.

Details Pane (Protocol)

This pane is displayed if you select a specific protocol. User interface elements are described below:

UI Element (A–Z)	Description
	Add new connection details for selected protocol type.
	Remove a protocol.
	Edits a protocol. For details, see "Protocol Parameter Dialog Box" on page 165.

UI Element (A–Z)	Description
⬆️ ⬇️	Click a button to move a protocol up or down to set the order in which credential sets are attempted. DFM executes all the protocols in the list with the first protocol taking priority.
Protocol	Click to view details on the protocol, including user credentials.

Description Pane

User interface elements are described below:

UI Element (A–Z)	Description
Description	The description that was entered during domain creation.
Domain Type	For details, see Domain Type in "Add New Domain Dialog Box" on page 153.

Data Flow Probes Pane

Enables you to view a list of all Probes connected to the server.

To access	Click **Domains and Probes** or a domain.

User interface elements are described below:

UI Element (A–Z)	Description
IP	The IP range defined during Probe creation.
Last Access Time	The last time that the Probe requested tasks from the server.
Name	The Probe name as it appears in DFM.

UI Element (A–Z)	Description
Probe Version	The version of the Probe.
	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 Probe. To ensure compatibility, you must upgrade the Probe manually. For details, see the section about manually upgrading the Probe in the *HP Universal CMDB Deployment Guide* PDF.
Status	➤ **Connected.** The Probe has successfully connected to the server (the Probe connects every few seconds).
	➤ **Connected (suspended).** The Probe is suspended such that no jobs can be 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 not run.

To access	**Admin** > **RTSM Administration** > **Data Flow Management** > **Data Flow Probe Setup**. Select **Domains and Probes**.
Important information	Jobs that have a listening functionality (that do not perform discovery, for example, but listen to SNMP traps) are not included in a policy.
See also	➤ "Job Execution Policies" on page 94
	➤ "Domain Credential References" on page 103

User interface elements are described below:

UI Element (A–Z)	Description
⬆ ⬇	Move the policy up or down. DFM executes all the policies in the list with the first policy taking priority. If a job is included in two policies, DFM executes the first policy only for that job.
✚	Add a policy.
✖	Remove a policy.
✎	Edit a policy. Opens the Edit Policy dialog box.
Jobs	The jobs that are affected by the policy.
Probes	The Probes that are affected by the policy.
Time	The schedule of the policy.

Ranges Pane

Enables you to add and remove ranges that a Probe should work with.

To access	Click a Probe in the Domains and Probes pane.
Important Information	For details on searching for a specific range, see the **Find Probe Range by IP** button in "Domains and Probes Pane" on page 162.

User interface elements are described below:
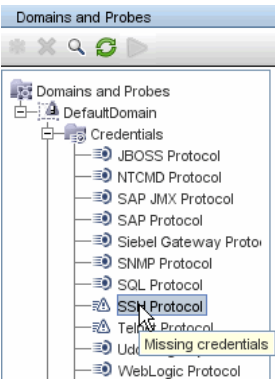
UI Element (A–Z)	Description
✚	Opens the **Add IP Range** dialog box.
✖	Click a range and click the button to remove a range from the list.
✎	Opens the Edit IP Range dialog box.

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 *RTSM Modeling Guide*.
	Imports ranges from a CSV file. Before using this feature, verify that the imported file is a valid CSV file, and that the ranges in the file do not conflict with existing ranges (there are no duplicate or overriding ranges).
Excluded	Displays the IP addresses that have been excluded from the range that the Probe uses to discover CIs. For details, see "Add/Edit IP Range Dialog Box" on page 149.
Range	The network IP addresses that the Probe uses to discover CIs. For details, see "Add/Edit IP Range Dialog Box" on page 149.

🔍 Domains and Probes Pane

Enables you to view, define, or edit a domain, a Probe, or a Probe's credentials, as well as manually upgrade the version of a Probe.

To access	Admin > RTSM Administration > Data Flow Management > Data Flow Probe Setup
Important Information	A missing credential is represented by an icon 🔺, as shown in the following image:
See also	"Job Execution Policies" on page 94

User interface elements are described below:

UI Element (A–Z)	Description
✳	**Add Domain or Probe.** Adds a domain or Probe, depending on what is selected. For details, see "Add New Domain Dialog Box" on page 153 or "Add New Probe Dialog Box" on page 154.
✖	**Remove Domain or Probe.** Deletes a domain or Probe, depending on what is selected.
🔍	**Find Probe Range by IP.** If a Probe has many defined ranges, you can locate a specific range: select the Probe and click **Find Probe Range by IP**. In the Find Probe Range dialog box, enter the IP address and click the **Find** button. DFM highlights the range in the Ranges pane.

UI Element (A–Z)	Description
	Reload Domain Information. Updates all domain and Probe information from the server.
	Suspend Probe. Suspends the Probe from the BSM Server such that no jobs can run. The button changes to a **Play** button. To resume the ability to run jobs on the Probe, click the **Play** button. **Note:** This option suspends only the ability to run jobs. All other processes continues to run as usual.
	Deploy Probe Upgrade. Opens the Deploy Probe Upgrade dialog box, enabling you to automatically upgrade the version of all the Data Flow Probes connecting to the UCMDB Server with the latest cumulative patch (CUP). In the Deploy Probe Upgrade dialog box, navigate to the Probe CUP .zip file. **Note:** ➤ During the upgrade process, all compatible Probes are automatically restarted. If an integration is running on a Probe while it is restarting, the integration stops running, and starts over when the 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, upgrading the CUP. ➤ Probes that are not compatible with the UCMDB Server are not updated using this feature and must be updated manually. For details, see the *HP Universal CMDB Deployment Guide* PDF.

🔖 Edit Related Probes Dialog Box
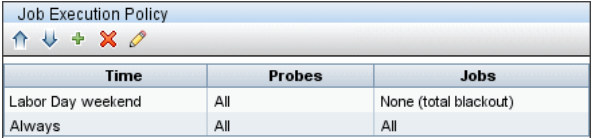
Enables you to select specific Probes.

To access	Click the **Related Probes** button 🖉 in the Edit Policy dialog box.
See also	"Job Execution Policies" on page 94

🔖 Edit Timetable Dialog Box

Enables you to set the times when a Probe must run a job execution policy.

To access	Click the **Edit** 🖉 button in the Edit Policy dialog box.
See also	"Add/Edit Policy Dialog Box" on page 152

User interface elements are described below:

UI Element (A–Z)	Description
Description	Add a description of the specific policy. This field is mandatory. **Tip**: The text you enter here appears in the Time box in the Job Execution Policy pane, so it is recommended that the description be informative:
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. **Note:** To clear a time unit, click the cell a second time.

🔧 Protocol Parameter Dialog Box

Displays the attributes that can be defined for a protocol.

To access	Admin > **RTSM Administration** > **Data Flow Management** > **Data Flow Probe Setup** > **Domains and Probes** > **Domain** > **Credentials**, select a protocol and click the **Add** or **Edit** button.
Important Information	For the description of each protocol, see "Supported Protocols" on page 108.

🔧 Scope Definition Dialog Box

Enables you to set the range that a protocol must discover.

To access	Click the **Edit** button in the Protocol Parameters dialog box.

User interface elements are described below:

UI Element (A–Z)	Description
Selected Probes	To select specific Probes whose IP range must be changed, click **Edit**. For details, see "Choose Probe Dialog Box" on page 358.
Selected Ranges	➤ **All.** The protocol runs discovery on all ranges for the domain. ➤ **Selected Range.** For the procedure to select a specific range on which the protocol runs discovery or to define an excluded range, see "Add/Edit IP Range Dialog Box" on page 149.

Selecting Probes

The Choose Probe, Edit Probe Limitations for Query Output, and Edit Related Probes dialog boxes include the following elements:

UI Element (A–Z)	Description
>	**Add Selected Probe.** Adds a Probe to the Selected Probes column.
<	**Remove Selected Probe.** Removes a Probe from the Selected Probes column.
All Data Flow Probes	➤ Select to add all Probes in the Non-selected Probes list. ➤ Clear to add a specific Probe from the Non-selected Probes list.
Non-selected Probes	Probes that are not included in the policy/filter/limitations.
Selected Probes	Probes that are included in the policy/filter/limitations.

Troubleshooting and Limitations

Troubleshooting

➤ **Problem**. You cannot transfer a Data Flow Probe from one domain to another. Once you have defined the domain of a Probe, you can change its ranges, but not the domain.

Solution. Install the Probe again:

a (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 160.

b Remove the existing Probe from RTSM. For details, see the **Remove Domain or Probe** button in "Domains and Probes Pane" on page 162.

c Install the Probe. For details, see "Data Flow Probe Installation on the Windows Platform" on page 51.

During installation, make sure you give a different name to the Probe from the one used by the old Probe. For details, see step in or step in in the *RTSM Data Flow Management Guide*.

➤ **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.

➤ **Problem. The connection between the BSM 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. The Discovery tab is not displayed in the main page of BSM.**

Solution. Install a license for the Probe. For details, see "Licensing Models for Run-time Service Model".

➤ **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 RTSM 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.

Limitations

Limitation. If you reconfigure a DFM probe to work with a different UCMDB server, you must first run the clearProbeData.bat file before you restart the probe.

6

Adapter Management

This chapter includes:

Concepts

Tasks

Reference

Concepts

🔩 Automatically Deleted CIs and Relationships and Candidates for Deletion CIs

During discovery, the Data Flow Probe compares CIs found during the previous, successful invocation with those found during the current invocation. A missing component, such as a disk or software, is assumed to have been removed from the system, and its CI is deleted from the Probe's database.

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 on aging, see "The Aging Mechanism Overview" in the *RTSM Administration Guide*.

You can define that CI instances are to be deleted for specific jobs. For details, see "How to Configure the Data Flow Probe to Automatically Delete CIs" on page 176.

By default, the Data Flow Probe deletes CI instances of certain CITs, for example, the current configuration for the Host Resources and Applications jobs (snmp: file system, installed software, osuser, service).

Candidates for Deletion

You can mark a CI instance as a candidate for deletion. This enables you to isolate CIs instead of them being automatically deleted when they are not discovered.

Discovery forces its aging status to change to **aged**, so that the CI appears in the Aged CIs box. Its time-to-deletion by the aging mechanism is shortened (to 20 days, by default).

Note:

➤ 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 "Results Management Pane" on page 203.

➤ Carefully choose the CIs that are to be candidates for deletion. For example, process CITs are not good candidates because they are often shutting down and starting up again and as a result may be deleted at every invocation.

➤ You can use this procedure to delete relationships, too. For example, the contained 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.

Example of Automatic Deletion

During the previous invocation, the Data Flow Probe ran the **Host Resources and Applications by WMI** job and discovered a host with disks a, b, c, and d. During the current invocation, the Probe discovers disks a, b, and c, compares this result with the previous result, and deletes the CI for disk d.

More Information

➤ You can view deleted CIs in the Probe log and in the Deleted column in the Statistics Results pane. For details, see "Data Flow Probe Log Files" on page 132 and "Statistics Results Pane" on page 378.

➤ For details on setting automatic deletion, see "Automatic Deletion" on page 203 in the Results Management pane.

➤ For details on aging, see "The Aging Mechanism Overview" in the *RTSM Administration Guide*.

🧩 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" on page 172

➤ "Running Software Default View" on page 172

Discovery Process

The discovery process runs as follows:

➤ The Host Resources and Applications jobs are activated.

➤ DFM searches for processes on the machines in your environment.

➤ DFM 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 RTSM.

Running Software Default View

A default view displays the mapping of relationships between applications: **Admin** > **RTSM Administration** > **Modeling** > **Modeling Studio** > **Resources** pane > **Root** > **Application** > **Deployed Software**.

You can configure DFM to discover running software. For details, see "How to Discover Running Software – Scenario" on page 177.

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 links.

➤ 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 link to the same process (**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 232.

portNumberToPortName.xml File

The portNumberToPortName.xml file is used by DFM as a dictionary to create Port CIs by mapping port numbers to meaningful port names. When a port is discovered, the Probe extracts the port number, searches in the portNumberToPortName.xml file for the port name that corresponds to this port number, and creates the Port CI with that name. If the port name does not appear in this file, the Probe uses the port number as the port name.

For details on adding new ports to be discovered, see "How to Define a New Port" on page 180.

Note: The results of running a **Network Connections – Active Discovery** job appear in the Topology Map with the port names instead of the port numbers (the port title is the value of the Port Name attribute, defined in the CIT). For details, see "Add/Edit Attribute Dialog Box" in the *RTSM Modeling Guide*.

Tasks

⚜ 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. For details on how the Data Flow Probe deletes CIs, see "Automatically Deleted CIs and Relationships and Candidates for Deletion CIs" on page 170.

1 Select the CIs to be Deleted

   a Access the **Results Management** pane in the **Adapter Configuration** tab.

   b Select the **Enable Automatic Deletion** check box.

   c Click the **Add** button to open the Choose Discovered Class dialog box. For details, see "Choose Discovered Class Dialog Box" on page 210.

   d Select the deletion method for the CIT: **Auto Delete** or **Candidate for Deletion**.

   e Click the **Save** button at the bottom of the page.

2 View Results

To view the deleted CIs, access the Deleted column in the Statistics Results pane. For details, see "Statistics Results Pane" on page 378.

⚒ 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. DFM 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 page 177

➤ "Create a Command Line Rule" on page 178

➤ "Define the Value of an Attribute" on page 179

➤ "Activate the Job" on page 180

1 Prerequisites

Display the Attribute Assignment Rules dialog box:

a Select **Admin** > **RTSM Administration** > **Data Flow Management** > **Discovery Control Panel**. In the **Discovery Modules** pane, select the **Network Discovery** module > **Host Resources and Applications** > **Software Element CF by Shell**. In the **Properties** tab, select **Global Configuration Files** > **applicationSignature.xml**. For details, see "Global Configuration Files Pane" on page 197.

Tip: If the Global Configuration Files pane does not display, click the arrow below the Trigger Queries pane.

---

b Click the **Edit** button to open the Software Library dialog box. For details, see "Software Library Dialog Box" on page 233.

c Choose the signature to be edited. Click the **Edit** button to open the Software Identification Rule Editor dialog box. For details, see "Software Identification Rule Editor Dialog Box" on page 231.

d Click the **Set Attributes** button to open the Attributes Assignment Editor dialog box. For details, see "Attribute Assignment Editor Dialog Box" on page 208.

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, DFM uses the information in the command lines discovered by the regular expression to populate a CI's name attribute with the database name.

a To create a Command Line rule that includes a regular expression, in the Attributes Assignment Rules dialog box, click the **Add** button in the Parsing Rules pane. For details, see "Parse Rule Editor Dialog Box" on page 222.

b In the Parse Rules Editor dialog box, build the rule:

➤ Enter a unique name in the Rule ID field: **r1**.

➤ Choose **Command Line** in the Process Attribute field.

➤ Enter the following regular expression in the Regular Expression field: **.+\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 fulfils 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 DFM to discover the
Oracle databases, and the value it should take.

a In the Attributes Assignment Rules dialog box, click the **Add** button in
the Attribute Assignments pane, to select the attribute.

b In the Attribute Editor dialog box:

➤ 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)}**.
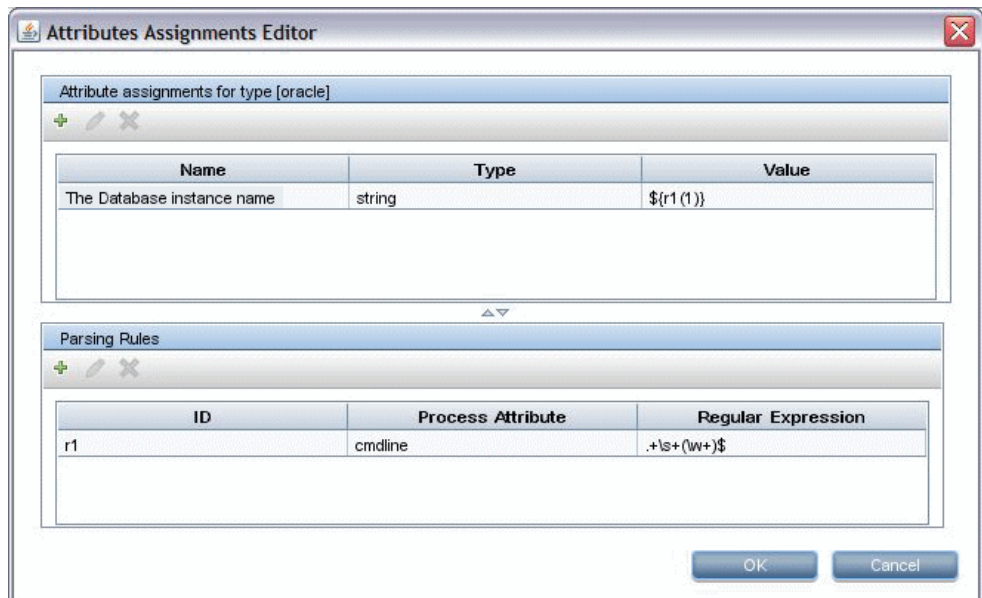
This dialog box is configured as follows: DFM enters the value of the
first group (**(\w+)$**) in the command line regular expression
(**${r1(1)}**) in the name attribute of the Oracle database CI.

During discovery, DFM 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.

179

4 **Activate the Job**

For details, see "How to Manually Activate Jobs" on page 337 and "Discovery Modules Pane" on page 383.

How to Define a New Port

To define a new port by editing the portNumberToPortName.xml file:

1 In the Adapter Management window (**Admin** > **RTSM Administration** > **Data Flow Management** > **Adapter Management**), search for the portNumberToPortName.xml file: click the **Find resource** button and enter **portNumberToPortName.xml** in the **Name** box. Click **Find Next**, then click **Close**.

The file is selected in the Resources pane and the file contents are displayed in the View pane.

For an explanation of the **portNumberToPortName.xml** file, see "portNumberToPortName.xml File" on page 174.

2 Add another row to the file and make changes to the parameters:

```
<portInfo portProtocol="xxx" portNumber="xxx" portName="xxx" discover="0"
cpVersion="xx"/>
```

➤ **portProtocol.** The network protocol used for discovery (udp or tcp).

➤ **portNumber.** The port number to be discovered.

➤ **portName.** The name that is to be displayed for this port.

➤ **discover. 1**. This port must be discovered. **0**: This port should not be discovered.

➤ **cpVersion**. Use this parameter when you want to export the **portNumberToPortName.xml** file to another RTSM system with the Package Manager. If the **portNumberToPortName.xml** file on the other system includes ports for this application but does not include the new port you want to add, the **cpVersion** attribute ensures that the new port information is copied to the file on the other system.

The **cpVersion** value must be greater than the value that appears in the root of the **portNumberToPortName.xml** file.

For example, if the root **cpVersion** value is **3**:

```
<portList
parserClassName="com.hp.ucmdb.discovery.library.communication.downloader.
cfgfiles.KnownPortsConfigFile" cpVersion="3">
```

the new port entry must include a **cpVersion** value of **4**:

```
<portInfo portProtocol="udp" portNumber="1" portName="A1" discover="0"
cpVersion="4"/>
```

Note: If the root **cpVersion** value is missing, you can add any non-negative number to the new port entry.

This parameter is also needed during Content Pack upgrade. For details, see "How to Use the cpVersion Attribute to Verify Content Update" on page 181.

How to Use the cpVersion Attribute to Verify Content Update

The cpVersion attribute is included in the portNumberToPortName.xml file, and indicates in which Content Pack release a port has been discovered. For example, the following code defines that the LDAP port 389 has been discovered in Content Pack 5.00:

```
<portInfo portProtocol="tcp" portNumber="389" portName="ldap" discover="1"
cpVersion="5"/>
```

During a Content Pack upgrade, DFM uses this attribute to perform a smart merge between the existing portNumberToPortName.xml file (which may include user-defined ports) and the new file. Entries previously added by the user are not removed and entries previously deleted by the user are not added.

For an explanation of the portNumberToPortName.xml file, see "portNumberToPortName.xml File" on page 174.

To verify that a DFM Content Pack is successfully deployed:

1 Install the latest Service Pack release.

2 Start the BSM Server.

3 Verify that all services are running. For details, see "How to View the Status of Processes and Services" in *Platform Administration*.

4 Install and deploy the latest Content Pack release. For details, refer to the Content Pack installation guide.

5 Access the portNumberToPortName.xml file (**Admin** > **RTSM Administration** > **Data Flow Management** > **Adapter Management** > **Packages** > **Network** > **Configuration Files** > **portNumberToPortName.xml**).

6 Verify that any user-defined ports have not been deleted and any ports deleted by the user have not been added.

🔨 How to Manage Adapter Configurations

You should edit adapter and XML files in one of the following ways:

Use the Adapter Management module

This method is recommended.

1 Navigate to **Admin** > **RTSM Administration** > **Data Flow Management** > **Adapter Management**.

2 In the Resources pane, select the adapter file: **Packages** > **<package name>** > **Adapters**.

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 191 and "Adapter Configuration Tab" on page 199.

> ➤ To define specific settings for the selected adapter, right-click the
> adapter and select **Edit Adapter Source** from the shortcut menu.

Use Package Manager

Edit the package and redeploy it. For details, see "Package Manager" in the
RTSM Administration Guide.

Use the JMX Console

1 Launch the Web browser and enter the server address, as follows:
http://BSM Server Host Name or IP>:21212/jmx-console.

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

2 Under UCMDB, click **UCMDB:service=Packaging Services** to open the
JMX MBEAN View page.

3 Locate the **listSubsystems** operation.

4 Enter the Customer ID value and click **Invoke**.

5 Click the **discoveryPatterns** or **discoveryConfigFiles** link.

6 Click the resource to edit.

Change the Full Population value

Because the RTSM 9.0x adapter only synchronizes changes, **over time** CIs
are not touched and are aged out; therefore, by default the RTSM 9.0x
adapter runs a full population job every seven days.

To change the full population value:

1 Access the Resources pane: **Data Flow Management** > **Adapter
Management** > **Resources**.

2 Select the **CmdbAdapter** adapter file: **CmdbAdapter** > **Adapters** >
CmdbAdapter.

 3 Right-click the **CmdbAdapter** file and choose **Edit Adapter Source**.

 4 In the source file, locate the following tag:
 <full-population-days-interval>7</full-population-days-interval>.

 5 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 Attach Discovery Documentation to a Discovery Package

This task describes how to attach updated or new documentation to a discovery package.

This task includes the following steps:

➤ "Prerequisites" on page 184

➤ "Deploy the document on the UCMDB server" on page 185

➤ "Attach the document to the relevant discovery package" on page 185

1 Prerequisites

 a Create the help document in PDF format.

 b Copy the PDF into a folder called **docs**.

 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 *RTSM Administration Guide*.

3 Attach the document to the relevant discovery package

a Navigate to **Admin** > **RTSM Administration** > **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 Filter Probe Results

You can filter Probe results for all adapters, so that only results of interest to you are sent to the HP Universal CMDB Server. (You can also filter specific adapters. For details, see "Adapter Configuration Tab" on page 199.)

Note:

➤ You can use regular expressions in filters.

➤ Attributes in the filter should be of type string only. For details on attribute types, see "Attributes Page" in the *RTSM Modeling Guide*.

➤ 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.

➤ DFM filters first according to the <includeFilter> and then applies the <excludeFilter> on the results of <includeFilter>.

Configure a Filter

Locate the **globalFiltering.xml** file: in **Adapter Management**, open the **DDM Infra** folder and click the **Configuration Files** folder. Select **globalFiltering.xml** to display the code 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="ipAddress">
        <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 **not DefaultProbe**.

The following example shows a 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>
```

Reference

🔍 Resource Files

The following file can be changed to enable DFM in non-default systems. The location of this file is: **Admin** > **RTSM Administration** > **Data Flow Management** > **Adapter Management** > **Packages** > **Network** > **Configuration Files**.

oidToHostClass.xml

The oidToHostClass.xml file contains a list of OID numbers, for all CIs in the system that have an ID. This list is required for mapping CIs to their correct CIT, and for converting the discovered OID number of an operating system or a device into string data.

To access the oidToHostClass.xml file, in Adapter Management, search for the file by clicking the **Find resource** button and entering **oidto** in the **Name** box. Click **Find Next**, then click **Close**.

The file is selected in the Resources pane and the file contents are displayed in the View pane.

Note: If an OID is discovered and its details do not appear in the oidToHostClass.xml file, its CIT is registered in the CMDB as host.

The oidToHostClass.xml file includes the following parameters:

➤ **class.** The converted CIT name of the discovered OID. Under this name, the operating system or device appears in the CMDB and in Run-time Service Model.

➤ **vendor.** The vendor of the operating system or device.

➤ **os.** A specific operating system, for example, Linux. This parameter is optional.

➤ **model.** A specific model, for example, JETDIRECT,JD30. This parameter is optional.

➤ **oid.** The discovered OID.

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.

➤ **discoveryPolicy.xml.** Includes the schedule when the Probe does not execute tasks. For details, see "Add/Edit Policy Dialog Box" on page 152. Located in **Admin** > **RTSM Administration** > **Data Flow Management** > **Adapter Management** > **Packages** > **AutoDiscoveryInfra** > **Configuration Files**.

➤ **jythonGlobalLibs.xml.** A list of default Jython global libraries that DFM loads before running scripts. Located in **Admin** > **RTSM Administration** > **Data Flow Management** > **Adapter Management** > **Packages** > **AutoDiscoveryContent** > **Configuration Files**.

Adapter Management User Interface

This section describes:

➤ Find Resource/Jobs Dialog Box on page 215

➤ Find Text Dialog Box on page 216

➤ Input Query Editor Window on page 217

➤ Parse Rule Editor Dialog Box on page 222

➤ Permission Editor Dialog Box on page 223

➤ Resources Pane on page 225

➤ Script Editor Window on page 229

➤ Script Pane on page 229

➤ Software Identification Rule Editor Dialog Box on page 231

➤ Software Library Dialog Box on page 233

🔍 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 a specific adapter in the Resources pane.
Relevant tasks	"How to Implement a Discovery Adapter" in the *RTSM Developer Reference Guide*

User interface elements are described below:

UI Element (A–Z)	Description
Adapter Category	Used to arrange adapters by category.
Content Help	The Help document associated with the adapter, in PDF format. To select a different Help document for the adapter do one of the following: ➤ Click ✏ and select the relevant PDF file. ➤ Right-click the adapter's name in the tree and click **Edit adapter source**. Find the following line in the code: <RelatedDocument>*name_of_pdf*.pdf</RelatedDocument> and change the name of the PDF. To detach the selected Help document, click ✖.
Description	A detailed description of the adapter's purpose, including relevant comments.
Display Name	A display name to identify the adapter.
Type	For **Discovery** adapters: **jython**; for **Integration** adapters: can be of various types.
Used as Integration Adapter	Select to define that this adapter is an integration adapter. **Note**: These adapters cannot be used for defining Discovery jobs, and are accessible only through the Integration Studio.

Input Pane

User interface elements are described below:

UI Element (A–Z)	Description
Input CI Type ...	The input CIT is used as the adapter input. For details, see "Define Adapter Input (Trigger CIT and Input Query)" in the *RTSM Developer Reference Guide*. Click the button to choose a CIT to use as the input.

UI Element (A–Z)	Description
	Edit the Input query.
	Remove the Input query.
Input Query	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.)
	Note: Since this field is optional, not all adapters include an Input query. **None** signifies this adapter does not have an Input query definition.
	➤ 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.
	For details, see "Input Query Editor Window" on page 217.
	For an explanation, see "Trigger CIs and Trigger Queries" on page 33.
	For an example, see "Example of Input Query Definition" in the *RTSM Developer Reference Guide*.

UI Element (A–Z)	Description
Triggered CI Data	⊕ 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.
	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:
	${VARIABLE_NAME.attributeName}
	where **VARIABLE_NAME** can be one of three predefined variables:
	➤ **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, ${SOURCE.network_netaddr} indicates that the trigger CI is a network.

194

Used Scripts Pane

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

UI Element (A–Z)	Description
⬆ ⬇	Change the order of the scripts. DFM runs the scripts in the order in which they appear here.
➕	Add a script to the adapter.
✖	Remove a script from the adapter.
✏	Edit the selected script in the Script Editor that opens.
<Scripts>	A list of Jython scripts used by the adapter.

Required Permissions Pane

Enables you to view the permissions that you have configured for an adapter.

To access	**Admin** > **RTSM Administration** > **Data Flow Management** > **Adapter Management** > select an adapter > **Adapter Definition** tab > **Required Permissions** pane.
Important information	➤ Workflow: ➤ Configure the permissions in the Permission Editor dialog box. ➤ View the permissions in this pane. ➤ When working with jobs in the Discovery Control Panel window, view these permissions for a specific job. ➤ For details on the fields in this pane, see "Permission Editor Dialog Box" on page 223.
See also	➤ "Permission Editor Dialog Box" on page 223 ➤ "Discovery Permissions Window" on page 386 ➤ "Viewing Permissions While Running Jobs" on page 327

User interface elements are described below:

UI Element (A–Z)	Description
![add icon]	Adds a permission object. The Permission Editor dialog box opens. For details, see "Permission Editor Dialog Box" on page 223.
![edit icon]	Edits a selected permission object. For details, see "Permission Editor Dialog Box" on page 223.
![delete icon]	Deletes a selected permission object.
![up down icons]	Changes the order of permissions on a selected permission object. The order given here is the order in which the credentials are verified.
![export icon]	Exports a permission object in Excel, PDF, RTF, CSV, or XML format. For details, see "Browse Views Mode" in the *RTSM Modeling Guide*.

Required Discovery Protocols Pane

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

UI Element (A–Z)	Description
![add icon]	Opens the Add Required Protocol dialog box.
![delete icon]	Removes an existing protocol.
\<Protocols>	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.

Discovered CITs Pane

User interface elements are described below:

UI Element (A–Z)	Description
	Opens the Choose Discovered Class dialog box, to select a CIT that is to be discovered by the adapter. For details, see "Choose Discovered Class Dialog Box" on page 210.
	Removes the CIT from the list of CITs that the adapter discovers.
	Displays a map of the CITs and links that are discovered by the adapter, instead of a list. Click the button to open the Discovered CITs Map window. The CIs and relationship links discovered by the adapter are shown.
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.

To access	➤ In Adapter Management, select an adapter and the **Adapter Definition** tab. ➤ In Discovery Control Panel, select a job and the **Properties** tab.
Important information	The configuration file applicationsSignature.xml opens the Software Library dialog box. For details, see "Software Library Dialog Box" on page 233. The applicationsSignature.xml file contains a list of all applications that DFM attempts to find in the environment.
Relevant tasks	"How to Discover Running Software – Scenario" on page 177

User interface elements are described below:

UI Element (A–Z)	Description
	Opens the Global Configuration Files dialog box, to select configuration files that are needed by the adapter.
	Deletes a selected configuration file.
	Opens the appropriate editor for a selected configuration file. For example, the file msServerTypes.xml opens the Script Editor.

Adapter Parameters Pane

User interface elements are described below:

UI Element (A–Z)	Description
	Opens the Parameter Editor. Enter details on the parameter. The value you enter here is assigned to the attribute.
	Removes a parameter.
	Select a parameter and click the button to open the Parameter Editor and make changes.
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	"The DiscoveryProbe.properties File" on page 137

Probe Selection Pane

Enables you to specify which Probe to use with an adapter.

Important information	By default, DFM automatically chooses the Probe for the Trigger CI according to the CI's related node. After obtaining the CI's related node, DFM chooses one of the node's IPs and chooses the Probe according to the Probe's network scope definitions.
	This may fail in the following situations:
	➤ A Trigger CI does not have a related node (such as the **network** CIT).
	➤ A triggered CI's node has multiple IPs, each belonging to a different Probe.
	To resolve these issues, you can specify which Probe to use with the adapter by:
	➤ In the Probe Selection section, selecting **Override default probe selection**.
	➤ In the Probe box, typing the Probe to use for the task.

User interface elements are described below:

UI Element (A–Z)	Description
Override default probe selection	You can use calculated values such as: **${Network.network_domain}** This value uses a syntax similar to that used by Triggered CI data in the **Adapter Definition** tab > **Input** pane. For details, see "Input Pane" on page 192.

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.
	➤ **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.
	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.
	When requested (in the Discovery Status pane), DFM displays the log retrieved from the Probe (if a log has been created). For details, see "Discovery Status Pane" on page 372.
	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**.
	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 "How to Record DFM Code" in the *RTSM Developer Reference Guide*.
Include results in communication log	Select to enable capturing the discovered results with the created communication log; these discovered results may help in investigating various discovery problems.
Max. execution time	The maximum time allowed for an adapter to run on one Trigger CI.

UI Element (A–Z)	Description
Max. threads	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).
	The default value is defined in the **DiscoveryProbe.properties** file, in the **appilog.agent.local.services.defaultMaxJobThreads** parameter.
	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 *HP Universal CMDB Discovery and Integration Content Guide* PDF.

Results Management Pane

User interface elements are described below:

UI Element (A–Z)	Description

Automatic Deletion	Enables marking specific CITs for deletion or as candidates for deletion, if the Data Flow Probe does not find them during its next invocation.
	
	To add CITs to the list of CIs, click the **Add** button. In the Choose Discovered Class dialog box, choose the CITs that should be automatically deleted.
	
	The changes you make here are added to the adapter file, for example:
	
	`<resultMechanism isEnabled="true">`
	`    <autoDeleteCITs isEnabled="true">`
	`        <CIT>shell</CIT>`
	`            <candidateForDeletionCIT>node</`
	`candidateForDeletionCIT>`
	`    </autoDeleteCITs>`
	`</resultMechanism>`
	
	For details on how the Data Flow Probe handles CI deletion, see "Automatically Deleted CIs and Relationships and Candidates for Deletion CIs" on page 170.

Enable aging	Select this check box to run the aging mechanism that specifies how long a period must pass in which CIs are discovered, before DFM treats these CIs as no longer relevant and removes them. For details on aging, see "The Aging Mechanism Overview" in the *RTSM Administration Guide*.

UI Element (A–Z)	Description
Enable Automatic Deletion	Choose between:
	➤ **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).
	When this check box is selected, the **Automatic Deletion** pane is enabled. For details, see "Automatic Deletion" on page 203.
	For details on how the Data Flow Probe handles CI deletion, see "Automatically Deleted CIs and Relationships and Candidates for Deletion CIs" on page 170.

UI Element (A–Z)	Description
Enable collecting 'Discovered by' data	➤ **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.
	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 Status of Application Discovery (Rediscover a View)" and "Show Discovery Status and Changes Dialog Box" in the *RTSM Modeling Guide*.
Fail entire bulks due to invalid CIs	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.
	Clear the check box to have the results sent to the RTSM with only the invalid CIs (and their topology) dropped from the results. In the above example, 999 objects would be processed. BSM displays an error message when you view the results.

Result Grouping Pane

User interface elements are described below:

UI Element (A–Z)	Description
Grouping Interval (Seconds)	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. The default value is 30 seconds. **Note**: If you enter a value in both boxes, DFM applies the value of whichever occurs first.
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 DFM process.

To access	**Admin** > **RTSM Administration** > **Data Flow Management** > **Adapter Management** or right-click a job in the Discovery Control Panel window and click **Go to Adapter**.

Important information	**Note:** 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).
	Caution: Only administrators with an expert knowledge of the DFM process should delete packages.
See also	➤ "Adapter Definition Tab" on page 191
	➤ "Global Configuration Files Pane" on page 197
	➤ "Adapter Configuration Tab" on page 199
	➤ "Script Pane" on page 229
	➤ "Resources Pane" on page 225
	➤ the *HP Universal CMDB Discovery and Integration Content Guide* PDF
	➤ "Configuration File Pane" on page 212
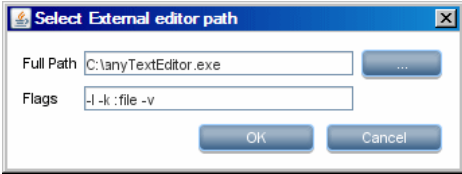
Adapter Source Editor Window

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 225

User interface elements are described below:

UI Element (A–Z)	Description
	Find specific text in the adapter script. For details, see "Find Text Dialog Box" on page 216.
	Goes to a specific line in the adapter script. In the Go To Line dialog box, enter the line number.
	Opens the adapter script in an external text editor.

UI Element (A–Z)	Description
	Edits the external editor preferences. You can run the editor by adding flags to the path. In the following example: **:file** sets the place of the file in relation to the flags. The user cannot set the file name.
	Toggles between the advanced editor and a simple text editor. You can use the simple editor when the advanced editor causes problems.
	Signifies that the code is valid.
	Signifies that the code is invalid.

Attribute 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	Click **Set Attributes** in the Software Identification Rule Editor dialog box.
Relevant tasks	"How to Discover Running Software – Scenario" on page 177
See also	➤ "Parse Rule Editor Dialog Box" on page 222 ➤ "Attribute Editor Dialog Box" on page 209 ➤ "Software Identification Rule Editor Dialog Box" on page 231

User interface elements are described below:

UI Element (A–Z)	Description
✚	Adds a regular expression that determines the attribute of the CI to be discovered, or an attribute.
✏	Edits an existing regular expression or attribute.
✖	Deletes the regular expression or the attribute.
Attribute assignments for type	For details, see "Attribute Editor Dialog Box" on page 209.
Parsing Rules	For details, see "Parse Rule Editor Dialog Box" on page 222.

🔍 Attribute Editor Dialog Box

Enables you to define a rule that discovers a CIT according to an attribute. The attribute is defined according to a regular expression.

To access	**Software Identification Rule Editor** > **Set Attributes button** > **Attributes Assignment Editor**. Click the **Add** button in the **Attributes Assignment for Type** pane.
Relevant tasks	"How to Discover Running Software – Scenario" on page 177
See also	"Parse Rule Editor Dialog Box" on page 222

User interface elements are described below:

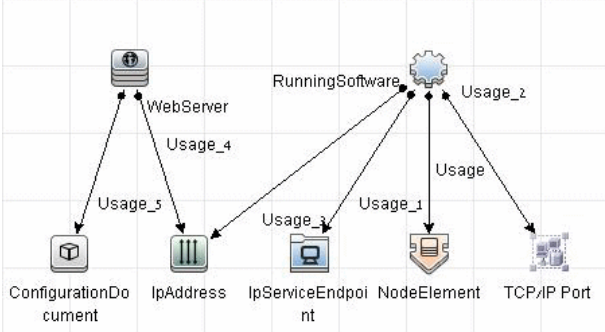| UI Element (A–Z)	Description
Name	Choose from the list of attributes of the CIT selected in the Editor. This attribute name is replaced by the value found by the regular expression. To find an attribute, start typing the name.

UI Element (A–Z)	Description
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.
	Use the following syntax for the value:
	${<rule ID name>(<group number>)}
	For example, **${DB_SID(1)}** means that DFM should search for the Rule ID with the name **DB_SID** and retrieve its regular expression.
	DFM should then retrieve the code for the first group (**1**). For example, in the regular expression **.+\s+(\w+)$**, the first group is **(\w+)$** — a word or words that appear at the end of the line.

🔧 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	➤ **Admin** > **RTSM Administration** > **Data Flow Management** > **Adapter Management**. In the Resources pane, select an adapter. In the **Adapter Definition** tab > **Discovered CITs** pane, click the **Add Discovered CIT** button.
	➤ **Admin** > **RTSM Administration** > **Data Flow Management** > **Adapter Management**. In the Resources pane, select an adapter. 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:
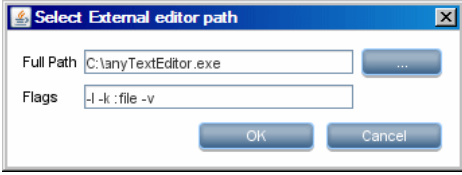
UI Element (A–Z)	Description
Link	Enables DFM to discover CITs only when they are linked by link types you choose in this box.
	Note: This section is relevant only when adding a discovered CIT, not for defining CITs for automatic deletion.
	Select a link type from the list and click the button [...] 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.
	Note: 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. For example, both nodes and IPs and nodes and ports are linked by **usage**. You may need to receive results only for nodes and IPs that are connected by the **usage** link, and not 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:
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	The following files are for internal use only and should only be changed by users with an advanced knowledge of adapter-writing: ➤ discoveryPolicy.xml ➤ jythonGlobalLibs.xml For details, see "Resource Files" on page 189 and "Internal Configuration Files" on page 190.

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 216.
📝	Goes to a specific line in the configuration file. In the Go To Line dialog box, enter the line number.
📝	Opens the file in an external editor.
📋	Edits the external editor preferences. You can run the editor by adding flags to the path. In the following example: Select External editor path Full Path C:\anyTextEditor.exe ... Flags -l -k :file -v OK Cancel **:file** sets the place of the file in relation to the flags. The user cannot set the file name.

UI Element (A–Z)	Description
	Toggles 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	Click the **Add** button in the **Identifying Processes** pane in the Software Identification Rule Editor dialog box.
See also	"Software Identification Rule Editor Dialog Box" on page 231

User interface elements are described below:

UI Element (A–Z)	Description
Attributes	Opens the Attributes Assignments Editor dialog box for the identifying process.
Command Line	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**.

213

UI Element (A–Z)	Description
Key Process	Select this check box if, during discovery, DFM must distinguish between applications that run similar processes (IP, port, command line, or owner). For an explanation of this box, see "Identifying Running Software by Processes" on page 173.
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.
Name	Enter the exact name of the process, for example, **java.exe**.
Port	Add a port number or name, either by typing a number or by clicking the **Add** button then selecting the ports in the Global Ports List. ➤ 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 (the running software can use any port), select the **All Ports** option.
Port match is optional	➤ Select this check box to enable discovery of processes that are not listening at any of the ports entered in the Port field (identification is by process name only). ➤ Clear this check box to enable discovery of processes based on process name and the port number entered in the Port field.

Find Resource/Jobs Dialog Box

Enables you to build a search query to find a particular resource or job.

| To access	➤ **Discovery Control Panel** > **Discovery Modules** pane. Click the **Search for Discovery Job** button.
	➤ **Adapter Management** > **Resources** pane. Click the **Find resource** button.
See also	"Resources Pane" on page 225

User interface elements are described below:

UI Element (A–Z)	Description
	Selects a CIT from the dialog box that opens. Click **OK** to return to the Find Resource dialog box.
	Note: This button is not accessible when **Name** is selected.
Direction	Searches forwards or backwards through the packages.
Find All	Highlights all instances of the text entered in **Name**.
Find Discovery Job by/ Find Discovery resource by	Choose between:
	➤ **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
[Find] [Find All]	➤ 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	Type the text to be found or click the down arrow to choose from previous searches. 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.
Options	Select an option to narrow your search.
Origin	Enables a search of the entire scope or from the current cursor position.
Target	➤ **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	**Admin** > **RTSM Administration** > **Data Flow Management** > **Adapter Management** > select an adapter > **Adapter Definition** tab > **Input** pane > click the **Edit Input Query** button next to the **Input Query** box.
See also	➤ "Trigger CIs and Trigger Queries" on page 33 ➤ "Trigger Query Editor Window" on page 422

User interface elements are described below:

UI Element (A–Z)	Description
<Panes>	➤ CI Type Selector Pane ➤ Editing Pane ➤ Information Pane
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 *RTSM Modeling
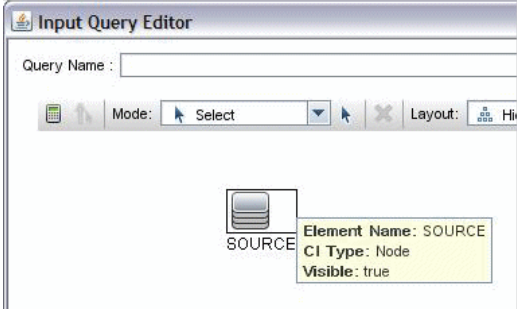Guide*.

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.
	Note: Each time you select the same object from the tree, you must rename the object node to have a unique name.
Relevant tasks	➤ "How to Define a TQL Query" in the *RTSM Modeling Guide*
	➤ "How to Create a Pattern View" in the *RTSM Modeling Guide*
See also	"How to Add Query Nodes and Relationships to a TQL Query" in the *RTSM Modeling Guide*

Editing Pane

User interface elements are described below:

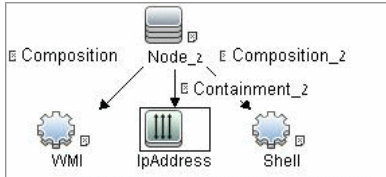| UI Element (A–Z)	Description
<node>	Hold the cursor over a node to view information about the node:
<right-click menu>	For details, see "Shortcut Menu Options" in the *RTSM Modeling Guide* .
<Toolbar>	For details, see "Toolbar Options" in the *RTSM Modeling Guide* .

Information Pane

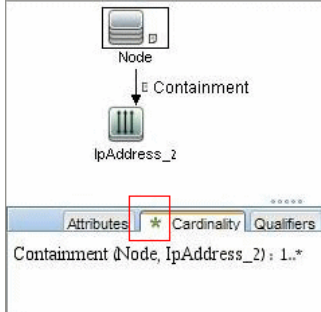Displays the properties, conditions, and cardinality for the selected node and relationship.

Important information	Hold the pointer over a node to view information: A small green indicator is displayed next to the tabs that include information:

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 *RTSM Modeling Guide*.
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 *RTSM Modeling Guide*.
Details	➤ **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: ➤ **Include subtypes.** Display both the selected CI and its descendants in the topology map. **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.
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 *RTSM Modeling Guide*.

UI Element (A-Z)	Description
Qualifiers	Displays the qualifier conditions defined for the node or the relationship. For details, see "Qualifier Tab" in the *RTSM Modeling Guide*.
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 *RTSM Modeling Guide*.

Parse Rule Editor Dialog Box

Enables you to create a rule that matches an attribute to process-related information (IP, port, command line, and owner).

To access	**Software Identification Rule Editor** > **Set Attributes** > **Attributes Assignment Editor** > **Parsing Rules** > **Add**
Important information	Only users with a knowledge of regular expressions should make changes to a rule.
Relevant tasks	"How to Discover Running Software – Scenario" on page 177
See also	➤ "Attribute Editor Dialog Box" on page 209 ➤ "Software Identification Rule Editor Dialog Box" on page 231

User interface elements are described below:

UI Element (A–Z)	Description
Process Attribute	Choose between the **Port**, **IP**, **Command Line**, **Name**, or **Owner** process-related information. The rule is invoked on the attribute you choose here.

UI Element (A–Z)	Description
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. For example, a command line process includes the following regular expression: **.+\s+(\w+)\$** 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. The following command line matches this regular expression: **c:\ora10\bin\oracle.exe UCMDB**
Rule ID	Enter a unique name for the rule. The Rule ID is needed to identify the rule in the Attributes Assignment Editor pane. For details, see "Additional Attributes" on page 232.

Permission Editor Dialog Box

Enables you to configure an adapter you have written, so that users can view permissions for the job.

To access	Admin > RTSM Administration > Data Flow Management > Adapter Management > select an adapter > Adapter Definition tab > Required Permissions pane > click the Add button.
Important information	The information you define here is not dynamic; if an adapter is changed, the information in this dialog box is not updated.
See also	➤ "Discovery Permissions Window" on page 386 ➤ "Viewing Permissions While Running Jobs" on page 327 ➤ "Required Permissions Pane" on page 195 ➤ "Discovery Job Details Pane" on page 371

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
	Opens 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.
	Deletes a permission object.
	Edits 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 cat needs the /etc/passwd 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 wizard, and you can import an external resource.

To access	Admin > RTSM Administration > Data Flow Management > Adapter Management
Important information	Depending which level you select in the Resources pane, different information is displayed in the View pane.
	If you select:
	➤ One of the following folders: Discovery 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.
	➤ A specific adapter: The **Adapter Definition** and **Adapter Management** tabs are displayed. For details, see "Adapter Definition Tab" on page 191 and "Adapter Configuration Tab" on page 199.
	➤ A script or configuration file: The script editor is displayed. For details, see "Script Pane" on page 229.
	➤ An external resource: Information about the file is displayed.
See also	"Package Manager User Interface" in the *RTSM Administration Guide*.

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

UI Element	Description
	Click to: ➤ **Create an 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**. The new adapter is added to the << No Package >> folder. Edit the adapter. For details, see "Adapter Definition Tab" on page 191 and "Adapter Configuration Tab" on page 199. For details on moving an adapter to a package, see "How to Create a Custom Package" in the *RTSM Administration Guide*. For details on creating integration adapters, see "Discovery and Integration Adapters" on page 29. ➤ **Create a Jython script.** Enter the script name. For details, see "Script Pane" on page 229. ➤ **Create a 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 "Configuration File Pane" on page 212. ➤ **Import an external resource.** In the browser that opens, locate the resource to be imported and click **Open**. ➤ **Create a Discovery Wizard.** Name the new wizard. By default, the file takes an .xml extension. A new file is added to the Discovery Wizard folder of the << No Package >> folder. The file is in template format.
	Deletes the resource.
	Opens the Find Resource dialog box. For details on filtering, see "Filtering Results" on page 98.
	Refreshes the list of packages.

UI Element	Description
	Packages tree. Displays a list of all packages.
	Package root. Displays a list of all resources included in the package. You can view any of these resources by clicking the resource in the Resources pane.
<Configuration files>	Right-click a file to: ➤ **Save as.** Saves the file under a new name. Use this option to clone an existing file. The new file includes all attributes of the existing file. Make any necessary changes to the file and save it. ➤ **Delete**. Deletes the configuration file. The resource is removed completely from the system. ➤ **Open in Frame.** Select to open the file in a new window.

<External resource files>	An external resource is any file needed to perform discovery or integration. For example, the **nmap.exe** file is needed for credential-less discovery.
	
	➤ Right-click a file to:
	    ➤ **Save as.** Save the resource under a new name. Use this option to clone an existing resource. The new resource includes all attributes of the existing resource and is saved to the same location in the file system. Make any necessary changes to the new resource and save it.
	    ➤ **Delete**. Deletes the file. The file is removed completely from the system.
	➤ Select the file to display information in the View pane.
	    You can open an external resource or export it (you should provide a name for the file you are exporting).

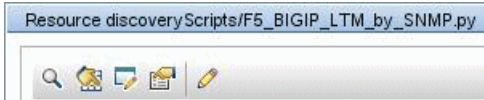| UI Element	Description
<Adapter files>	Right-click a file to: ➤ **Save as.** Save the adapter under a new name. Use this option to clone an existing adapter. The new adapter includes all attributes of the existing adapter. Give a name to the new adapter, and change the necessary attributes. ➤ **Delete**. Deletes the adapter. The adapter is removed completely from the system. ➤ **Go to Discovery job.** When enabled, opens the Discovery Control Panel window with the job selected. This option is enabled if the adapter is included in a job. ➤ **Go to Integration Point.** When enabled, opens the Integration Studio with the integration point selected. This option is enabled if the integration point for the adapter is defined. ➤ **Edit adapter source.** Opens the adapter source editor where you can make changes to the adapter. For details, see "Adapter Source Editor Window" on page 207.
<Script files>	Right-click a file to: ➤ **Save as.** Save the script under a new name. Use this option to clone an existing script. The new script includes all attributes of the existing script. Make any necessary changes to the script and save it. ➤ **Delete**. Deletes the script. The script is removed completely from the system. ➤ **Open in Frame.** Select to open the script in a new window. For details on editing the script, see "Adapter Source Editor Window" on page 207.

🔖 Script Editor Window

Enables you to edit a specific script that is part of a package.

To access	➤ Right-click a script in the Resources pane and choose **Open in Frame**.
	➤ Select a configuration file in the Global Configuration Files pane and click the **Edit** button.
	For details, see "Script Pane" on page 229.
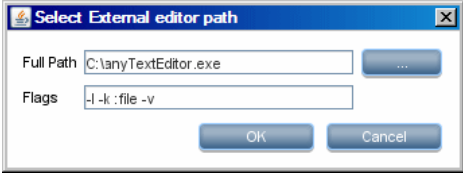
🔖 Script Pane

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	The script pane title bar includes the actual physical location of the script. For example, the following script is located in **C:\hp\UCMDB\DataFlowProbe\runtime\probeManager\discoveryScripts** (or **probeGateway\discoveryScripts**):
See also	"Adapter Development and Writing" in the *RTSM Developer Reference Guide*

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

UI Element (A–Z)	Description
🔍	Finds specific text in the script. For details, see "Find Text Dialog Box" on page 216.
🗺	Goes to a specific line in a script. In the Go To Line dialog box, enter the line number.

UI Element (A–Z)	Description
	Opens the script in an external text editor.
	Edits the external editor preferences. You can run the editor by adding flags to the path. In the following example: **:file** sets the place of the file in relation to the flags. The user cannot set the file name.
	Toggles between the advanced editor and a simple text editor. You can use the simple editor when the advanced editor causes problems.
	For Jython files, signifies that the code is valid.
	For Jython files, signifies that the code is not valid.
	See Validation Information below. **Note**: This button is displayed when a script contains Framework API errors.

UI Element (A–Z)	Description
<script>	The Jython script used by the package. For details on working with Jython, see "How to Create Jython Code" in the *RTSM Developer Reference Guide*.
Validation Information	If a script is not valid, Validation Information displays the errors in the script, for example: Script has failed validation. At line 48: Factory.getProtocolProperty(found. This is a problem - Usage of Factory is deprecated. Use Framework.getProtocolProperty instead. Click **Fix validation errors** then **OK** to update the script. The error may occur due to changes in the Framework object's API. For details, see "RTSM (HP Universal CMDB) Web Service API" in the *RTSM Developer Reference Guide*.

Software Identification Rule Editor Dialog Box

Enables you to define a new running software rule.

To access	Data Flow Management > Discovery Control Panel. In the Discovery Modules pane, select Network Discovery > Host Resources and Applications > Software Element CF by Shell. In the Properties tab, select Global Configuration Files > applicationSignature.xml. In the Software Library dialog box, click the Add button or select an existing element and click the Edit button.
Important information	Each parse rule must be matched by at least one process.
Relevant tasks	"How to Discover Running Software – Scenario" on page 177
See also	"Global Configuration Files Pane" on page 197

User interface elements are described below:

UI Element (A–Z)	Description
Set Attributes	Adds attributes to the component. For details, see "Attribute Assignment Editor Dialog Box" on page 208.
Set Configuration Files	Opens the Optional Configuration Files dialog box.
➕	Adds a process.
✖	Deletes a selected process .
✏	Edits a selected process.
Additional Attributes	To add attributes, click the Set Attributes button. For details, see "Attribute Assignment Editor Dialog Box" on page 208.
Category	You can: ➤ 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. The changes you make here are immediately displayed in the Software Library dialog box.
CI Type	Select the CIT that is to be discovered.
Discovered Product Name	The name of the running software to be created by this signature.
Identifying Processes	To add a process that can identify specific running software, click the **Add** button. The Edit Process dialog box opens. For details, see "Edit Process Dialog Box" on page 213.
Optional Configuration Files	A list of configuration files. Click the **Set Configuration Files** button to open the Optional Configuration Files dialog box. To add a configuration file, in the Optional Configuration Files dialog box, click the **Add** button and, in the **Configuration File Names** box, enter the full path to the running software's configuration file and the file name.

UI Element (A–Z)	Description
Software Signature ID	The name of the definition. **Note**: This is not the running software's name but a name you give to differentiate this discovery from similar discoveries.
Supported versions	Versions supported for this running software.
Vendor	The vendor of this running software.

🔍 Software Library Dialog Box

Enables you to view the logical groups of running software.

To access	➤ **Discovery Control Panel window** > **Network Discovery** > select one of the **Host Resources and Applications module** jobs. Locate the **Global Configuration Files** pane in the Properties tab. Select **applicationsSignature.xml** and click the **Edit** button.
	➤ **Adapter Management window** > select one of the **Host_Resources_By_SNMP/TTY/WMI** adapters. Locate the **Global Configuration File**s pane in the **Adapter Definition** tab. Select **applicationsSignature.xml** and click the **Edit** button.
	➤ In the Infrastructure Wizard Preferences page, open the **Choose Software Element to be discovered and configure Identification** box.
Important information	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 231.
	The code you define in this dialog box and the Software Element Editor dialog box overwrites the code in applicationsSignature.xml.

Relevant tasks	"How to Discover Running Software – Scenario" on page 177
See also	"Global Configuration Files Pane" on page 197

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.
	Defines a new software element. For details, see "Software Identification Rule Editor Dialog Box" on page 231.
	Deletes a selected software element.
	Edits a selected software element. For details, see "Software Identification Rule Editor Dialog Box" on page 231.
<List of software elements>	List of objects that are software elements.

7

Data Flow Probe Status

This chapter includes:

Concepts

➤ Data Flow Probe Status Overview on page 236

Tasks

➤ How to View Current Status of Discovered CIs on page 237

Reference

➤ Data Flow Probe Status User Interface on page 238

Concepts

Data Flow Probe Status Overview

You use Data Flow Probe Status to view the current status of the discovered CIs in the Probes. Data Flow Probe Status retrieves the status from the Probes and displays the results in a view.

The view is not automatically updated; to refresh the status data, click the **Get snapshot** button.

Tasks

🔧 How to View Current Status of Discovered CIs

This task describes how to view the current status of discovered CIs.

This task includes the following steps:

➤ "Prerequisites" on page 237

➤ "Access Data Flow Probe Status" on page 237

1 Prerequisites

Verify that the Probe is enabled and is connected to the BSM Gateway server. For details, see "How to Get Started with the RTSM Data Flow Probe" on page 99.

2 Access Data Flow Probe Status

a Go to **Admin** > **RTSM Administration** > **Data Flow Management** > **Data Flow Probe Status**.

b Select a connected Probe.

All current jobs in the Probe are listed, together with their status. For details, see "Data Flow Probe Status Window" on page 240.

c Click the **Get Snapshot** button.

d Select jobs from the Progress list and click the **View Job progress** button. The Job Details window opens.

Reference

🔍 Data Flow Probe Status User Interface

This section includes:

➤ [Job Name] Dialog Box on page 238

➤ Data Flow Probe Status Window on page 240

🔍 [Job Name] Dialog Box

Enables you to view details about a job, including its scheduling, as well as job statistics.

To access	➤ Select a job in the Progress pane of the Data Flow Probe Status window and click the **View job progress** 🖼️ button. or ➤ Double-click a job the Progress pane of the Data Flow Probe Status window.

User interface elements are described below:

UI Element (A–Z)	Description
Job Details	**Status.** Can be **Scheduled** (the job runs according to a defined schedule) or **Running** (the job is running now).
	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.
Schedule	**Previous invocation.** The last time that DFM ran the job.
	Next invocation. The next time that DFM is scheduled to run the job.
	Last duration. The length of time, in seconds, taken to run the job in the previous invocation.
	Average duration. The average duration, in seconds, 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).
Statistics Results	For details, see "Statistics Results Pane" on page 242.

🔍 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	**Admin** > **RTSM Administration** > **Data Flow Management** > **Data Flow Probe Status**
Important Information	Depending on what you select in the Domains Browser pane, different information is displayed in the viewing pane. If you select: ➤ a domain, you can view details and CIT statistics for the domain. For details, see "Details Pane" on page 155 and "Statistics Results Pane" on page 242. ➤ a Probe, you can view details on the Probe (such as the Probe IP), the progress of a job and you can view CIT statistics. For details, see "Details Pane" on page 241, "Progress Pane" on page 242, "Statistics Results Pane" on page 242, and "Probe Snapshot Information" on page 244.
Relevant tasks	"How to View Current Status of Discovered CIs" on page 237
See also	"Data Flow Probe Status Overview" on page 236

Details Pane

User interface elements are described below:

UI Element (A–Z)	Description
Domain Type	**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 which is defined with a range. The external domain may contain only one Probe whose name equals the domain name. However, you can define several external domains in your system.
	For details on defining domains, see "Add New Domain Dialog Box" on page 153.

Progress Pane

User interface elements are described below:

UI Element (A–Z)	Description
	Select a CI and click **View job progress** to view details of a job. For details, see "[Job Name] Dialog Box" on page 238.
Job	The name of the job. Double click a job to open a dialog box displaying job details. For details, see "[Job Name] Dialog Box" on page 238.
Next invocation	The next time that the Probe is scheduled to run.
Previous invocation	The last time that the Probe ran.
Progress	➤ If a job has not started running, the Progress column displays **Scheduled**. ➤ If a job is running, the progress of the running job is displayed.
Thread count	The number of threads currently allocated to this job.
Triggered CIs	The number of CIs triggered in the job.

Statistics Results Pane

Enables you to view details and CIT statistics.

To access	Click the Default Domain or Probe name in the Domains Browser pane.

User interface elements are described below:

UI Element (A–Z)	Description
	Retrieves the latest data from the Probe (data is not automatically updated).
	Set the time range for which to display statistics about the CITs. ➤ **All.** Displays statistics for all job runs. ➤ **Last Hour/Day/Week/Month.** Choose a period of time for which to display statistics about the CITs. ➤ **Custom Range.** Opens 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.
<Column title>	Click a column title to change the order of the CITs from ascending to descending order, or vice versa.
<right-click a title>	Choose from the following options: ➤ **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 Select 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 *RTSM Modeling Guide*.
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.

UI Element (A–Z)	Description
Filter	The time range set with the Set Filter button.
Last updated	The date and time that the statistics table has been updated for a particular Probe.
Total	The total number of CIs in each column.
Updated	The number of CIT instances that have been updated.

Probe Snapshot Information

User interface elements are described below:

UI Element (A–Z)	Description
🖼	Displays the current status of the discovered CIs and jobs on the selected Probe.
Last updated	The date and time at which the Get snapshot button was last pressed (the date and time of the data displayed in Data Flow Probe Status).
Probe IPs	The IP addresses defined for the Probe.
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 388.
Status	The status of the Probe: ➤ **Connected.** The Probe has successfully connected to the server (the Probe connects every few seconds). ➤ **Connected (suspended).** The Probe 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.

8

DDM Community

This chapter includes:

Reference

Reference

🔍 Discovery and Integration Content Packs

The DDM Community Web site provides customers with a convenient way to obtain the latest Discovery and Integration Content Pack. You need an HP Passport user name and password to log in. The URL for this Web site is: https://h20090.www2.hp.com/.

Part III

Integration

9

Integration Studio

This chapter includes:

Concepts

Tasks

Reference

Concepts

🔹 Integration Studio Overview

The Integration Studio is where you manage your RTSM integration points and connect and share information with external repositories, such as other RTSMs, BTO Software products, or third-party products.

Integration points in the RTSM 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 RTSM; however, you can create additional adapters using the Federation Framework SDK. For details, see "How to Add an Adapter for a New External Data Source" in the *RTSM Developer Reference Guide*.

You can also create adapters in the Adapter Management module. For details, see "Resources Pane" on page 225.

For details about how to set up integration points for data integrations, see "Integration Studio Page" on page 277.

Integration points can be of one of the following types:

➤ "Population" on page 251

➤ "Federation" on page 251

➤ "Data Push" on page 254

Population

An integration of Population type copies data from an external data repository into the RTSM, so that the RTSM now controls the data.

You use population in one of the following scenarios:

➤ When you need to track changes made by the RTSM 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 RTSM from other sources in such a way that the source of the data still retains control of the data.

You use the RTSM'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 RTSM only when it is really needed.

Federation also has the benefit that the federated data does not burden the RTSM 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 RTSM does not offer change tracking on federated data because the data does not reside within the RTSM and the RTSM 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 *RTSM Modeling Guide*.

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 RTSM, as well as from other federated data sources, according to how you have configured integration points. As data arrives at the RTSM, 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 on Retrieving Data from Multiple Data Repositories" on page 293.

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 RTSM.

➤ The core data repository must be the RTSM.

➤ 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 266.

➤ 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 RTSM with the attributes from the external data repository.

For details on the Mapping Engine, see "Federation Framework Flow for Federated TQL Queries" in the *RTSM Developer Reference Guide*.

For details on selecting attributes to be included in the federation, see "Federation Tab" on page 266.

For details on how reconciliation is performed, see "Reconciliation" on page 429.

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 RTSM. However, you do not want to store all the desktop data in the RTSM as this is inefficient and unnecessary. It is enough to store core attributes such as name and MAC address in the RTSM, 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 BSM 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 RTSM; 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: RTSM and VMware.

Data Push

An integration of Data Push type copies data from the RTSM to an external data repository, so that the RTSM no longer retains control over this data.

You use data push integrations to feed important data from your RTSM into an external system to facilitate your necessary business processes. An example of this is pushing data discovered by DFM into HP 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.

Tasks

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 page 255

➤ "Set a reconciliation priority" on page 255

➤ "View Instances in IT Universe Manager" on page 255

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 258.

2 Set a reconciliation priority

In the Integration Point pane, select the integration, and click the **Reconciliation Priority Manager** button. For more details, see "Reconciliation Priority Window" on page 465.

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 *RTSM 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 RTSM with data.

This task includes the following steps:

➤ "Create an integration point" on page 256

➤ "Set a reconciliation priority" on page 256

➤ "Run the population job" on page 256

➤ "Build a view of the population results" on page 257

➤ "View instances in IT Universe Manager" on page 257

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 258.

2 Set a reconciliation priority

In the Integration Point pane, select the integration, and click the **Reconciliation Priority Manager** button. For more details, see "Reconciliation Priority Window" on page 465.

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 268.

Select the job.

➤ To synchronize all data for the first time, click the **Run All-Data Sync** button.

➤ To synchronize only the data changes since the job last ran, click the **Run Changes Sync** button.

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 *RTSM 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 *RTSM 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 RTSM to another data repository.

This task includes the following steps:

➤ "Create an integration point" on page 257

➤ "Set Reconciliation priority" on page 257

➤ "Run the Data Push job" on page 258

➤ "Build a view of Data Push results" on page 258

➤ "View instances in IT Universe Manager" on page 258

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 258.

2 Set Reconciliation priority

In the Integration Point pane, select the integration, and click the **Reconciliation Priority Manager** button. For more details, see "Reconciliation Priority Window" on page 465.

3 Run the Data Push job

Data Push 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 268.

Select the job.

➤ To synchronize all data for the first time, click the **Run All-Data Sync** button.

➤ To synchronize only the data changes since the job last ran, click the **Run Changes Sync** button.

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 *RTSM 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 *RTSM Modeling Guide*.

How to Set Up an Integration Point

This task describes how to set up an integration point for a particular integration with UCMDB.

Note: The integration adapters provided with the Discovery and Integration 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" on page 259

➤ "Create an integration point" on page 259

➤ "Add the integration jobs and schedule the jobs to run" on page 260

➤ "For a federation-type integration, define the data to be federated" on page 260

➤ "Save the integration point" on page 260

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 Manage Adapter Configurations" on page 182.

➤ **New External Data Source Adapters:** To configure an adapter for an new external data source, see "How to Add an Adapter for a New External Data Source" in the *RTSM Developer Reference Guide*.

2 Create an integration point

In UCMDB, select **Admin** > **RTSM Administration** > **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 281.

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 285.

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 the *HP Universal CMDB Discovery and Integration Content Guide* PDF.

e Configure the adapter's protocol credentials, where required. For a list of supported protocols, see "Supported Protocols" on page 108.

f Enter the Probes to use for the integration.

g **For Jython Integration adapters only:** Create or select a trigger CI instance for the integration.

3 Add the integration jobs and schedule the jobs to run

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 278.

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 266.

5 Save the integration point

Make sure to save the integration point settings.

🪝 How to Create a CI Topology

You can 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 that you have added to the topology.

For details on creating the topology, see "Topology CI Creation Wizard" on page 288.

🪝 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: You perform the following procedure for each data repository that the package is to be deployed to.

This task includes the following steps:

➤ "Prerequisites" on page 261
➤ "Change timeout - optional" on page 262
➤ "Select the integration point" on page 262
➤ "Select the package" on page 262
➤ "View deployment results" on page 263
➤ "View Log files" on page 263

1 Prerequisites

   a Verify that the Data Flow Probe is configured correctly and is connected to UCMDB.

   b Verify that the version of UCMDB running on the remote machine is version 9.02 or later.

  c Verify that UCMDB running on the remote machine is up and running.

  d Create the package that must be deployed to the remote machine, and deploy this package to the local UCMDB Server.

  Note: By default, you cannot deploy a package that is larger than 10 MB.

---

  e Create an integration point on the local UCMDB Server, that uses the **UCMDB9.x** adapter.

2 **Change timeout - optional**

You can change the time after which UCMDB times out package deployment. If UCMDB cannot connect to the remote machine in 5 minutes, by default, the deployment is timed out.

3 **Select the integration point**

  a In the Integration Point pane, select the integration point that you created in step 1 on page 261. For details, see "Integration Point Pane" on page 275.

  b Click the **Deploy Remote Package** button.

4 **Select the package**

  a In the **Deploy Remote Package** dialog box, select a package from the list of packages existing on the local UCMDB Server. This is the package that you created in step 1 on page 261. For details, see "Deploy Package to Remote Data Repository using Integration Point" on page 265.

  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.

Successful deployment: A package is successfully deployed if all its resources are successfully deployed.

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, version 9.02 or later	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.

Reference

🔍 Integration Studio User Interface

This section includes (in alphabetical order):

🔖 Data Push Tab

This tab 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 268.

➤ View statistics results for jobs that have run. For details, see "Statistics Tab" on page 272.

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.
See also	"New Integration Job/Edit Integration Job Dialog Box" on page 278

🔖 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 275.
Relevant tasks	"How to Deploy a Package to a Remote Data Repository" on page 261

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 *RTSM 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.

User interface elements are described below:

UI Element (A-Z)	Description
	Clears all selected items.
	Inverts the selections.
	Expands the entire hierarchical tree structure.

UI Element (A-Z)	Description
	Collapses the hierarchical tree structure.
CI Type Retrieval Mode	➤ **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 RTSM.
	Retrieve the attribute from the UCMDB too. The attribute can be federated as well as physically retrieved from the RTSM (if any attributes of CI instances exist in the database).
	Note:
	➤ 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	You can define which attributes of an external CIT are to be included in the federation:
	➤ 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.
	Note: Attributes are defined in the CIT Manager. For details, see "Add/Edit Attribute Dialog Box" in the *RTSM Modeling Guide*.
Supported and Selected CI Types	Displays a hierarchical tree containing the supported and selected CI Types and attributes.
	When queried by an TQL query, the CITs you select here are configured to retrieve the data from this external data repository.
	Select the CITs to be supported by this integration point.
	For **BACKPIsAdapter**, select **Real Time KPI**.

❧ 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	➤ 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, 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	➤ "How to Work with Population Jobs" on page 256
	➤ "How to Work with Data Push Jobs" on page 257
See also	➤ "Statistics Tab" on page 272
	➤ "Query Status Tab" on page 273
	➤ "Job Errors Tab" on page 274
	➤ "Discovery Scheduler Dialog Box" on page 388

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 278.
✏	**Edit Integration Job.** Enables you to edit an existing integration job.
✖	**Delete Integration Job.** Deletes the selected integration job from the list.

UI Element (A-Z)	Description
	Refresh. Refreshes the list of integration jobs.
	Note: If you refresh the list of jobs before you save a new job, you are given a choice:
	➤ **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 Changes Sync. Runs the selected population or data push job and synchronizes only the changes in the data since the last time the job was run.
	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.
	Note: 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.
	Run All-Data Sync. Runs a full population or data push job. This job copies or pushes all the relevant data for the job.
	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.

UI Element (A-Z)	Description
<right-click integration job menu>	In addition to the options described above, the right-click menu provides the following functionality: ➤ **Show Results For Job**. DFM sends an ad-hoc request to the Probe and retrieves the latest results of the job. 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. **Available for:** Population jobs only. **Note:** Results are not displayed if the total number of results exceeds 10,000. ➤ **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 201. **Available for:** Population jobs based on Jython adapters only.
Job Name	Name given to the population or data push job.

UI Element (A-Z)	Description
Last Synchronization Type	This column is displayed for data push jobs. The type of the last run: ➤ **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.
Status	**Population jobs:** ➤ **Did not run**. The job has not yet run. ➤ **Waiting for Probe**. The job is waiting for the Probe. ➤ **Pending results**. The job is currently running or is scheduled to run in the future. ➤ **Succeeded**. The job ran successfully. ➤ **Succeeded with warnings**. The job ran successfully but warnings were reported. ➤ **Failed**. The job did not run successfully. ➤ **Disabled.** The integration point is deactivated or the trigger CI is missing. **Data push jobs:** ➤ **Did not run**. The job has not yet run. ➤ **Running**. The job is currently running. ➤ **Ended**. The period between **Running** and **Succeeded** or **Failed**. ➤ **Succeeded**. The last run was successful. ➤ **Failed**. The last run was not successful.

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
	Refreshes the list of CITs.
	Displayed for population jobs only.
	Select the time range or Probe for which to display statistics about the selected job.
	➤ **By Time Range**:
	➤ **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.
	➤ **Custom Range.** Opens 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.

UI Element (A–Z)	Description
<Statistics table>	➤ **CIT**. The name of the discovered CIT. Displayed for population jobs only. ➤ **Query Name**. The name of the query whose data is being pushed. Displayed for data push jobs only. ➤ **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.
Last updated	The date and time that the Statistics table was last updated for the selected job.
Valid to	The date when the data was last synchronized.

Query Status Tab

This tab displays information about the queries defined for the job.

User interface elements are described below:

UI Element (A–Z)	Description
	Refreshes the list of queries.
Finish Time	Displayed for data push jobs only. The time at which data from this query stopped being pushed.
Query Name	The name of the query.
Query Status	**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.
Start Time	Displayed for data push jobs only. The time at which data from this query started being pushed.

Job Errors Tab

This tab displays the errors or warnings reported during the job run.

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

UI Element (A–Z)	Description
	Refreshes the list of errors.
	Select a row and click this button to view details of a message.
<List of error messages>	**Message**. A message describing the cause of failure. **Severity**. For details, see "Error Severity Levels" in *RTSM Developer Reference Guide*. **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 RTSM, in which case the RTSM then has a local copy of these CIs, while the **ServiceManagerAdapter** adapter retrieves data from HP ServiceCenter and HP Service Manager, but HP ServiceCenter or HP 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 191.

To access	Located in the left pane of the Integration Studio.
Relevant tasks	"How to Deploy a Package to a Remote Data Repository" on page 261
See also	➤ "Data Push Tab" on page 265 ➤ "Federation Tab" on page 266 ➤ "Population Tab" on page 284

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 281.
✏️	**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.

UI Element (A-Z)	Description
	Full Integration Refresh. Refreshes the list of integration points and fully refreshes the selected integration point.
	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 261. **Note**: This button is enabled for integration points based on the UCMDB 9.x adapter (which supports package deployment capabilities).
	Open 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 465.
	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.
	Export To XML. Enables you to export the integration point's configuration in XML format. **Note:** You must save a new integration point before you can export its configuration.
<List of integration points>	Displays the list of previously defined integration points.
<right-click integration point menu>	In addition to the options described above, the right-click menu provides the following functionality: ➤ **Go to Adapter.** Opens the adapter used by the integration job in the Adapter Management module.

❧ Integration Studio Page

This page enables you to create and manage integration points.

To access	Select **Admin** > **RTSM Administration** > **Data Flow Management** > **Integration Studio**.

User interface elements are described below:

UI Element (A-Z)	Description
⚙	**Reconciliation Priority Manager.** Opens the Reconciliation Priority Manager. For details, see "Reconciliation Priority Window" on page 465.
Integration Point pane	Enables you to create integration points and edit their configuration. For details, see "Integration Point Pane" on page 275.
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: ➤ "Data Push Tab" on page 265 ➤ "Federation Tab" on page 266 ➤ "Population Tab" on page 284

❧ 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.
See also	"Integration Jobs Pane" on page 268

User interface elements are described below:

UI Element (A-Z)	Description
Name	Enter a name for the job. **Note:** The name must not exceed 45 characters.
Job Definition area	Enables you select integration queries for the job definition. For details, see "Job Definition" below. **Available for:** Non-Jython adapters only.
Scheduler Definition area	Enables you to schedule when to run the integration job. For data push jobs, you can set different schedules for all-data synchronization and change synchronization. For details about the scheduling options, see "Scheduler Definition" below.

Job Definition

UI Element (A-Z)	Description
🟦	**Add Query.** Opens the Enables you to add an available integration query to the job definition.
❌	**Delete Query.** Enables you to delete the selected query from the job definition.
<Query table>	Displays the queries selected for the integration job. **For non-Jython-based Data Push jobs:** Selecting a query's **Allow Deletion** check box enables the deletion of CIs or links for the query from the remote data repository.

UI Element (A-Z)	Description
Allow Integration Job to delete removed data	Enables the deletion of CIs or links per job from the local RTSM. **Available for:** Non-Jython-based Population jobs only.
Select the Job Type	Enables you to select the type of job queries to use for the integration. ➤ **Changes - History-based.** CIs and direct links, not virtual links. Has better performance. ➤ **RMI - Full Topology Comparison.** Supports CIs and all links types. **Note:** Calculated links are not supported. **Available for:** Service Manager Data Push jobs only

Scheduler Definition

UI Element (A-Z)	Description
All-Data Sync tab	Enables you to schedule an all-data synchronization. **Available for:** Data Push jobs only
Changes Sync tab	Enables you to schedule a changes synchronization. **Available for:** Data Push jobs only
Cron Expression	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 *RTSM Modeling Guide*.
Ends	Enables you to select when the job should stop running. ➤ **Never.** The job continues to run until manually stopped. ➤ **Until.** Enables you to select the date when the job should stop running. **Note**: This option is disabled when you select **Once.**

UI Element (A-Z)	Description
Repeat	Enables you to select how often to run the integration job. The available options are: ➤ **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 *RTSM Modeling Guide*.
Repeat every	Enables you to type a value for the interval between successive runs. **Available:** When you select **Repeat > Interval** or **Yearly**. **Unit of time:** ➤ **Interval.** Minutes; Hours; Days; Weeks ➤ **Yearly.** Years
Repeat on	**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.
Repeat on the following dates every month	When you select **Repeat > Day of Month,** enables you select days of the month to run the job. The job runs every month. To clear the selection click the Reset button.
Scheduler enabled	When selected, you can choose scheduling options for the integration job.

UI Element (A-Z)	Description
Server Time	The time on the UCMDB server.
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 the ⟳ button.

🔍 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	Do one of the following:
	➤ Click the **New Integration Point** button ✳ in the Integration Point pane.
	➤ Click the **Edit Integration Point** button 🖉 in the Integration Point pane.
Important information	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.
	Each mandatory field is marked with an asterisk.
Relevant tasks	"How to Create a CI Topology" on page 261

User interface elements are described below:

UI Element (A-Z)	Description
Adapter	Select the adapter for your integration point to use. For details about each adapter, see "Select Adapter Dialog Box" on page 285. For help on the selected adapter, click the **Show Content Help** ? button.
CMDB State (Data Push)	The state of the source machine. Values are: ➤ Actual ➤ Authorized **Note:** This field is visible only when using an adapter that supports data push and on an RTSM for which authorized state has been defined.
Credentials ID	Enables you to set credentials for relevant adapter integration points. To open the **Choose Credentials** dialog box, click ⋯ . For details on adding credentials, see "Supported Protocols" on page 108.
Integration Description	Enter a brief description of the integration point.
Integration Name	Enter a name for the integration point. **Note:** The name may not exceed 45 characters.
Is Integration Activated	Select this check box to create an active integration point. You clear the checkbox if you want to deactivate an integration, for instance, to set up an integration point without actually connecting to a remote machine.

UI Element (A-Z)	Description
Probe Name	The name of the Data Flow Probe used to run population jobs. Do one of the following: ➤ Select the name of a specific Probe that will be used for the population jobs of this integration. When you manually select a Probe, any probe IP ranges that you defined in the Probe settings are ignored. ➤ Use the Auto-Select option. In this case, the RTSM attempts to choose the correct probe according to the IP ranges that were defined for the available Probes. **Note**: A Probe installed on a Linux machine is defined as an Integration Probe and appears in this list.
Push Back IDs	Specifies whether to push back the global IDs after CIs are populated into the server. **Available for:** UCMDB 9.x adapters.
Trigger CI Instance	Displays the CI that is to be used by the integration point as a trigger when integrating with a remote machine. ➤ **Select Existing CI**. Enables you to select the trigger CI through which data is collected during integration. For details, see "Element Instances Dialog Box" in the *RTSM Modeling Guide*. ➤ **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 288. To manage or view the trigger CI, right-click the CI. For details on these operations, see "IT Universe Manager Shortcut Menu" in the *RTSM Modeling Guide*. **Available for:** Jython-based integration adapters only **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.

Note: Additional fields are available, depending on the adapter you select. Descriptions of each field may be viewed by hovering your mouse over that field on the screen. See the *RTSM Developer Reference Guide* for details about specific adapters.

Population Tab

This tab enables you to:

➤ Schedule jobs that populate the RTSM with data from external data repositories. For details, see "Integration Jobs Pane" on page 268.

➤ View statistics results for jobs that have run. For details, see "Statistics Tab" on page 272.

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.
See also	"New Integration Job/Edit Integration Job Dialog Box" on page 278

🔍 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 "How to Add an Adapter for a New External Data Source" in the *RTSM Developer Reference Guide*.

The Integration Framework SDK enables you to create new adapters that connect BSM with external products and services. For details, see "Developing Java Adapters" in the *RTSM Developer Reference Guide*.

To access	Click ... in the New Integration Point/Edit Integration Point Dialog Box.
Important information	The list of adapters displayed depends on your UCMDB License. If you have the UCMDB Foundation License, only the HP Product adapters are displayed.
Relevant tasks	➤ "How to Work with Federated Data" on page 255 ➤ "How to Work with Population Jobs" on page 256 ➤ "How to Work with Data Push Jobs" on page 257
See also	"New Integration Job/Edit Integration Job Dialog Box" on page 278

User interface elements are described below:

UI Element (A-Z)	Description
	Collapses the hierarchical tree structure.
	Expands the hierarchical tree structure.
	Displays help about the selected adapter.
<list of adapters>	Displays a list of out-of-the-box adapters. For details, see "Out-of-the-Box Integration Adapters" below.

Out-of-the-Box Integration Adapters

Note: Most of the adapters listed below are provided with the Discovery and Integrations Content Pack. Unless otherwise indicated, information about each of these adapters can be found in the *HP Universal CMDB Discovery and Integration Content Guide* PDF, or by clicking the **Show Content Help** button for each adapter.

Adapter Name (A-Z)	Description
HP BTO Product Adapters	
BACKPIsAdapter.	Select to define an integration that enables a user to create a FTQL to retrieve, in an external application, the status and values of KPIs that are connected to CIs. For details, see "Viewing KPIs in External Applications" in the *RTSM Developer Reference Guide*.
BSM	Used to perform a population sync from BSM to UCMDB. For details, see <u>RTSM Best Practices PDF</u>.
DDMI	Used to populate and federate data from DDMI.
NNMi: Population from NNMi	Used to populate data from NNMi.
NNMi: Push IDs into NNMi	Used to push UCMDB Node IDs into NNMi.
ServiceCenter 6.2x	Used to federate data from HP ServiceCenter version 6.2x.
Service Manager 7.0x	Used to federate data from HP Service Manager version 7.0x.
Service Manager 7.1x - 9.2x	Used to federate data from HP Service Manager versions 7.1x-9.2x and push data to HP Service Manager versions 7.1x-9.2x.
Storage Essentials	Used to populate CIs and relationships from Storage Essentials.

Adapter Name (A-Z)	Description
Systems Insight Manager	Used to populate CIs and relationships from HP SIM.
UCMDB 8.x	Used to populate data from RTSM version 8.0x or push data to RTSM version 8.0x.
UCMDB 9.x	Used for populating and federating data from RTSM version 9.0x. For details, see "Multiple Deployments with Version 9.0x CMDBs" on page 300.
Third Party Product Adapters	
BMC Atrium	Used to push CIs and relationships to BMC Atrium.
CA CMDB	Used to push CIs and relationships to CA CMDB.
EMC Control Center	Used to populate CIs and relationships from EMC Control Center.
Microsoft SMS	Used to populate and federate data from Microsoft SMS.
Software AG ARIS	Used to populate CIs and relationships from IDS Scheer ARIS.
Troux: Population from Troux	Used to populate CIs from Troux.
Troux: Data Push into Troux	Used to push data into Troux.
Other	
UCMDB API Population	Used to define an integration that specifies the reconciliation priority for data that is added to the RTSM using the RTSM API. For details, see "RTSM (HP Universal CMDB) API" in the *RTSM Developer Reference Guide*.

✿ 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	Select a discovery Jython adapter in the **New Integration Point** dialog box. In the Trigger CI Instance menu, choose **Create New CI**.
	Note: This wizard is available for discovery Jython adapters only, when the **Used as Integration Adapter** check box is selected. Moreover:
	➤ All conditions (attributes, cardinality, qualifiers, and so on) are disregarded in the Input query.
	➤ Only regular links (not join or compound links) are allowed in the Input query.
	For details on the **Used as Integration Adapter** check box, see "Adapter Definition Tab" on page 191.
Important information	➤ **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 281
Wizard Map	The Topology CI Creation wizard contains:
	Topology Preview > Define CI: <CI name> > Define Credentials > Topology Creation > Summary

🔖 Topology Preview

Enables you to preview the topology definition of the integration point.

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
▦	**Show Legend.** Toggles between hiding and displaying the topology legend.
<toolbar and legend>	For details, see "Toolbar Options" in the *RTSM Modeling Guide*.

🔍 Define CI: <CI name>

Enables you to define properties of a new CI instance of the CIT.

Important information	➤ 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	➤ 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 "Domain Credential References" on page 103 and "Details Pane" on page 155.
	➤ This page is displayed if the adapter writer has defined that credentials are needed to access the discovered component.
See Also	For details on using the buttons and shortcut menus, see "Domains and Probes Pane" on page 162.
	For details on the protocols, see "Supported Protocols" on page 108.
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	➤ If DFM displays a success message, click **Finish**. **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. ➤ 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 Services" on page 437. ➤ 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**

🔍 Troubleshooting and Limitations

This section includes troubleshooting and limitations for the Integrations Studio functionality.

This section includes the following topics:

➤ "Limitations on Retrieving Data from Multiple Data Repositories" on page 293

➤ "Limitations on All Adapters" on page 294

Limitations on Retrieving Data from Multiple Data Repositories

➤ When a virtual link exists between two data repositories, HP BSM supports mapping in the following cases only:

> ➤ The BSM 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 (BSM) and B's data repositories (BSM, d2, d3).
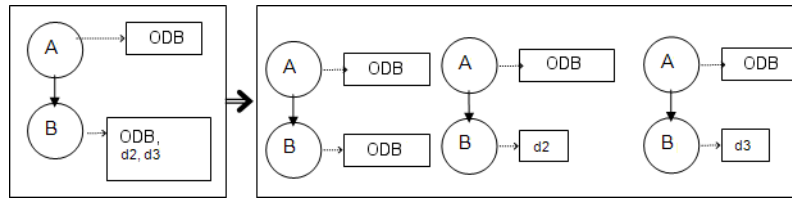
> ➤ The same data repositories lie at both ends of the link. The link is an internal link of each data repository and no mapping is required.
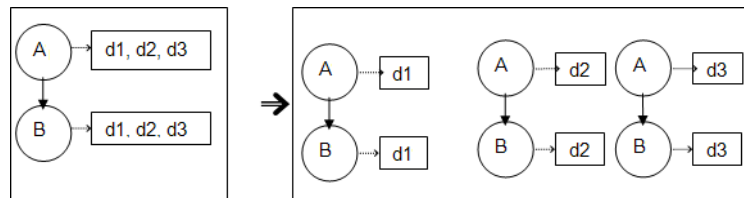
Limitations on All Adapters

➤ 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 *RTSM Modeling Guide*.

➤ Do not choose a CIT to be supported by an external data repository if instances of this CIT exist in the local RTSM, as this can lead to state inconsistency. For example, if there are instances of the CPU CIT in the local RTSM, you must not choose the CPU when defining an external data repository, even if the selected adapter supports it.

➤ When configuring a population or data push job between two RTSMs, verify that the class model is the same in the two RTSMs.

➤ After modifying a TQL query that is used for in a population or data push job, it is recommended to run a differential synchronization and then a full synchronization. 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.

➤ After a job runs successfully, its status remains as "Succeeded" even after the job definition is changed (for example, selecting another TQL query or enabling deletion) and saved.

➤ You cannot edit the values of attributes that are configured to be retrieved from both an external data repository and UCMDB during federation.

10

Integrating Multiple CMDBs

This chapter includes:

Concepts

➤ Integrating Multiple CMDBs Overview on page 296

➤ Configuration Management System (CMS) on page 296

➤ Global ID on page 297

➤ Use Cases – Multiple CMDB Deployments on page 298

➤ Multiple Deployments with Version 9.0x CMDBs on page 300

➤ Federation in Version 9.0x CMDBs on page 304

Tasks

➤ How to Perform Initial Synchronization on page 307

➤ How to Configure Global ID Generation on page 308

➤ How to Use SSL with the UCMDB 9.x Adapter on page 309

➤ How to Set Up Integrations Between Two BSMs on page 310

➤ How to Set Up Integrations between CMS and BSM on page 311

➤ How to Configure CMS-RTSM Credentials Synchronization on page 314

Reference

Troubleshooting and Limitations on page 317

Concepts

🏵 Integrating Multiple CMDBs Overview

Note: Synchronization between the CMS and RTSM uses the multiple CMDBs mechanism that is part of BSM. References to UCMDB and CMDB in this chapter refer to the instance of UCMDB that is embedded in BSM.

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 following table shows the versions of BSM and CMS that can be synchronized:

BSM version	RTSM version (supported and tested)	CMS versions – for CMS sync	
		Supported	Tested
BSM 9.00	RTSM 9.0.1	CMS 9.01	CMS 9.01
BSM 9.01	RTSM 9.011	CMS 9.01	CMS 9.01
BSM 9.10	RTSM 9.021	CMS 9.00, 9.01, or 9.02	CMS 9.02

🏵 Configuration Management System (CMS)

The 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. 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

Global ID

The global ID is a unique CI ID (generated by the CMS or another CMDB that has been designated as a global ID generator for that CI type), that identifies that CI across the entire portfolio, making it easier to work in multiple CMDB environments.

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 308.

🔧 Use Cases – Multiple CMDB Deployments

RTSM–CMS Solution
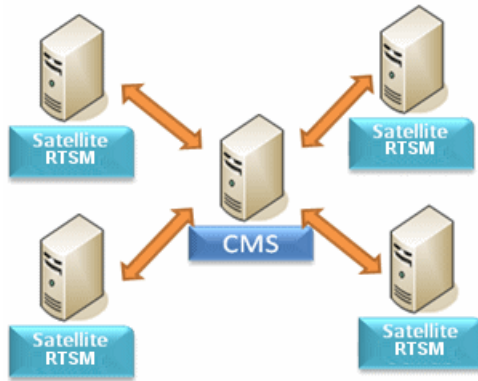
The solution includes:

➤ RTSM

➤ The central CMDB acting as the CMS

➤ Service Manager (SM)

RTSM is the operational storage of BSM. Configuration items (CIs) discovered by different BSM data sources are reconciled and stored in the RTSM.

It is recommended to connect DDM to the central CMDB instance (which can also serve as a CMS) and then use topology synchronization between CMDB/CMS and BSM to populate RTSM with additional CIs that are relevant for operational use cases.

For guidelines on which topology is recommended to be synchronized from CMS to RTSM and from RTSM to CMS, see "When to Use CMS-BSM Synchronization?" in the *RTSM Best Practices* PDF.

To setup CMS-BSM synchronization, it is recommended to use an out-of-the-box integration point. See "How to Set Up Integrations between CMS and BSM" on page 311 to learn how to configure the out-of-the-box integration point.

BSM supports a hierarchical deployment that allows the forwarding of events and topology from one BSM instance to another. The main motivations for building hierarchical deployment are:

➤ **Scale.** When a hierarchy of BSM deployments is defined to deal with a very large number of events. The upper instances of the deployment get only "important" summary events.

➤ **Geographical distribution.** When several Data Centers in different geographical locations manage their own instances of BSM. In this use case, the data from the different geographical locations can be consolidated into one central instance (Manager Of Managers).

➤ **Organizational structure.** When the structure of the organization includes several BSM instances for each business unit or department. The consolidated picture is achieved either by synchronizing those instances two ways or by defining one central MoM (Manager of Managers) instance.

➤ **Functional structure.** When the IT department chooses to manage applications and infrastructure separately by creating two separate BSM instances for Application owners and Infrastructure owners. In this deployment, there can be several BSM instances, each one operated by domain experts — APM (Application Performance Management performed by BSM), NNMi, or HPOM.

➤ **Different consumers.** When the multi-tenancy is implemented by multiple instances of BSM.

➤ **Organizational mergers and acquisitions.** Sometimes there are several BSM instances as a result of mergers and acquisitions. Consolidation can be achieved by synchronizing the data to one central instance.

To setup simple BSM-BSM synchronization, it is recommended to use an out-of-the-box integration point. See "How to Set Up Integrations Between Two BSMs" on page 310 to learn how to configure the out-of-the-box integration point.

For details about setting up a custom integration point, see "How to Work with Population Jobs" on page 256.

For more complex deployments that include both hierarchical, multiple BSM deployments, and CMS, as part of one ecosystem, see "BSM Hierarchical Deployment" in the *RTSM Best Practices* PDF.

⚙ Multiple Deployments with Version 9.0x CMDBs

This section includes:

➤ "Population from BSM 9.0x (CMS Synchronization)" on page 300

➤ "Query Support" on page 300

➤ "Global ID Synchronization" on page 301

➤ "Automatic Completion of Reconciliation Data" on page 303

➤ "Out-of-the-Box Integration TQL Query" on page 304

Population from BSM 9.0x (CMS Synchronization)

When you use the UCMDB 9.0x adapter to create an integration point, you are able to synchronize data between different CMDB instances using population. For details on population, see "How to Work with Population Jobs" on page 256.

During population, global IDs are synchronized. For details, see "Global ID Synchronization" on page 301.

Query Support

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 9.0x 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 9.0x 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 *RTSM Administration Guide*.

You can create TQL queries for integration. For details, see "Topology Query Language" in the *RTSM 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 RTSM-B, which may be any RTSM. RTSM-B uses the population flow to populate data from the CMS.

Because synchronization is performed in two directions, global IDs are also updated on RTSM-B.
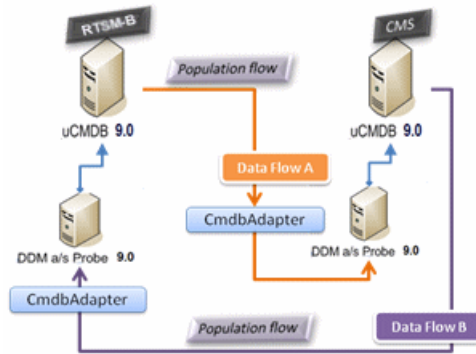
➤ Pushback of IDs

The CMS uses the population flow to retrieve data from RTSM-B. CIs are reconciled with the data in the CMS.

The global-ID in the CMS for each CI received is pushed back to RTSM-B.
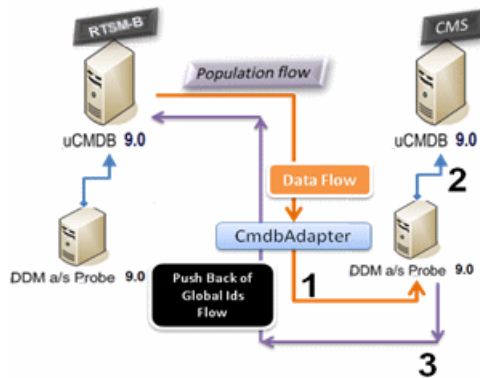
The default state of this option is disabled.

Automatic Completion of Reconciliation Data

The UCMDB 9.0x 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.

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 "Results Management Pane" on page 203.

Out-of-the-Box Integration TQL Query

The RTSM to CMS integration TQL query is used to:

➤ Populate data from the RTSM to the CMS. Such data can include BusinessElements, CI collections, Parties and any infrastructure element connected to them and all the links between them.

➤ Populate locations connected to any of these CIs (that are defined as sub-graphs for each CI).

HP Software recommends that you schedule this query to run every 10 minutes, so that both the RTSM and the CMS are continually updated with the most recent CIs.

To define this schedule:

1 In the Job Definition window, select the **Scheduler Definition** checkbox.

2 Select the **Cron** repeat type.

3 In the **Cron Expression** field, enter *** 0/10 * * * ? *** and click **Validate**.

Note: You should take into account the amount of time it takes to run a full sync, and adjust the schedule of the out-of-the-box query (a differential sync) accordingly.

Federation in Version 9.0x CMDBs

Federation allows the CMDB to retrieve data in real time (on-the-fly) from any remote data repository, and combine it with 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 255.

Using the UCMDB 9.0x 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 CITs, 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 9.0x 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.

In the following example, the SM integration point is defined with **incidents** as federated CIs, and the RTSM has **incidents** federated from the CMS. Whenever the RTSM requests an **incident**, it requests it from the CMS, which in turn requests it from SM and returns the answer to the RTSM.
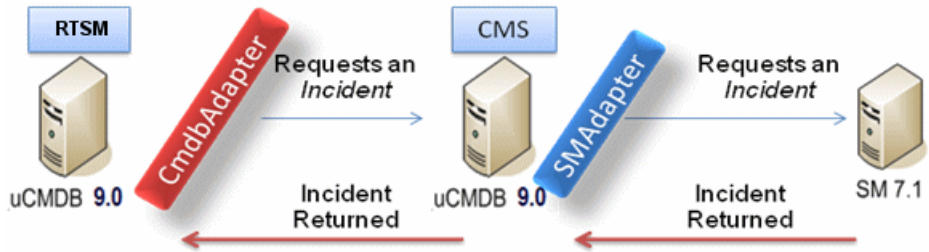
Tasks

🔧 How to Perform Initial 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 RTSM. The procedure is generally intended to be performed only once, on a new system.

Note: This procedure can be performed only on UCMDB version 9.02 or later.

---

1 Launch a Web browser that connects to the CMS, and enter the following address: **http://<CMS server>:8080/jmx-console**.

2 Click **UCMDB:service=Multiple CMDB Instances Services** to open the JMX MBEAN View page.

3 Click the **fetchAllDataFromAnotherCMDB** method.

4 Enter values as required for the following fields:

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

➤ Customer ID
➤ Remote user name
➤ Remote password
➤ Remote host name
➤ Remote port **21212**

➤ Remote Customer name (default value is **Default Client**)

➤ Maximum chunk size

➤ CI type to sync (default value is **managed_object**, causing all CI types to be synchronized)

➤ Relation type to sync (the default value is **managed_relationship**, causing all relation types to be synchronized)

5 Click **Invoke**.

🔧 How to Configure Global ID Generation

1 Launch the Web browser and enter the following address: **http://<RTSM server>:21212/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 or which UCMDB/RTSM instance is acting as the CMS, use the **getGlobalIdGeneratorScopes** method.

⚡ How to Use SSL with the UCMDB 9.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 commands (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
hppass -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 changeit -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 Two BSMs

The following steps describe how to create integration points and jobs to integrate between two BSMs.

➤ "Configure an RTSM-to-RTSM integration point" on page 310

➤ "Define a population job (optional)" on page 311

➤ "Run the population job (optional)" on page 311

1 Configure an RTSM-to-RTSM integration point

a Navigate to **Admin** > **RTSM Administration** > **Data Flow Management** > **Integration Studio**.

b Select the RTSM integration point.

c Click the **Edit Integration Properties** button.

Enter the following information:

Name	Recommended Value	Description
Hostname/IP	**<user defined>**	The name of the server on which the remote RTSM resides.
Credentials	**<user defined>**	Use the credentials necessary for connecting to the remote RTSM machine. For details, see "Domain Credential References" on page 103.
Probe Name	**<user defined>**	The name of the probe to be used for the synchronization.
Is Integration Activated	**selected**	Select this check box to create an active integration point.

d Click **Save**.

2 Define a population job (optional)

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 from step 1. For details, see "New Integration Job/Edit Integration Job Dialog Box" on page 278.

Note:

➤ When integrating between multiple CMDBs, population queries must be set up for the source CMDB.

➤ Select the **Allow Delete** 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.

---

3 Run the population job (optional)

Click the **Run Changes Sync** button to make sure that the integration has been successfully configured.

🔧 How to Set Up Integrations between CMS and BSM

The following steps describe how to create an integration point for CMS-RTSM synchronization. In this procedure, the CMS can be an RTSM installation or a standalone CMDB.

➤ "Deploy CMStoRTSM_Sync.zip package" on page 312

➤ "Define an integration point" on page 312

➤ "Schedule the CMS to RTSM Sync population jobs" on page 313

➤ "Run the population jobs" on page 313

➤ "Configure delegation of federation" on page 313

1 Deploy CMStoRTSM_Sync.zip package

Follow the procedure described in "How to Deploy a Package to a Remote Data Repository" on page 261.

2 Define an integration point

a Navigate to **Admin** > **RTSM Administration** > **Data Flow Management** > **Integration Studio**.

b Select the CMS to RTSM Sync integration point.

c Click the **Edit Integration Properties** button.

Enter the following information:

Name	Recommended Value	Description
Credentials	**<user defined>**	Select the credentials that are to be used to connect to the CMS. For details, see "Domain Credential References" on page 103.
Hostname/IP	**<user defined>**	The name of the server on which the CMS resides.
Is Integration Activated	**selected**	Select this check box to create an active integration point.
Probe Name	**<user defined>**	The name of the probe that is to be used for synchronization.

d Click **Test Connection** and then click **OK**.

3 Schedule the CMS to RTSM Sync population jobs

This step is optional, and required only if a user wants to change the default scheduling. Default scheduling for Virtualization_sync topology query language (TQL) is every 5 minutes, and for all other TQLs, every 10 minutes.

a Click the Population tab.

b Select each of the CMS to RTSM Sync jobs for which you want to change the default scheduling.

c Set the required settings for each job in the Scheduler pane.

4 Run the population jobs

Click the **Run Changes Sync** button for each job to make sure that the integration has been successfully configured.

5 Configure delegation of federation

The same integration point is used to configure delegation of federation to CMS. For more details, see "Federation in Version 9.0x CMDBs" on page 304.

By default, the federation of the following classes is delegated to CMS: Incident, Problem, Request for Change and KPIObjective. To modify the out-of-the-box configuration, go to the Federation tab for CMS to RTSM synchronization integration point and modify the selection of the federated classes.

⚒ How to Configure CMS-RTSM Credentials Synchronization

Make sure that LW-SSO is configured on the CMS. For proper configuration, the init string should be same as on the RTSM. If the CMS and the RTSM are in different domains, both domains should be added to the LW-SSO configuration). For details, see "Configure LW-SSO Settings on the RTSM Server" in the *RTSM Data Flow Management Guide*.

To change the CM instance name on a UCMDB instance:

Note: This procedure must be performed immediately after installation.

---

1 On the RTSM that is not the global ID generator, launch the Web browser and enter the following address:
   http://<RTSM server>:21212/jmx-console.

2 Click **UCMDB:service=Security Services** to open the JMX MBEAN View page.

3 Click the **CMGetConfiguration** method.

4 Click **Invoke**.

   The XML of the current CM configuration is displayed.

5 Copy the contents of the displayed XML and paste them into a text editor.

6 Change the instance name to RTSM or any name that is unique in the deployment of multiple data repositories.

   Example:

   ```
   <serverInstance>
       <instanceName>RTSM</instanceName>
   </serverInstance>
   ```

7 Copy the updated XML.

8 Navigate back to the **Security Services** JMX MBean View page.

9 Click the **CMSetConfiguration** method.

10 Paste the copied XML into the **Value** field.

11 Click **Invoke**.

To synchronize credentials:

1 On the machine that is the destination for the synchronization, launch the Web browser and enter the following address: **http://<RTSM server>:21212/jmx-console**.

2 Click **UCMDB:service=Security Services** to open the JMX MBEAN View page.

3 Click the **CMGetConfiguration** method.

4 Click **Invoke**.

The XML of the current CM configuration is displayed.

5 Copy the contents of the displayed XML and paste them into a text editor.

6 Make the following changes:

➤ On line 24: uncomment the <replication> tag by changing <!--replication> to <replication>.

➤ On line 25: enter the user name ADMIN in the <globalIntegrationUser> tag, as follows: <globalIntegrationUser>ADMIN</globalIntegrationUser>.

➤ On line 28: insert the relevant customer ID, as follows: <customer>
    <id>*relevant customer ID*</id>

7 On the machine that is the source for the synchronization, launch the Web browser and enter the following address: **http://<RTSM server>:21212/jmx-console**.

8 Click **UCMDB:service=Security Services** to open the JMX MBEAN View page.

9 Click the **CMGetConfiguration** method.

10 Click **Invoke**.

The XML of the current CM configuration is displayed.

11 Copy the contents of the displayed XML and paste them into a text editor

12 Make the following changes:

➤ Copy the <CMEncryptionDecryption>...</CMEncryptionDecryption> section (lines 6 through 22) from the XML mentioned in step 11 and paste them into lines 37 through 53 of the XML mentioned in step 5.

➤ On line 55: uncomment the <rest> tag by changing <!--rest> to <rest>.

➤ On line 57: uncomment the <serverConnectionInfo> tag by changing <!--serverConnectionInfo> to <serverConnectionInfo>.

➤ On line 59: enter the replication source server name, as follows: <serverHost>*relevant source CMDB host*</serverHost>.

➤ In line 61: configure the relative URL for the CM application, as follows: <serverContext>cm/rest</serverContext>.

13 Copy the updated XML from the text editor.

14 Navigate back to the **Security Services** JMX MBean View page on the machine that is the destination for the synchronization.

15 Click the **CMSetConfiguration** method.

16 Paste the copied XML into the **Value** field.

17 Click **Invoke**.

Reference

🔍 Troubleshooting and Limitations

Troubleshooting

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

➤ RTSM server logs

  ➤ fcmdb.log

  ➤ fcmdb.adapters.log

  ➤ error.log

  ➤ cmdb.reconciliation.log (for population jobs)

➤ Probe logs

  ➤ wrapperProbeGw.log

  ➤ fcmdb.log

  ➤ fcmdb.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 RTSM with additional CIs or links, in order to contain sufficient information to insert the CIs into the RTSM.

➤ **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 RTSM.

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 RTSM 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. Select **Show full path between source and target CIs** in the query's Compound Relationship properties.

➤ **Problem.** Authentication fails.

Solution. Since the UCMDB 9.0x adapter uses the RTSM API for connection, set up an integration user to ensure that you provide proper credentials. For details, see "How to Create an Integration User" in the *RTSM Developer Reference Guide*.

Limitations

➤ If the TQL query for a population job (defined on the source) includes CI types or links on the source that do not exist on the target, or links that are not valid, those types or links are ignored in the target data repository.

➤ If you are planning to synchronize between an RTSM and another data repository, it is recommended that you increase the Model capacity level on to the Server Deployment Page. After this, you must restart all BSM servers.

➤ Since the UCMDB 9.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.

➤ Selecting the **root_container** property in the Layout Settings dialog box (in any of the nodes in a query that is used for synchronization) when you create a TQL query may cause the synchronization to fail.

➤ When synchronizing a federated query:

  ➤ Always supply all the necessary reconciliation data, for example linked **ip_address** and **interface** CIs for every node CI.

  ➤ When a CI type has **root_container** as a required attribute, always add the CI type that contains it and the composition link between them.

➤ If attributes that were key attributes in version 8.0x are updated in version 9.0x, a differential push job will create a new CI in version 8.0x. This means that the CI that was previously pushed is not updated, and a new CI is created with the updated data. The old CI may be deleted using the aging mechanism. For details, see "CI Lifecycle and the Aging Mechanism" in the *HP Universal CMDB Administration Guide*.

➤ The following relationships are not supported:

  ➤ Sub-graph relationships

  ➤ Virtual/compound relationships

  ➤ Relationships with key attributes (such as client-server)

➤ Federated TQL queries are not supported for data push jobs.

Part IV

Discovery

11

Discovery Control Panel

This chapter includes:

Concepts

➤ Discovery Control Panel Overview on page 324

➤ Viewing Permissions While Running Jobs on page 327

➤ Managing Problems With Error Reporting on page 328

➤ The Permissions Document on page 328

Tasks

➤ How to Use Discovery Control Panel – Basic Mode Workflow on page 330

➤ How to Use Discovery Control Panel – Advanced Mode Workflow
  on page 331

➤ How to View Job Information on the RTSM Data Flow Probe on page 336

➤ How to Manually Activate Jobs on page 337

➤ How to Manage Errors on page 337

➤ How to Find Errors on page 339

Reference

➤ Operation Commands on page 340

➤ Job Operation Parameters on page 349

➤ Discovery Control Panel User Interface on page 351

Concepts

🔩 Discovery Control Panel Overview

The Discovery Control Panel pages enable you to activate jobs that discover the components of your system. You activate discovery with one of the following methods:

➤ Use **Basic Mode** to run discovery for a specific component (for example, the infrastructure, J2EE applications, or databases), using configurable, default preferences.

For details on the workflow, see "How to Use Discovery Control Panel – Basic Mode Workflow" on page 330.

For details on the Discovery wizard, see "Basic Mode Window" on page 354.

Note: Basic Mode is displayed by default when you access the Discovery Control Panel.

➤ Use **Advanced Mode** to run discovery to customize a run by making changes to a job.

For details on the workflow, see "How to Use Discovery Control Panel – Advanced Mode Workflow" on page 331.

For details on the Discovery wizard, see "Advanced Mode Window" on page 352.

Jobs are organized in modules as follows:

➤ **Cluster and Load Balancing Solutions.** The modules discover Microsoft Cluster, ServiceGuard, Veritas, Alteon LB, Cisco CSS, F5 Big IP, and Microsoft NLB.

➤ **Database**. Discovery first finds instances of databases, then of the database resources (for example, users, tables, tablespaces) for each database instance. Run-time Service Model includes predefined default views of the DB2, Oracle, and Microsoft SQL Server databases.

➤ **Deprecated Jobs.** Contains jobs that are no longer supported and should not be used.

➤ **Enterprise Applications.** The modules discover Active Directory, Microsoft Exchange, Oracle E-Business Suite components, the SAP environment based on Computer Center Management System (CCMS), the Siebel environment (such as the Siebel topology and database), WebSphere MQ, and the UDDI registry Web services.

➤ **Discovery-Based Product Integrations** (Content Packs 9.0 and earlier). These modules are needed for integration between RTSM and NNM Layer 2, Storage Essentials, EMC Control Center, IDS Scheer Aris, System Insight Manager, and Troux.

Note: If you have Content Pack 9.01 or later, these integration adapters no longer appear in this module. Instead, they are defined and run from the Integration Studio. For details, see "Out-of-the-Box Integration Adapters" on page 286.

➤ **J2EE Application Servers.** The modules discover JBoss, Oracle Application Server, WebLogic, and WebSphere components.

➤ **Mainframe.** This module discovers Mainframe applications.

➤ **Network Connections.** All jobs in these modules run queries against the Data Flow Probe's MySQL database to retrieve network connectivity information inserted by the **Host Resources and Applications** and/or **TCP By Shell/SNMP** and/or **Collect Network Data by Netflow** jobs.

➤ **Network Discovery.** The modules discover resources on Windows and UNIX hosts, for example, disk information, running processes or services, host connections, and so on.

➤ **Others.** This module holds the jobs necessary to discover document files and directories, discover hosts, import data from external sources, and serve as a template example.

➤ **Storage.** This module discovers Storage applications.

➤ **Virtualization Solutions.** The module discovers VMware components.

➤ **Web Servers.** The modules discover Apache and Microsoft IIS for Windows, SunOne for Solaris, and IBM HTTP Server.

Note: To view Help on Discovery Control Panel components:

➤ For details on the Discovery Modules pane, see "Discovery Modules Pane" on page 383.

➤ For details on the Details tab, see "Discovery Control Panel - Details Tab" on page 370.

➤ For details on the Properties tab, see "Properties Tab" on page 413.

➤ For details on the Dependency Map tab, see "Dependency Map Tab" on page 368.

Discovery Wizards

As the creation of Discovery wizards entails a very advanced knowledge of Data Flow Management, it is recommended that you contact HP Software Support before beginning the work.

🔷 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; if an adapter is changed, the information in this dialog box is not updated.

For details, see "Discovery Permissions Window" on page 386.

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 Status pane shows that DFM 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.

🕸 Managing Problems With Error Reporting

During discovery, many errors may be uncovered, for example, connection failures, hardware problems, exceptions, time-outs, and so on. DFM displays these errors in Discovery Control Panel, in both Basic and Advanced Mode. 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.

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 Status pane. For details, see "Discovery Status Pane" on page 372.

🕸 The Permissions Document

Note: This functionality is available as part of Content Pack 4.00 or later.

You can view a list of DFM jobs together with the protocols and permissions needed to access the job components. For example, you can view information about what is needed to execute a basic login when running the Host Resources by Shell job.

To view the list, access this file: http://<UCMDB Server>:8080/ucmdb-ui/docs/permissions.jsp.

The list is organized by module and consists of the following information:

➤ Module

➤ Job

➤ Protocol

➤ Operation, usage description, objects and parameters

Example of Permissions Document Contents

Database - Oracle. The module name.

Oracle RAC Topology by Shell. The job name.

Discovers Oracle RAC Topology by Shell. The job description. This section is omitted if no description is defined in the application.

Protocol: Shell. The protocol name: SQL, Shell, WMI, SNMP, and so on. For a full list, see "Domain Credential References" on page 103.

Operation	Usage Description	Objects and Parameters
file read	Parsing of listener and tnsnames configuration files	cat $ORACLE_HOME\network\listener.ora cat $ORACLE_HOME\network\admin\tnsnames.ora

Tasks

⚓ How to Use Discovery Control Panel – Basic Mode Workflow

This task describes how to begin mapping your system and its components, using the Discovery wizards. You run this workflow to use default values for the components in an infrastructure, database, or J2EE discovery.

Note: For details of running Data Flow Management in Advanced Mode, see "How to Use Discovery Control Panel – Advanced Mode Workflow" on page 331.

---

1 Prerequisites

Verify that the RTSM Data Flow Probe is installed. For details on installing the Probe, see "Data Flow Probe Installation on the Windows Platform" on page 51 or "Data Flow Probe Installation on the Linux Platform" on page 75.

For details on licensing, see "Licensing Models for Run-time Service Model" on page 39.

2 Access the Discovery Wizard

For details, see the relevant wizard: "Infrastructure Discovery Wizard" on page 393, "J2EE Discovery Wizard" on page 401, or "Database Discovery Wizard" on page 360.

🎺 How to Use Discovery Control Panel – Advanced Mode Workflow

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 of running discovery in Basic Mode, see "How to Use Discovery Control Panel – Basic Mode Workflow" on page 330.

This task includes the following steps:

➤ "Prerequisites" on page 331

➤ "Determine the network range" on page 332

➤ "Set the relevant credentials" on page 332

➤ "Activate the relevant jobs" on page 333

➤ "Make changes to relevant adapters" on page 333

➤ "Monitor the DFM process" on page 334

➤ "View Result Statistics" on page 335

➤ "Troubleshoot the Results" on page 336

1 Prerequisites

a Verify that the RTSM Data Flow Probe is installed. For details on installing the Probe, see "Data Flow Probe Installation on the Windows Platform" on page 51 or "Data Flow Probe Installation on the Linux Platform" on page 75.

For details on licensing, see "Licensing Models for Run-time Service Model" on page 39.

b Verify that the relevant packages are deployed.

For details, see "How to Deploy a Package" in the *RTSM Administration Guide*.

2 **Determine the network range**

You must define the network range of the network to be discovered. For details, see "Add/Edit IP Range Dialog Box" on page 149.

Note: Adapters try to connect to every IP in a range. Therefore, if a range is wide, network performance may be affected.

---

3 **Set the relevant credentials**

To enable Data Flow Management to connect to servers or applications using specific protocols, you must set the relevant credentials (for example, NTCmd, SNMP, TTY, or WMI). For details on protocol parameters, see "Domain Credential References" on page 103. For details on the Details pane in the Data Flow Probe Setup window, see "Details Pane" on page 155.

Note: Data Flow Management tries to connect to a host by using each credential in turn. DFM then saves the successful credential. The next time DFM connects to this host, it first tries to connect using the successful credential.

---

4 **Activate the relevant jobs**

Once you have defined the network range and set credentials, you can run discovery on specific jobs. For details, see the *HP Universal CMDB Discovery and Integration Content Guide* PDF.

Tip: You can view a full description of a job. Select a module and locate the Description pane in the Properties tab.

Example – Finding SNMP Connections:

You can search for all jobs that discover SNMP connections: in the **Discovery Control Panel** > **Discovery Modules** pane, click the **Search for Discovery Job** icon. In the **Find Job**s dialog box, enter **SNMP** in the **Name** box and click **Find All**. For details, see "Find Jobs Dialog Box" on page 392.

5 **Make changes to relevant adapters**

You can customize adapters to discover infrequent system components. For details on adapter writing, see "Adapter Development and Writing" in the *RTSM Developer Reference Guide*.

Caution: Do not make changes to default adapters without consulting HP Software Support.

---

6 **Monitor the DFM process**

For details on monitoring the CIs that are discovered by the run, see "Statistics Results Pane" on page 378.

a   Define a query

You create a query that retrieves information about CIs and CITs from the CMDB. For details, see "How to Define a TQL Query" in the *RTSM Modeling Guide*.

If necessary you can trigger queries to manually discover objects. For details, see "Trigger Queries Pane" on page 418.

b   Build a View for each query

A view enables you to build a subset of the overall IT universe model, containing only those CIs in the CMDB that relate to a specific discovery. For details, see "Pattern View Editor" in the *RTSM Modeling Guide*.

Example – Creating a View to Display Discovered CI Instances:

To view the number of instances found by BSM, select **Admin > RTSM Administration > Modeling > IT Universe Manager**, and display the view you created, as seen in the following illustration:
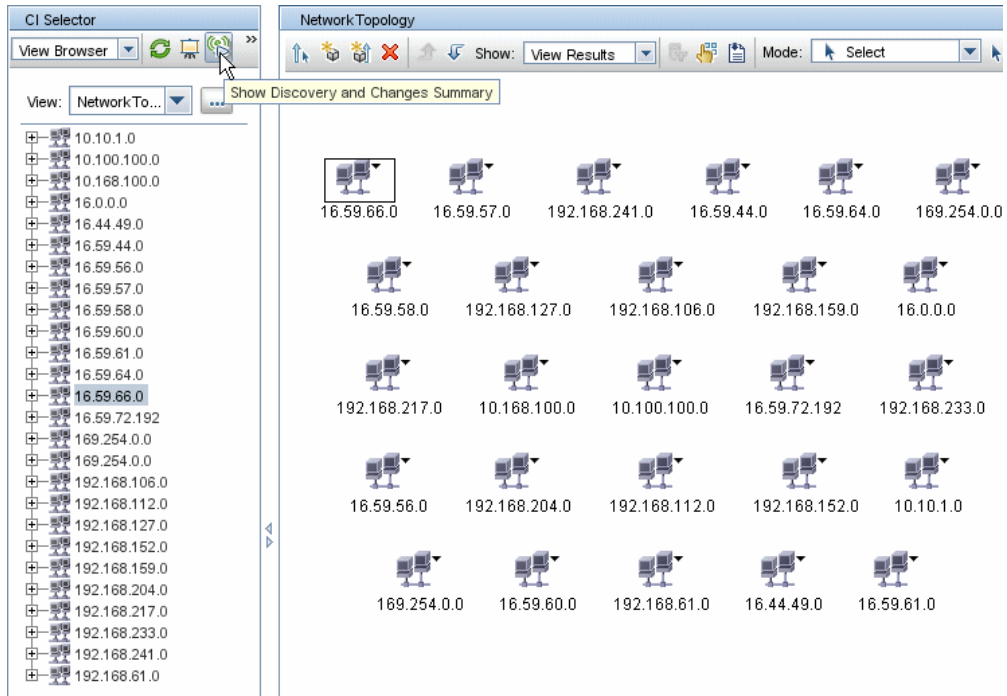
7 View Result Statistics

You can display overall statistics for a job or you can filter the results by time range or by Probe. Each time you log in to Run-time Service Model and access Discovery Control Panel, the statistical data is updated so that the data displayed is the latest for the selected module or job.

For details on working with the statistical data, see "Statistics Results Pane" on page 378.

You can also view discovered CIs by accessing the Probe Snapshot Information pane. For details, see "Data Flow Probe Status Window" on page 240.

8 Troubleshoot the Results

You can check DFM results to see which errors are being reported. For details, see "Discovery Status Pane" on page 372.

🦖 How to View Job Information on the RTSM Data Flow Probe

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

This task includes the following steps:

➤ "Access the MBean operations" on page 336
➤ "Locate the operation to invoke" on page 336
➤ "Run the operation" on page 337

1 Access the MBean operations

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

a Launch the Web browser and enter the following address:

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

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

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

2 Locate the operation to invoke

In the MBean View page, locate the operation. For details, see "Operation Commands" on page 340 and "Job Operation Parameters" on page 349.

3 Run the operation

Click the 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).

How to Manually Activate Jobs

You can activate a job by clicking the **Activate** button in the Discovery Modules pane. You can manually activate a CI by disabling the query and adding a CI. (You disable a query in the **Edit Probe Limitation for Queries Output** dialog box. You manually add a CI in the Choose CIs to Add dialog box.) The job runs using only the redispatched CIs. For details, see "Discovery Modules Pane" on page 383.

How to Manage Errors

This task describes how to investigate problems that arise during a run.

Note: For details about severity levels and so on, see "Managing Problems With Error Reporting" on page 328.

This task includes the following steps:

➤ "Prerequisites" on page 339

➤ "Run the Discovery Wizard or Select the Job" on page 339

➤ "Locate the Problem CI" on page 339

➤ "Troubleshoot the problem" on page 338

1 Prerequisites

Set up DFM. For details, see Part II, "Data Flow Management Setup."

2 Run the Discovery Wizard or select the job

In Basic Mode, you can view error messages for a default job. In Advanced Mode, you can view error messages for one job, one module, or all modules. For details on running a wizard in Basic Mode, see "How to Use Discovery Control Panel – Basic Mode Workflow" on page 330. For details on running a job, see "How to Use Discovery Control Panel – Advanced Mode Workflow" on page 331.

3 Locate the problem CI

Use the Discovery Status pane to drill down to the error messages. For details, see "Discovery Status Pane" on page 372.

Example:

DFM displays the error message:

```
<< Progress message, Severity: Fatal>>
Probe DefaultProbe is missing at least one of the discovery pattern's required protocols for job:
DB2 Connection by SQL


                                                          OK
```
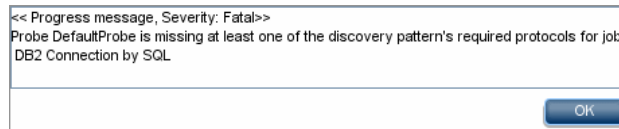
4 Troubleshoot the problem

- ➤ For Fatal errors, you should contact HP 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 201.

- ➤ For details on managing problems, see "Managing Problems With Error Reporting" on page 328.

🔨 How to Find Errors

This task describes how to investigate problems that arise during a run.

Note: For details about severity levels and so on, see "Managing Problems With Error Reporting" on page 328.

This task includes the following steps:

➤ "Prerequisites" on page 339

➤ "Run the Discovery Wizard or Select the Job" on page 339

➤ "Locate the Problem CI" on page 339

1 Prerequisites

Set up DFM. For details, see Part II, "Data Flow Management Setup."

2 Run the Discovery Wizard or Select the Job

In Basic Mode, you can view error messages for a default job. In Advanced Mode, you can view error messages for one job, one module, or all modules. For details on running a wizard in Basic Mode, see "How to Use Discovery Control Panel – Basic Mode Workflow" on page 330. For details on running a job, see "How to Use Discovery Control Panel – Advanced Mode Workflow" on page 331.

3 Locate the Problem CI

Use the Discovery Status pane to drill down to the error messages. For details, see "Discovery Status Pane" on page 372.

Example of an error message:

```
<< Progress message, Severity: Fatal>>
Probe DefaultProbe is missing at least one of the discovery pattern's required protocols for job:
DB2 Connection by SQL
```
```
                                                              OK
```
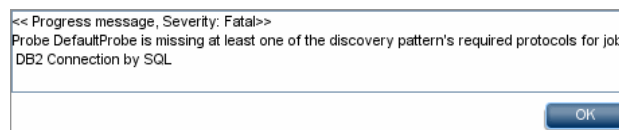
Reference

🔍 Operation Commands

For details on viewing job information, see "How to View Job Information on the RTSM Data Flow Probe" on page 336.

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 349.

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

viewJobExecHistory

Enter the name of a job to retrieve a history of job invocations. A message 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 349.

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 time ranges are shown.

viewJobProblems

Enter the name of a job or the name of a Trigger CI to retrieve a list of Trigger CIs that have problems.

Note: You must fill in at least one of the fields.

For details on the job operation parameters, see "Job Operation Parameters" on page 349.

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 349.

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 *RTSM Developer Reference Guide*. For details on the ObjectStateHolder method, refer to 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 349.

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

Column	Description
Job Name	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.
CI Type	Filters the list to show results for one CIT only.
Total CIs	Goes to the **viewJobResultCiInstances** page, to view a list of all CIs that have been discovered by a job.

Column	Description
Triggered CIs	Goes 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:
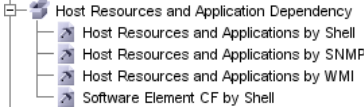
Column	Description
Job Name	Displayed if the **jobID** field is left empty. The job name as it appears in Data Flow Management. Click a job to go to its **viewJobStatus** page, to view its status and scheduling information.
CI Type	Filters the list to show results for one CIT only.
Touched CIs	Goes to 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 349.
Non Touched CIs	Goes 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	Goes 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	Goes 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.

343

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 349.

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, for example: 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. **Blocked.** Not in use. **Removed.** The job is no longer active. **Running.** The job is currently running. **Scheduled.** The job is scheduled to run. For details on scheduling jobs, see "Discovery Scheduler Dialog Box" on page 388. 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.
Errors	The number of errors for a specific job. Goes to the **viewJobErrorsSummary** page, to view a list of error messages reported on this job.
Triggered CIs	The Trigger CIs that have been run by the job. Goes to the **viewJobTriggeredCIs** page.
Last Invocation	The date and time that the job was last run.

Column	Description
Next Invocation	The date and time that the job is next scheduled to run.
Last Total run duration (seconds)	The total time that it took for the job to run in the last invocation. Compare this result with the average time taken for a job to run. The discrepancy is probably due to periods of time when a job waits for another job to finish.
Avg run duration (seconds)	The average time that the job ran, calculated from all previous invocations.
Recurrence	The number of times that the job was invoked. Goes to the **viewJobExecHistory** page, to retrieve a history of job invocations.
Results	The number of CITs that have been discovered by the job. Goes to the **viewJobResults** page to view the CITs.

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 349.

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.

Column	Description
Progress	A summary of the current run, 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	**Thread Name.** The thread that is now running this job. Goes to the **viewJobThreadDump** page. You use this page when a thread is running for a long time, and you must verify that this is because the thread is working hard, and not because there is a problem.
	Curr Dest. ID. The name of the node on which the job is running.
	Curr Dest. IP. The IP for which the job is discovering information.
	Work Time (Sec). The length of time that this thread is running.
	Communication Log. Goes 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 201.

Column	Description
Discovery Jobs Information table	**Status.** The severity of the job's status, as calculated by the Probe. For details, see "Status" on page 344.
	Errors. Goes to **viewJobErrorsSummary** page, to view a list of error messages reported on this job.
	Triggered CIs. Goes to **viewJobTriggeredCIs** page, to view a list of Trigger CIs that are part of a 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). For details, see "Last Total run duration (seconds)" on page 345.
	Avg run duration (seconds). For details, see "Avg run duration (seconds)" on page 345.
	Recurrence. The number of times that the job was invoked. Goes to **viewJobExecHistory** page, to view a history of job invocations.
Results	The number of CITs that have been discovered by the job. Goes to the **viewJobResults** page to view the CITs.

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 page 349.

The results page displays the following information:

Column	Description
No.	The number of the job in the list.
Triggered CI ID	The CI instances that have been discovered by the job. Goes to the **viewJobResults** page to view information about their CITs.
Last Execution	The date and time that the job was last run.
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, 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

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 *RTSM 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	○ True ⦿ False	⦿ True ○ False	○ True ⦿ False
(boolean)includeNonTouchedCis	⦿ True ○ False	⦿ True ○ False	○ True ⦿ 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 Resources and Applications by SNMP**:
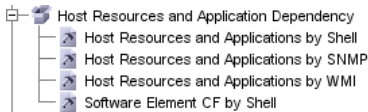
➤ **maxRows**. The maximum number of rows that should be displayed in the results table. The default is 100 or 1000.

➤ **maxTriggeredCIs**. See **maxRows**.

➤ **objectID**. The RTSM object ID.

➤ **showRemovedJobs**. Shows information about jobs that are not currently scheduled to run, but that have run previously. These jobs take the state of **REMOVED**.

➤ **showResults**. Indicates whether to display the **Show Results** column. If the Show Results column is present, you can navigate from **viewJobsStatuses** to **viewJobResults**.

➤ **triggerCI**. The RTSM object ID of the trigger for a job.

➤ **triggeredCiID**. See **triggerCI**.

🔍 Discovery Control Panel User Interface

This section describes:

Advanced Mode Window

Enables you to view and manage modules and jobs, to activate jobs, and to follow job progress.

To access	**Admin** > **RTSM Administration** > **Data Flow Management** > **Discovery Control Panel**
Important information	Each change you make in Discovery Control Panel is delivered to and stored in the RTSM. 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: processing document domainScopeDocument.bin Processing document domainScopeDocument.bin is done. **Note**: Basic Mode is displayed by default when accessing Discovery Control Panel.
Relevant tasks	"How to Use Discovery Control Panel – Advanced Mode Workflow" on page 331

User interface elements are described below:

UI Element (A–Z)	Description
Dependency Map	Displays a visual representation of the real-time progress of the process. For details, see "Dependency Map Tab" on page 368.
Details tab	Enables you to manage a module's CIs and view CI statistics. For details, see "Discovery Control Panel - Details Tab" on page 370.

UI Element (A–Z)	Description
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 Pane" on page 383.
Properties tab	Enables you to view and administer the properties of modules and jobs. For details, see "Properties Tab" on page 413.

Add New Port Dialog Box

Enables you to add new ports through which to connect for specific discoveries.

To access	**Data Flow Management** > **Discovery Control Panel** > **Basic Mode tab** > **Discovery Wizard's Port Scanning page**
Relevant tasks	➤ "Database Discovery Wizard" on page 360 ➤ "J2EE Discovery Wizard" on page 401

User interface elements are described below:

UI Element (A–Z)	Description
	Add port. Enables you to add a port to the list of available ports.
	Edit Port. Enables you to change the number of a port selected in the list.
	Remove Port. Enables you to remove a port selected in the list.

🔍 Basic Mode Window

Enables you to use a Discovery wizard to discover infrastructure, databases, and J2EE applications.

To access	**Admin** > **RTSM Administration** > **Data Flow Management** > **Discovery Control Panel**

Important information	Basic mode includes the following panes:
	
	➤ **List of wizards**. Enables you to choose the wizard to run. For details, see "Infrastructure Discovery Wizard" on page 393, "Database Discovery Wizard" on page 360, or "J2EE Discovery Wizard" on page 401.
	
	➤ **Summary pane**. Enables you to run the wizard and to stop DFM running. For details, see "Summary Pane" on page 355.
	
	➤ **Discovery Overview pane**. Enables you to:
	   ➤ View a brief run status and to drill down to problematic Trigger CIs. For details, see "Discovery Status Pane" on page 372.
	   ➤ View statistics results. For details, see "Statistics Results Pane" on page 378.
	   This pane is displayed once discovery has been run for a component.
	
	Note: Basic Mode is displayed by default when accessing Discovery Control Panel.
	
	For details on Advanced Mode, see "Advanced Mode Window" on page 352..

Relevant tasks	"How to Use Discovery Control Panel – Basic Mode Workflow" on page 330
See also	"Discovery Control Panel Overview" on page 324

User interface elements are described below:

UI Element (A-Z)	Description
	Refreshes the list of wizards.
Advanced Mode tab	Runs DFM when you need to customize a run by making changes to a job, adapter, and so on. For details, see "Advanced Mode Window" on page 352.
Basic Mode tab	(Currently displayed) Runs DFM for a specific component (for example, the infrastructure, J2EE applications, or databases), using configurable, default preferences.

Summary Pane

Enables you to run a Discovery wizard.

To access	**Admin** > **RTSM Administration** > **Data Flow Management** > **Discovery Control Panel**
Important information	Depending on whether a wizard has already run, the Summary pane displays the following information: ➤ If a wizard has not yet run, the Summary pane displays the steps to be performed in the wizard and the **Configure and Run** button. ➤ If a wizard has run, the Summary pane displays a summary of the run parameters, the **Configure** and **Stop Discovery** buttons, and the results of the previous run in the Discovery Progress pane. To run a discovery, select a wizard in the left pane and click **Configure** or **Configure and Run** to open the Discovery wizard. To stop a discovery run, click **Stop Discovery**.
Relevant tasks	"How to Use Discovery Control Panel – Basic Mode Workflow" on page 330

🔍 Choose CIs to Add Dialog Box

Enables you to choose CIs to run with selected jobs.

To access	➤ **Admin** > **RTSM Administration** > **Data Flow Management** > **Discovery Control Panel**. In the Details tab, locate the **Discovery Status** pane. Click the **Add CI** button.
	➤ In the Oracle TNSName File Location page of the Database Discovery wizard, click the **Add CI** button.

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

UI Element (A–Z)	Description
<Column title>	Click a column title to change the order of the CITs from ascending to descending order, or vice versa.
<right-click a title>	Choose from the following options: ➤ **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 Select 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 *RTSM Modeling Guide*.
Add button	**Note:** If you choose CIs with an error status to add to the trigger list, a message is displayed when you click the **Add** button.

UI Element (A–Z)	Description
Search CIs	Contains filters with which you can limit the number of CIs that appear in the Search Results pane. ➤ **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.** Displays the search results.
Search Results	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. ➤ **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 is added to the Discovery Status table. **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**. 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.

✏️ Choose Discovery Query Dialog Box

Enables you to add a Trigger query to a job.

To access	Click the **Add Query** button in the Trigger Queries pane.

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

UI Element (A–Z)	Description
<Discovery query name>	The query that queries the RTSM for the selected CIT.
Query Preview	Hold the cursor over an element to view details.

✏️ Choose Probe Dialog Box

Enables you to filter the Probe list.

To access	Click a **Filter** button in the **Discovery Control Panel** > **Details** tab:
	➤ **Triggered CIs** pane **Filter** button. For details on the menu options, see "Discovery Status Pane" on page 372.
	➤ **Statistics** pane Filter button. For details on the menu options, see "Statistics Results Pane" on page 378.

✏️ Configuration Item Properties Dialog Box

Enables you to view CI properties.

To access	In the **Discovered CIs** dialog box, right-click a CI and choose **Properties**.
Important information	For details, see "Configuration Item Properties Dialog Box" in the *RTSM Modeling Guide*.
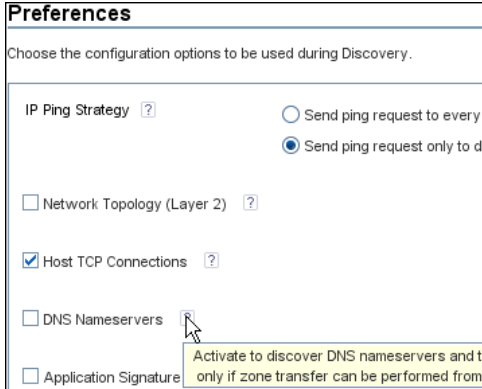
🔍 Create New Discovery Job Window

Enables you to create a job.

To access	Right-click a module in the Discovery Modules pane, and choose **Create new** > **Job**.
Important information	➤ Job names must be limited to a length of 50 characters. ➤ Job names must not start with a numeric value.
See also	For details on the panes in this window, see: ➤ "Discovery Job Details Pane" on page 371 ➤ "Parameters Pane" on page 417 ➤ "Trigger Queries Pane" on page 418 ➤ "Global Configuration Files Pane" on page 197 ➤ "Discovery Scheduler Pane" on page 414

🔍 Database Discovery Wizard

Enables you to discover databases such as DB2, Oracle, Microsoft SQL, and Sybase.

To access	**Admin** > **RTSM Administration** > **Data Flow Management** > **Discovery Control Panel** > **Basic Mode**. Select the Database Discovery wizard from the list in the left pane. Click **Configure and Run**.

Important information	For more information, hold the pointer over a question mark icon:
	
	Preferences
	Choose the configuration options to be used during Discovery.
	
	IP Ping Strategy [?] ○ Send ping request to every
	                                    ● Send ping request only to d
	
	☐ Network Topology (Layer 2) [?]
	
	☑ Host TCP Connections [?]
	
	☐ DNS Nameservers [?]
	              Activate to discover DNS nameservers and t
	☐ Application Signature only if zone transfer can be performed from

Wizard map	The Database Discovery wizard contains: **Database Discovery Wizard** > Define Credentials > Database Port Scanning > Custom JDBC Drivers > Oracle TNSName File Location > Schedule Discovery > Summary

Define Credentials

Enables you to configure connection data for each protocol.

Important information	➤ You configure protocols depending on what must be discovered and which protocols are supported on your site's network.
	➤ For a list of protocols, see "Domain Credential References" on page 103.
	➤ General information about the wizard is available in "Database Discovery Wizard" on page 360.
Wizard Map	The Database Discovery wizard contains:
	Database Discovery Wizard > **Define Credentials** > Database Port Scanning > Custom JDBC Drivers > Oracle TNSName File Location > Schedule Discovery > Summary

User interface elements are described below:

UI Element (A–Z)	Description
➕	Add new connection details for selected protocol type.
✖	Remove a protocol.
✏	Edit a protocol. Opens the Protocol Parameters dialog box.

UI Element (A–Z)	Description
⬆ ⬇	Move a protocol up or down. Data Flow Management executes all the protocols in the list with the first protocol taking priority.
Protocol	Displays details on the protocol, including user credentials. **Note**: A missing credential is represented by an icon ⧉, as shown in the following image:

Database Port Scanning

Enables you to discover the port itself and subsequently to discover the database.

Important information	General information about the wizard is available in "Database Discovery Wizard" on page 360.
Wizard Map	The Database Discovery wizard contains: Database Discovery Wizard > Define Credentials > **Database Port Scanning** > Custom JDBC Drivers > Oracle TNSName File Location > Schedule Discovery > Summary

User interface elements are described below:

UI Element (A–Z)	Description
➕	**Add port.** Opens the Add New Port dialog box, enabling you to select ports to be scanned. For details, see "Add New Port Dialog Box" on page 353.
✏️	**Edit Port.** Opens Edit Port dialog box, enabling you to change the number of a port selected to be scanned.
✖️	**Remove Port.** Enables you to remove a selected port from the list.

🔍 Custom JDBC Drivers

Enables you to select the JAR file for the DB2 and Sybase JDBC drivers.

Important information	General information about the wizard is available in "Database Discovery Wizard" on page 360.
Wizard Map	The Database Discovery wizard contains:
	Database Discovery Wizard > Define Credentials > Database Port Scanning > **Custom JDBC Drivers** > Oracle TNSName File Location > Schedule Discovery > Summary

User interface elements are described below:

UI Element (A–Z)	Description
DB2 JDBC Driver version 8.x	Select the check box and click **Import file...** to locate the appropriate JAR file in the DB2 JDBC installation, as follows: ➤ db2java.zip ➤ db2jcc.jar
DB2 JDBC Driver version 9.x	Select the check box and click **Import file...** to locate the appropriate JAR file in the DB2 JDBC installation, as follows: ➤ db2java.zip ➤ db2jcc.jar ➤ db2jcc_license_cu.jar ➤ db2jcc_license_cisuz.jar
Sybase JDBC Driver	Select the check box and click **Import file...** to locate the **3pclasses.jar** JAR file in the Sybase JDBC installation.

🔍 Oracle TNSName File Location

Enables the discovery of Oracle databases. You provide the location of the TNSNames.ora configuration file that contains database information needed to discover Oracle databases, such as port, node, SID, and so on.

Important information	General information about the wizard is available in "Database Discovery Wizard" on page 360.
Wizard Map	The Database Discovery wizard contains: Database Discovery Wizard > Define Credentials > Database Port Scanning > Custom JDBC Drivers > **Oracle TNSName File Location** > Schedule Discovery > Summary

User interface elements are described below:

UI Element (A–Z)	Description
Server host	Select the hosts on which the TNSNames.ora file is located. Click the **Add CI** button to choose the Trigger CIs that represent these hosts. For details, see "Choose CIs to Add Dialog Box" on page 356.
TNSNames.ora file location	Enter the location of the TNSNames.ora file in the server host system. You can enter several locations (separate the locations by commas). If you terminate the path with a delimiter (for example, **c:\temp**), DFM assumes that the file name is **tnsnames.ora**.

🔍 Schedule Discovery

Enables you to define a schedule for a specific job.

Important information	General information about the wizard is available in "Database Discovery Wizard" on page 360.
Wizard Map	The Database Discovery wizard contains:
	Database Discovery Wizard > Define Credentials > Database Port Scanning > Custom JDBC Drivers > Oracle TNSName File Location > **Schedule Discovery** > Summary

User interface elements are described below:

UI Element (A–Z)	Description
🕐	Opens the Time Templates dialog box, enabling you to define a daily or weekly schedule to run selected jobs. For details, see "Time Templates Dialog Box" on page 421.
Allow Discovery to run at	Choose the time at which the job should run.
Repeat Every	Select how often the job should run.
	Note: To schedule a job to run only once, you must use the Discovery Scheduler in Advanced mode. For details, see "Discovery Scheduler Dialog Box" on page 388.

🔍 Summary

Enables you to review the wizard definitions before running a discovery.

Important information	To make changes to the run, click the **Back** button.
	General information about the wizard is available in "Database Discovery Wizard" on page 360.
Wizard Map	The Database Discovery wizard contains:
	Database Discovery Wizard > Define Credentials > Database Port Scanning > Custom JDBC Drivers > Oracle TNSName File Location > Schedule Discovery > **Summary**

User interface elements are described below:

UI Element (A–Z)	Description
Run	Click the button to run a discovery.

🔍 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

➤ CIs that were discovered as a result of the activated job.

To access	Click the **Dependency Map** tab in the **Discovery Control Panel** window.
Important information	Depending which level you select in the Discovery Modules pane, different information is displayed in the Dependency Map tab. If you select: ➤ **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 DFM 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.
See also	"Discovered by Window" on page 382

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

UI Element (A-Z)	Description
<right-click menu>	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.
	Depending on which object is selected, the following menu options are displayed:
	➤ When a job is selected:
	Show discovered CIs. Displays the CIs discovered by the job. To filter the query, select a CIT from the menu.
	Show trigger CIs. Displays the CIs that triggered the job.
	➤ When a CI is selected:
	Show all CIT instances. Displays all CIs of this CI type.
	➤ When a link from a CI to a job is selected:
	Show trigger CIs for job. Displays CIs (of the selected type) that triggered the job.
	➤ When a link from a job to a CI is selected:
	Show discovered instances. Displays CIs (of the selected type) that were discovered by the job.
<Toolbar>	For details, see "Toolbar Options" in the *RTSM Modeling Guide*.
<Tooltip>	Hold the pointer over a CI or job to display a description.
Show only active Discovery jobs	When the Discovery Modules root is selected in the Discovery Modules pane, this check box is displayed.
	Select to display all active jobs (from any module).

🔍 Discovery Control Panel - 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	Click the **Details** tab in **Discovery Control Panel**.
Important information	Depending which level you select in the Discovery Modules pane, different information is displayed in the Details tab.
	If you select:
	➤ **The Discovery Modules root** or a **Discovery module**, the Discovery Status and Statistics Results panes are displayed with information and statistics about all active jobs and errors discovered during a run. For details, see "Discovery Status Pane" on page 372 and "Statistics Results Pane" on page 378.
	➤ **A job**, the Discovery Job Details, Discovery Status, and Statistics Results panes are displayed. For details, see "Discovery Job Details Pane" on page 371, "Discovery Status Pane" on page 372, and "Statistics Results Pane" on page 378.
	➤ Several jobs or modules, the Selected Items pane is displayed. For details, see "Selected Items Pane" on page 377.

Discovery Job Details Pane

User interface elements are described below:

UI Element (A–Z)	Description
![Content Help button]	Opens the Help document related to the selected job's adapter.
	To update or modify this document, see "Adapter Definition Tab" on page 191.
	To see the full *HP Universal CMDB Discovery and Integration Content Guide* PDF, select **Help > Discovery and Integrations Content Help**.
![Edit Adapter button]	Goes to the adapter in the Resources pane.
![View CIs in Map button]	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.
![View Permissions button]	Displays permissions that are defined for specific adapters. For details, see "Discovery Permissions Window" on page 386.
	For details on editing these permissions, see "Permission Editor Dialog Box" on page 223.
Adapter	The adapter needed 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.
Job Name	The name and description of the job.
	Important: Job names must not start with a numeric value.
Required Protocols	The protocols needed by the activated job to access the system components.

Discovery Status Pane

Enables you to view a run status and to drill down to problematic Trigger CIs, to uncover specific problems that DFM encountered during the run, for example, incorrect credentials. You can also add newly-discovered CIs to the Trigger CI list.

To access	➤ In Basic Mode, locate the Discovery Overview pane.
	➤ In Advanced Mode, select a module or job, click the **Details** tab, and locate the Discovery Status pane.
Important information	➤ In **Basic Mode**, this pane enables you to view the results of the previous run for the selected job type (infrastructure, database, or J2EE application).
	➤ In **Advanced Mod**e, this pane enables you to view the results of the previous run for a selected module or job, or for all modules.
	➤ You can use the SHIFT and CTRL keys to select adjacent and non-adjacent CIs in a list.
	➤ Depending which level you select in Advanced Mode in the Discovery Modules pane, information is displayed in the Discovery Status pane for all modules, for a specific module, or for a specific job.
	➤ The information in this pane is automatically refreshed every thirty seconds.
Relevant tasks	"How to Check Status of Application Discovery (Rediscover a View)" in the *RTSM Modeling Guide*.

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

UI Element (A-Z)	Description
	Returns to the upper pane.
	Drills down to the Trigger CI that includes the problem. **Note**: This icon is displayed only when you can drill down from error or warning links.

UI Element (A-Z)	Description
⟳	Refreshes the status view.
➕	Adds a newly-discovered CI to the Trigger CI list. For details, see "Choose CIs to Add Dialog Box" on page 356.
✖	Removes a CI from the list, if the CI is no longer of interest. The CI is deleted from the specific job.

▽	Click and choose an option from the menu:
	
	➤ **By Status.** (This option is available only when the Total number of CIs is displayed.) Displays a list of Trigger CIs:
	   ➤ **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. Opens the Choose Probe dialog box.
	➤ **By Dispatch Type.** Displays a list of CIs according to one of the following options:
	   ➤ **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.** Removes any filters.

👓	Displays a message box containing an explanation of the failure. (You can also view messages by right-clicking the CI and selecting **Show error details**.)

UI Element (A-Z)	Description
	Opens the Triggered CIs dialog box with additional information about the CI. For details, see "Discovered CIs Window" on page 382.
	➤ **Show results for triggered CI.** DFM sends an ad-hoc request to the Probe and retrieves the latest results of the job (CIT name and number of discovered CIs) that is running on a specific Trigger CI.
	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 420.
	If no communication log exists in the Probe, a message is displayed. You can choose that DFM always creates communication logs. For details, see "Execution Options Pane" on page 201.
	Reruns the discovery.
	Find a CI.
<drill down>	You can drill down from a job or a module.
	➤ Drill down from a job to view a list of Trigger CIs that are included in the job.
	➤ Drill down from a module to view a list of the jobs in the module and the number of CIs returned by each job. Drill down from a job to its Trigger CIs.
	Note: A Trigger CI can be present in more than one job.

UI Element (A-Z)	Description

\<right-click CI menu\>	➤ **Show error details.** Displays a list of the different types of errors returned by this CI. For details, see "Error Severity Levels" in the *RTSM Developer Reference Guide*.
	
	➤ **Remove CI.** Select to delete the CI from the job. The CI is removed from that job only, even if it appears in more than one job.
	
	➤ **Rerun Discovery.** To run a specific CI or set of CIs, select the CIs. They are added to the list of CIs that the Probe is going to run (**Waiting for Probe**).
	
	➤ **Show results for triggered CI.** DFM sends an ad-hoc request to the Probe and retrieves the latest results of the job (CIT name and number of discovered CIs) that is running on a specific Trigger CI.
	
	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 420.
	
	If no communication log exists in the Probe, a message is displayed. You can choose that DFM always creates communication logs. For details, see "Execution Options Pane" on page 201.
	
	➤ **Debug.** Choose between:
	
	  ➤ **View communication log for triggered CI.** 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 201.
	
	  ➤ **Go to adapter.** Displays the adapter that is included in the job in Adapter Management.
	
	  ➤ **Go to job.** Displays the job in which the CI is included.
	
	  ➤ **Edit script**. Select a script to open it in a script editor.
	
	➤ **Undispatch.** Removes the Trigger CI.

UI Element (A-Z)	Description
Failed	Displays those CIs that returned a severity of type Error or Fatal. Right-click a job to rerun discovery. Double-click a job to display the error message. Right-click an error to deactivate or rerun a job.
In progress	Displays the number of Trigger CIs that are awaiting their turn to be run. Displays the jobs that are waiting to be run.
Look for	To search for a specific Probe, related host, or related IP, enter part of its name in the box and click **Search**.
Progress	The indicator shows a summary of the current discovery run, since the specific run was activated.
Success	DFM displays the number of CIs that have been run successfully (without errors). Displays the jobs (and the number of CIs in each job) that completed successfully. Select a CI and use the right-click CI menu to view information. **With warnings.** Displays a warning message for each job. Double-click a message to view the CIs that finished successfully with a warning. Right-click a message to view the right-click CI menu.
Total	Displays the status of all of a job's Trigger CIs. Double click a **Warning** or **Error** status to open the Message dialog box.
Waiting for Probe	The Trigger CIs that are waiting for the Probe or are waiting to run.

Selected Items Pane

User interface elements are described below (unlabeled elements are shown in angle brackets):
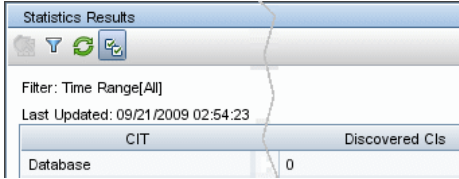
UI Element (A–Z)	Description
<right-click menu>	**Edit Scheduling**. Opens the Discovery Scheduler to define a schedule for a specific job. For details, see "Discovery Scheduler Pane" on page 414.
invoke immediately	➤ A check mark signifies that the DFM job runs as soon as the triggered CI reaches the 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 418.

Statistics Results Pane

Important information	UCMDB includes a purging mechanism for managing old DFM result statistics. This mechanism enables faster display of discovery result statuses. The old statistics records are merged and therefore they are still available for the user. This feature is controlled by two system parameters: ➤ **appilog.collectors.ResetDiscoveryStatisticsIntervalHours. name=Reset Discovery Statistics Interval by Hours**. This property defines the interval of merging discovery statistics (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 results statistics are being archived (the number of days after which the statistics are considered old).
See also	➤ "Data Push Tab" on page 265 ➤ "Population Tab" on page 284

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

UI Element (A–Z)	Description
	Select a CIT and click the **View Instances** button to view CI instances and their attributes. The Discovered CIs dialog box opens.
	A message is displayed when:
	➤ All the CIs that were discovered by this job were already discovered by another job.
	➤ All the CIs that this job discovered have been deleted.
	➤ The CI instances were discovered in a previous version.
	Note:
	➤ You can also view CI instances by double-clicking a row.
	➤ Only instances **created by** the job are shown. If there are no such instances, this button is not available.
	➤ CITs with no instantiated instances are displayed.

UI Element (A–Z)	Description

▽ (filter icon)	Select the time range or Probe for which to display statistics about the CITs.
	
	➤ **By Time Range**:
	   ➤ **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.
	   ➤ **Custom Range.** Opens 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.

⟳ (refresh icon)	Retrieves the latest data from the server (job results are not automatically updated in the Statistics pane).
☑ (icon)	**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: Statistics Results 🏠 ▽ ⟳ ☑ Filter: Time Range[All] Last Updated: 09/21/2009 02:54:23 CIT Discovered CIs Database 0
<Column title>	Click a column title to change the order of the CITs from ascending to descending order, or vice versa.

UI Element (A–Z)	Description
\<right-click a title\>	Choose from the following options: ➤ **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 Select 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 *RTSM Modeling Guide*.
CIT	The name of the discovered CIT.
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.
Filter	The time range set with the Set Time Range button.
Last updated	The date and time that the statistics table was last updated for a particular job.
Total	The total number of CIs in each column.
Updated	The number of CIT instances that were updated in the period selected.

🔍 Discovered by Window

Enables you to view CI instances of a CIT discovered by a job.

To access	➤ In the Statistics Results pane, select a CIT, and click the **View instances** button.
	➤ In the Dependency Map tab, select **Show Discovered CIs** or **Show all instances**.
Important information	➤ The Discovered by <job name> window includes the same information as the Element Instances window. For details, see "Element Instances Dialog Box" in the *HP Universal CMDB Modeling Guide*.
	➤ Depending on whether you select **Show discovered CIs** or **Show all instances** in the Dependency Map, you can view all CIs discovered by a selected job or all CIs of a selected type.
	➤ The CI instances displayed are retrieved from the server upon opening this window. The number of CIs may differ from the number of CIs displayed in the Statistics Results pane because some created CIs may have been merged or deleted since they were created by the job.

🔍 Discovered CIs Window

Enables you to view all CI instances found for a selected TQL node.

To access	➤ **Admin** > **RTSM Administration** > **Data Flow Management** > **Discovery Control Panel** > **Dependency Map** tab. Right-click a CIT and select **Show Triggered CIs**.
	➤ In the Discovery Status pane, click the **Show additional data** button
Important information	The Triggered CIs window includes the same information as the Element Instances window. For details, see "Element Instances Dialog Box" in the *HP Universal CMDB Modeling Guide*.
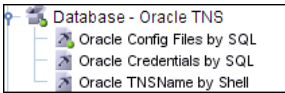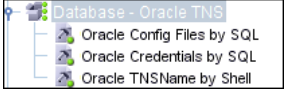
🔍 Discovery Modules Pane

Enables you to view and manage modules and jobs. Each module includes the jobs necessary to discover specific CIs.

To access	Admin > RTSM Administration > Data Flow Management > Discovery Control Panel. The default view is called Basic Mode and displays the Discovery Wizard. You can run the J2EE, database, or infrastructure discovery. Click Advanced Mode to view all modules.
Important information	**Caution:** Only administrators with an expert knowledge of the DFM process should delete modules.
	Obsolete. Contains several modules that are no longer relevant but remain for backward compatibility and upgrade purposes. Do not use these modules on new installations.
	No module. Contains jobs that are not included in any other module.

User interface elements are described below:

UI Element (A–Z)	Description
⟳	**Refresh All.** Updates the modules.
🔍	**Find Job.** Opens 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 392.
⚙	**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**.

UI Element (A–Z)	Description
	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.
	Represents a job. Displays information about the job. To view an adapter description, hold the pointer over a job.
	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" on page 385.
	One green dot signifies that some of a module's jobs are activated:
	Three green dots signify that all of a module's jobs are activated:
	An exclamation mark signifies that one or more of the jobs is experiencing a problem that could affect the DFM process, for example, a protocol connection failure.
	To view the reason for the problem, click the **(show errors)** link in the Discovery Status pane. For details, see "Failed" on page 376.
	Note: If a problem is resolved by clicking the **Refresh All** button, the Problem Indicator disappears.

UI Element (A–Z)	Description
Advanced Mode	(Currently displayed) Runs DFM to customize a run by making changes to a job, adapter, and so on.
Basic Mode	Runs DFM for a specific component (for example, the infrastructure, J2EE applications, or databases), using configurable, default preferences. For details, see "Basic Mode Window" on page 354.

Right-Click Menu

UI Element (A–Z)	Description
Activate	Click a module to run all its jobs. To run a specific job, select and activate it.
	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 Depend, IP, and Member CITs and relationships.
Clear Probe Results Cache	Clears the job's results cache on the probes.
	Note: Selecting to clear the results cache will send all discovery results again on the next execution of this job.
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 191.
	To see the full *HP Universal CMDB Discovery and Integration Content Guide* PDF, select **Help** > **Discovery and Integrations Content Help**.
Create new > Job	Opens the Create New Discovery Job. For details, see "Create New Discovery Job Window" on page 359.
Create new > Module	Defines a new name for the module root.
	Note: Module names must be limited to a length of 50 characters.
Deactivate	Stops the module or job from running.

UI Element (A–Z)	Description
Deactivate all jobs	Click **Discovery Modules** to display this option.
Delete	Click and answer **Yes** to the warning message.
Delete job	Click and answer **Yes** to the warning message.
Go to adapter	Edits the adapter in the Adapter Management window.
Edit Scheduling	Opens the Discovery Scheduler to define a schedule for a specific job.
Rename job	Opens the Choose Name dialog box. Enter a new name for the job. **Note:** You cannot rename active jobs.
Rerun Discovery	Runs the job again using the selected Trigger CIs.
Save as...	Clones the job.

🔍 Discovery Permissions Window

Enables you to view permissions data for jobs.

To access	**Admin** > **RTSM Administration** > **Data Flow Management** > **Discovery Control Panel** > **Advanced Mode**. Select a job. Locate the **Discovery Job Details** pane in the **Details** tab. Click the **View Permissions** button.
See also	➤ "Viewing Permissions While Running Jobs" on page 327 ➤ "Required Permissions Pane" on page 195 ➤ "Permission Editor Dialog Box" on page 223

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 *HP Universal CMDB Modeling Guide*.
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	➤ Right-click a job and choose **Edit scheduling**. ➤ Click the **Edit Scheduler** button in the Discovery Scheduler pane of the Properties tab in the Discovery Control Panel window.
Important information	➤ 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 can also 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. For details on creating a time template, see "Edit Time Template Dialog Box" on page 391.

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

UI Element (A–Z)	Description
Validate Expression	Validates the Cron expression you entered.
<Days of month>	(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. ➤ **Select all**. Select all the days. ➤ **Unselect all**. Clear all the selected days.
<Days of the week>	(Displayed when you select **Weekly.**) Select the day or days on which the action should run.
<Frequency>	➤ **Once.** Define the task to run only once. (Available for Advanced mode only.) ➤ **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>	(Displayed when you select **Monthly.**) Select the month or months in which the action must run.
End by	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**. **Note**: This step is optional. If you do not need to specify an ending date, leave the **End by** check box cleared.

UI Element (A–Z)	Description
Invocation hour	(Displayed 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. ➤ **Select all**. Select all the times. ➤ **Unselect all**. Clear all the selected times. **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.
Invocation Time	(Displayed 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.
Repeat every	(Displayed when you select **Interval**.) Type a value for the interval between successive runs and choose the required unit of time (minutes, hours, or days). **Note**: After each change, the next time that the job runs is the current time plus the interval; the job does not start immediately.
Start at	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**.
Time zone	Select the time zone according to which the Probe must schedule jobs. 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. For all Probes to start working at the same time, select a specific time zone. (This assumes that the Probes' system date and time and time zone are correctly configured.)

❖ Edit Probe Limitation for Query Output Dialog Box

Enables you to change the Probes on which a Trigger query is running. For details on selecting the Probes, see "Selecting Probes" on page 166.

To access	**Admin** > **RTSM Administration** > **Data Flow Management** > **Discovery Control Panel** > <selected job> > **Properties tab** > **Trigger Queries pane** > **Probe Limit** column > [...] .

❖ Edit Time Template Dialog Box

Enables you to define a time template to use when scheduling jobs.

To access	Use one of the following: ➤ Click the **Add** button in the Time Templates dialog box. ➤ In the Time Templates dialog box, select a time template and click 🖉.
Important information	The name of the time template must be unique.
See also	"Discovery Scheduler Dialog Box" on page 388

User interface elements are described below:

UI Element (A–Z)	Description
Every day between	Define a daily schedule when a job must run. You can also type in times. You can assign any hour and minute combination.
Time Template name	Enter a unique name.
Week Time	Define a weekly schedule when a job must run. Select this option to select a time in the Time Definition grid. To select adjacent cells in the grid, click and drag the pointer over the grid. To clear a time, click a cell in the grid a second time.

🔍 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 **Search for Discovery Jobs** button in the Discovery Modules pane.

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	Choose between: ➤ **Name.** Enter the name of the job or part of it. ➤ **Input type.** CIs that triggered 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.** CIs that are discovered as a result of the activated job.
Find Next	The next job meeting the search criteria is highlighted.

🔍 Infrastructure Discovery Wizard

Enables you to run discovery on the networks in your system.

To access	**Admin** > **RTSM Administration** > **Data Flow Management** > **Discovery Control Panel** > **Basic Mode**. Select **Infrastructure Discovery Wizard** from the list in the left pane. Click **Configure and Run**.
Wizard Map	The Infrastructure Discovery wizard contains: **Infrastructure Discovery Wizard** > Define IP Ranges > Define Credentials > Preferences > Schedule Discovery > Summary

🔍 Define IP Ranges

Enables you to set the network range for discovery for each Probe. 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.

Important information	Any changes made here affect the global configuration. General information about the wizard is available in "Infrastructure Discovery Wizard" on page 393.
Wizard Map	The Infrastructure Discovery wizard contains: Infrastructure Discovery Wizard > **Define IP Ranges** > Define Credentials > Preferences > Schedule Discovery > Summary

User interface elements are described below:

UI Element (A–Z)	Description
➕	For details, see "Add/Edit IP Range Dialog Box" on page 149.
✖	Select a range and click the button to remove the range from the list.
🖉	Select a range and click the button to edit an existing range.

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 *HP Universal CMDB Modeling Guide*.
	Imports ranges from a CSV file. Before using this feature, verify that the imported file is a valid CSV file, and that the ranges in the file do not conflict with existing ranges (there are no duplicate or overriding ranges).
Address Ranges	➤ **Range.** For details on the rules for defining ranges, see "Range" on page 151. ➤ **Excluded.** You can exclude part of a range. Select the range and click the **Add** button. In the dialog box, click the Advanced button. For details, see "Exclude Ranges" on page 150.
Data Flow Probes	Enables you to view details on the Probe, including range information. You can also add ranges to, or exclude ranges from, the Probe. For details on defining a Probe, see "Domains and Probes Pane" on page 162.

🔍 Define Credentials

Enables you to add, remove and edit a credentials set for protocols.

Important information	➤ You configure a credentials set depending on what must be discovered and which protocols are supported on your site's network.
	➤ For a list of protocols, see "Domain Credential References" on page 103.
	➤ General information about the wizard is available in "Infrastructure Discovery Wizard" on page 393.
Wizard Map	The Infrastructure Discovery wizard contains:
	Infrastructure Discovery Wizard > Define IP Ranges > **Define Credentials** > Preferences > Schedule Discovery > Summary

User interface elements are described below:

UI Element (A–Z)	Description
🟢➕	Add new connection details for selected protocol type.
	For a list of protocols, see "Domain Credential References" on page 103.
❌	Remove a protocol.
✏️	Edit a protocol. Opens the Protocol Parameters dialog box.
🔼 ⬇️	Click a button to move a protocol up or down to set the order in which credential sets are attempted. Discovery executes all the protocols in the list with the first protocol taking priority.
Protocol	Displays details on the protocol, including user credentials.

🔍 Preferences

Enables you to choose the configuration options to be used during discovery that are activated by the Infrastructure Discovery wizard.

Important information	General information about the wizard is available in "Infrastructure Discovery Wizard" on page 393.
Wizard Map	The Infrastructure Discovery wizard contains: Infrastructure Discovery Wizard > Define IP Ranges > Define Credentials > **Preferences** > Schedule Discovery > Summary

User interface elements are described below:

UI Element (A-Z)	Description
DNS Nameservers	Discovers DNS nameserver machines and the IPs they hold names for. Choose to activate only if zone transfer can be performed from the Probe machine to the nameserver machines — if the appropriate permissions exist on the DNS nameserver machines. **Network implications.** Discovery tries to connect to DNS nameserver servers.
Failover Cluster	Discovers failover clusters including HP Service Guard, Microsoft Cluster Service and Veritas Cluster.

UI Element (A-Z)	Description
Host Information	Select the host resources to be discovered. These resources can be physically or logically part of a host. After Discovery connects to a host, it discovers the following resources: ➤ For SNMP agents, the relevant Management Information Base (MIBs). ➤ For WMI agents, the relevant Windows Management Instrumentation Query Language (WQL) queries. Discovery can also execute shell commands on a machine. **Network implications.** The Software and Services network resources, because of the large quantities of data that they transmit, may cause very high network traffic. For this reason, the default is not to discover them.
Host TCP Connections	Discover TCP communication channels to map dependency relationships between hosts. This discovery requires that at least one protocol has a defined set of credentials. For details, see the previous Define Credentials step. **Network implications.** Discovery executes Shell commands on a machine to find open ports.

UI Element (A-Z)	Description
IP Ping Strategy	Choose the strategy for discovering IPs in your environment. This discovery requires that the SNMP protocol be configured in the previous Define Credentials step. ➤ **Send ping request to every address in defined IP range.** Select this option when you know that most of the IP addresses will respond, the network range is small, and most of the IPs in the range are of interest to you (are part of your network). ➤ **Send ping request only to discoverable IPs in a network.** Select this option when you know that not all IP addresses will respond and the network range is large. In this case, Discovery first discovers a network, then sends a ping request to all discovered IPs in that network. **Versions and Limitations:** Verify that you have the correct credentials set for all the machines between the Probe and one of the network's switches.
Network Topology	Activate to discover the connections, on a discovered switch (for example, a host), between a host and its physical port as well as between a host and its logical layout (VLANs, ELANs). This discovery requires that at least one protocol has a defined set of credentials. For details, see the previous Define Credentials step.

UI Element (A-Z)	Description
Port Scanning	The TCP ports appearing in the **Choose TCP ports for port scanning** list are scanned to discover open server ports. The ports are scanned on every discovered host.
	You can add new ports to be scanned, and you can remove existing ports from the list.
	To choose a port that does not appear in the list: **1** Click the **Add port** button to open the Add New Port dialog box. **2** Click the **Add port** button and enter the port name and number. **3** Click **OK**.
	Network implications.
	Note that the scanning process may affect performance on the network. Furthermore, you may need to inform machine owners that Discovery will be trying to connect to their machines.
Software identification	Select to discover software elements running on the discovered hosts. As part of software element discovery, the processes and ports that are related to the software element are also discovered. The Software Library dialog box opens. For details, see "Software Library Dialog Box" on page 233.
	Network implications.
	A search pattern that is too general causes a toll on performance. For example, do not enter a process name that consists of an asterisk (*****) only, as such a filter would try and retrieve all the processes running on all machines.

🔍 Schedule Discovery

Enables you to define a schedule for a specific job.

Important information	For details on scheduling Discovery, see "Discovery Scheduler Dialog Box" on page 388.
	General information about the wizard is available in "Infrastructure Discovery Wizard" on page 393.
Wizard Map	The Infrastructure Discovery wizard contains:
	Infrastructure Discovery Wizard > Define IP Ranges > Define Credentials > Preferences > **Schedule Discovery** > Summary

User interface elements are described below:

UI Element (A–Z)	Description
🕐	Opens the Time Templates dialog box, enabling you to define a daily or weekly schedule to run selected jobs. For details, see "Time Templates Dialog Box" on page 421.
Allow Discovery to run at	Choose the time at which the job should run.
Repeat Every	Select how often the job should run.
	Note: To schedule a job to run only once, you must use the Discovery Scheduler in Advanced mode. For details, see "Discovery Scheduler Dialog Box" on page 388.

🔖 Summary

Enables you to review the definitions before running discovery.

Important information	Click **Run** to begin Discovery.
	General information about the wizard is available in "Infrastructure Discovery Wizard" on page 393.
Wizard Map	The Infrastructure Discovery wizard contains:
	Infrastructure Discovery Wizard > Define IP Ranges > Define Credentials > Preferences > Schedule Discovery > **Summary**

🔖 J2EE Discovery Wizard

Enables you to run discovery on J2EE applications.

To access	**Admin** > **RTSM Administration** > **Data Flow Management** > **Discovery Control Panel** > **Basic Mode**. Select the J2EE Discovery wizard from the list in the left pane. Click **Configure and Run**.
Important information	For more information, hold the pointer over a question mark icon.
Wizard Map	The J2EE Discovery wizard contains:
	J2EE Discovery Wizard > Define Credentials > J2EE Port Scanning > WebLogic > WebSphere > JBoss > Oracle Application Server > Schedule Discovery > Summary

🔍 Define Credentials

Enables you to configure connection data for each protocol.

Important information	➤ You configure protocols depending on what must be discovered and which protocols are supported on your site's network.
	➤ For a list of protocols, see "Domain Credential References" on page 103.
	➤ General information about the wizard is available in "J2EE Discovery Wizard" on page 401.
Wizard Map	The J2EE Discovery wizard contains:
	J2EE Discovery Wizard > **Define Credentials** > J2EE Port Scanning > WebLogic > WebSphere > JBoss > Oracle Application Server > Schedule Discovery > Summary

User interface elements are described below:

UI Element (A–Z)	Description
➕	Add new connection details for selected protocol type.
✖	Remove a protocol.
✏	Edit a protocol. Opens the Protocol Parameters dialog box.

UI Element (A–Z)	Description
⬆ ⬇	Move a protocol up or down. Discovery executes all the protocols in the list with the first protocol taking priority.
Protocol	Displays details on the protocol, including user credentials. **Note**: A missing credential is represented by an icon ▧⚠, as shown in the following image:

🔍 J2EE Port Scanning

Enables you to choose the port number and port type through which to connect to the J2EE application.

Important information	General information about the wizard is available in "J2EE Discovery Wizard" on page 401.
Wizard Map	The J2EE Discovery wizard contains:
	J2EE Discovery Wizard > Define Credentials > **J2EE Port Scanning** > WebLogic > WebSphere > JBoss > Oracle Application Server > Schedule Discovery > Summary

User interface elements are described below:

UI Element (A–Z)	Description
➕	**Add port.** Opens the Add New Port dialog box, enabling you to select ports to be scanned. For details, see "Add New Port Dialog Box" on page 353.
✏️	**Edit Port.** Opens Edit Port dialog box, enabling you to change the number of a port selected to be scanned.
✖️	**Remove Port.** Enables you to remove a selected port from the list.

🔍 **WebLogic**

Enables you to select the JAR files for specific WebLogic versions.

Important information	Discovery supports the following WebLogic versions: 6.x, 7.x, 8.x, 9.x, and 10.x.
	To discover WebLogic:
	1 Obtain the following drivers:
	➤ **weblogic.jar** (versions 6.x, 7.x, and 8.x only)
	➤ **wlcipher.jar** (if WebLogic is running on SSL, for all versions)
	➤ **license.bea** (if WebLogic is running on SSL but only for versions 6.x, 7.x, and 8.x)
	➤ **client trust store JKS file** (for example, DemoTrust.jks, but only if WebLogic is running on SSL)
	➤ **wlclient.jar** (versions 9.x and 10.x only)
	➤ **wljmxclient.jar** (versions 9.x and 10.x only)
	2 Place the driver under the correct version folder in the following location: **C:\hp\UCMDB\DataFlowProbe\runtime\ probeManager\discoveryResources\j2ee\weblogic\ <version_folder>**. For example, **C:\hp\UCMDB\DataFlowProbe\runtime\ probeManager\discoveryResources\j2ee\weblogic\ 9.x**.
	3 On the WebLogic page in the J2EE Discovery wizard, select the check box for the versions to be discovered. Click **Import file...** to open a browse window. Browse to the appropriate WebLogic JAR file, as listed below.
	General information about the wizard is available in "J2EE Discovery Wizard" on page 401.
Wizard Map	The J2EE Discovery wizard contains:
	J2EE Discovery Wizard > Define Credentials > J2EE Port Scanning > **WebLogic** > WebSphere > JBoss > Oracle Application Server > Schedule Discovery > Summary

User interface elements are described below:

UI Element (A–Z)	Description
Activate using default JAR files (8.x only)	Select to enable discovery without specifying version-specific JAR files. This is less recommended and works on some environments only.
WebLogic version 6.x	➤ weblogic.jar ➤ For an SSL based discovery, select wlcipher.jar, license.bea, and the JKS file (for example, DemoTrust.jks)
WebLogic version 7.x	➤ weblogic.jar ➤ For an SSL based discovery, select wlcipher.jar, license.bea, and the client trust store JKS file (for example, DemoTrust.jks)
WebLogic version 8.x	➤ weblogic.jar ➤ For an SSL based discovery, select wlcipher.jar, license.bea, and the client trust store JKS file (for example, DemoTrust.jks)
WebLogic version 9.x	➤ wlclient.jar ➤ wljmxclient.jar ➤ For an SSL based discovery, select wlcipher.jar and the client trust store JKS file (for example, DemoTrust.jks)
WebLogic version 10.x	➤ wlclient.jar ➤ wljmxclient.jar ➤ For an SSL based discovery, select wlcipher.jar and the client trust store JKS file (for example, DemoTrust.jks)

🔍 WebSphere

Enables you to select the JAR files for specific WebSphere versions.

Important information	Discovery supports the following WebSphere versions: 5.x, 6.0, and 6.1.
	➤ To discover WebSphere, obtain the following certificates:
	➤ **client key store JKS file** (DummyClientKeyFile.jks if WebSphere is running on SSL and the file is required)
	➤ **client trust JKS file** (DummyClientTrustFile.jks if WebSphere is running on SSL)
	Out-of-the-box drivers are located on the Probe machine at the following location: **C:\hp\UCMDB\DataFlowProbe\runtime\ probeManager\discoveryResources\j2ee\websphere**
	➤ Restart the Probe console before running the DFM jobs.
	General information about the wizard is available in "J2EE Discovery Wizard" on page 401.
Wizard Map	The J2EE Discovery wizard contains:
	J2EE Discovery Wizard > Define Credentials > J2EE Port Scanning > WebLogic > **WebSphere** > JBoss > Oracle Application Server > Schedule Discovery > Summary

User interface elements are described below:

UI Element (A–Z)	Description
Activate using default JAR files (5.x, 6.x only)	Select to enable discovery without specifying version-specific JAR files. This is less recommended and works on some environments only.
WebSphere	Select the check box for the versions to be discovered. Click **Import file...** to open a browse window. Browse to the appropriate WebSphere JAR file, as follows: ➤ admin.jar ➤ com.ibm.mq.pcf.jar ➤ ffdc.jar ➤ iwsorb.jar ➤ j2ee.jar ➤ jflt.jar ➤ jmxc.jar ➤ jmxx.jar ➤ log.jar ➤ mail.jar ➤ ras.jar ➤ sas.jar ➤ security.jar ➤ soap.jar ➤ utils.jar ➤ wasjmx.jar ➤ websphere_arm_util.jar ➤ wlmclient.jar ➤ wsexception.jar ➤ wssec.jar

🔍 JBoss

Enables you to select the JAR files for specific JBoss versions.

Important information	Discovery supports the following JBoss versions: 3.x, 4.x.
	General information about the wizard is available in "J2EE Discovery Wizard" on page 401.
Wizard Map	The J2EE Discovery wizard contains:
	J2EE Discovery Wizard > Define Credentials > J2EE Port Scanning > WebLogic > WebSphere > **JBoss** > Oracle Application Server > Schedule Discovery > Summary

User interface elements are described below:

UI Element (A–Z)	Description
Activate using default JAR files (3.x, 4.x only)	Select to enable discovery without specifying version-specific JAR files. This is less recommended and works on some environments only.
JBoss version 3.x and 4.x	Select the check box for the versions to be discovered. Click **Import file...** to open a browse window. Browse to the **jbossall-client.jar** JBoss JAR file.

🔍 **Oracle Application Server**

Enables you to discover Oracle application servers.

Important information	General information about the wizard is available in "J2EE Discovery Wizard" on page 401.
Wizard Map	The J2EE Discovery wizard contains: J2EE Discovery Wizard > Define Credentials > J2EE Port Scanning > WebLogic > WebSphere > JBoss > **Oracle Application Server** > Schedule Discovery > Summary

User interface elements are described below:

UI Element (A-Z)	Description
Discover Oracle Application Server (version 10g)	Select to run Discovery for the Oracle Application Server, version 10g.

🔍 Schedule Discovery

Enables you to define a schedule for a specific job.

Important information	General information about the wizard is available in "J2EE Discovery Wizard" on page 401.
Wizard Map	The J2EE Discovery wizard contains: J2EE Discovery Wizard > Define Credentials > J2EE Port Scanning > WebLogic > WebSphere > JBoss > Oracle Application Server > **Schedule Discovery** > Summary

User interface elements are described below:

UI Element (A–Z)	Description
🕐	Opens the Time Templates dialog box, enabling you to define a daily or weekly schedule to run selected jobs. For details, see "Time Templates Dialog Box" on page 421.
Allow Discovery to run at	Choose the time at which the job should run.
Repeat Every	Select how often the job should run. **Note:** To schedule a job to run only once, you must use the Discovery Scheduler in Advanced mode. For details, see "Discovery Scheduler Dialog Box" on page 388.

🔍 Summary

Enables you to review the definitions before running discovery.

Important information	To make changes to the run, click the **Back** button.
	General information about the wizard is available in "J2EE Discovery Wizard" on page 401.
Wizard Map	The J2EE Discovery wizard contains:
	J2EE Discovery Wizard > Define Credentials > J2EE Port Scanning > WebLogic > WebSphere > JBoss > Oracle Application Server > Schedule Discovery > **Summary**

User interface elements are described below:

UI Element (A–Z)	Description
Run	Runs Discovery.

⚒ Properties Tab

Enables you to view and administer the properties of modules and jobs.

To access	Click the **Properties** tab in Discovery Control Panel.
Important information	Depending which level you select in the Discovery Modules pane, different information is displayed in the Properties tab.
	If you select:
	➤ **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 388.
	➤ **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 page 415.
	➤ **A job**, the Parameters, Trigger Queries, Global Configuration Files, and Discovery Scheduler panes are displayed. For details, see "Parameters Pane" on page 417, "Trigger Queries Pane" on page 418, "Global Configuration Files Pane" on page 197, and "Discovery Scheduler Pane" on page 414.

Discovery Scheduler Pane

Enables you to view information about the schedule set up for this job.

To access	Select a job in the Discovery Modules pane in the Discovery Control Panel window.

User interface elements are described below:

UI Element (A–Z)	Description
	Adds 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 "Edit Time Template Dialog Box" on page 391.
Allow Discovery to run at	Choose a template that includes the days and times when the job should run.
Edit scheduler	Opens the Discovery Scheduler. For details, see "Discovery Scheduler Dialog Box" on page 388.
Invoke on new triggered CIs immediately	Check box selected: The job runs as soon as the Trigger CI reaches the Probe. Check box cleared: the job runs according to the schedule defined in the Schedule Manager.

Global Configuration Files Pane

For details, see "Global Configuration Files Pane" on page 197.

Module Jobs Pane

Enables you to view the active jobs for a specific module.

To access	Select a module in the Discovery Modules pane in the Discovery Control Panel window.

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. (Use the SHIFT or CTRL key 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 results 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 title>	➤ Click a column title to change the order of the CITs from ascending to descending order, or vice versa.
	➤ Drag a column head to a different location in the table columns.
	➤ Right-click a column title to customize the table. Choose from the following options:
	  ➤ **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 *RTSM Modeling Guide*.

UI Element (A–Z)	Description
\<List of jobs\>	All jobs included in the module. (Displayed when a specific module is selected in the 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 388.
Invoke Immediately	➤ 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 Discovery Control Panel 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 MicrosoftSQLServer to the new value. Click **OK** in the Properties tab to save the change: For details on editing parameters in the Adapter Parameters pane, see "Adapter Parameters Pane" on page 198.
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.

To access	➤ Select a job in the Discovery Modules pane in the Discovery Control Panel window.
	➤ Create a job by right-clicking a module in the Discovery Modules pane, and choose **Create New Job**.

User interface elements are described below:

UI Element (A–Z)	Description
![plus icon]	**Add Query.** You can add one or more non-default TQL queries to be used as triggers to activate the selected job. Opens the Choose Discovery Query dialog box.
![remove icon]	**Remove Query.** Select the query and click the button.
	(No message is displayed. To restore the query, click the **Cancel** button.)
	Note: 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.
![dots icon]	Adds or removes Probes for a specific query. For details, see "Edit Probe Limitation for Query Output Dialog Box" on page 391.
![pencil icon]	Opens the Trigger Query Editor. For details, see "Trigger Query Editor Window" on page 422.
Probe Limit	The Probes being used for the discovery process. To add or remove Probes, click the button.
Query Name	The name of the Trigger query that activates the job.

🔍 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.

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 *RTSM Modeling Guide*.
<menu>	For details, see "Toolbar Options" in the *HP Universal CMDB Modeling Guide*.
<Topology Map>	For details, see "Topology Map Overview" in the *HP Universal CMDB Modeling Guide*.

🔭 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	**Discovery Control Panel**, select a module or job, select the **Details** tab. In the **Discovery Status** pane, drill down to a CI, right-click it, and choose **Show Results for Triggered CI**.

User interface elements are described below:

UI Element (A-Z)	Description
🖼️	Displays additional information in the Show Results for Triggered CI dialog box on a selected CIT.
🔍	Opens a topology map showing a result map for the Triggered CI. Right-click a CIT to view its properties.

Source CIs Dialog Box

The Source CIs dialog box includes the same components as the **Discovered CIs** dialog box. For details, see "Discovered by Window" on page 382.

Time Templates Dialog Box

Enables you to define a daily or weekly schedule to run selected jobs.

To access	**Admin** > **RTSM Administration** > **Data Flow Management** > **Discovery Control Panel** > **Properties tab** > **Discovery Scheduler pane** > **Edit Time Template** button

User interface elements are described below:

UI Element (A–Z)	Description
	Adds a time template. Opens the Edit Time Template dialog box.
	Deletes a selected time template.
	Edits a selected time template. Opens the Edit Time Template dialog box.

🐾 Trigger Query Editor Window

Enables you to edit a TQL query that has been defined to trigger jobs.

To access	**Admin** > **RTSM Administration** > **Data Flow Management** > **Discovery Control Panel** > **Properties** tab > **Trigger Queries pane** > select 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. 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.
See also	➤ "Trigger CIs and Trigger Queries" on page 33 ➤ "Input Query Editor Window" on page 217

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

UI Element (A–Z)	Description
<Panes>	➤ CI Type Selector Pane ➤ Editing Pane ➤ Information Pane
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 *HP 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 *HP Universal CMDB Modeling Guide*.
Relevant tasks	➤ "How to Define a TQL Query" in the *HP Universal CMDB Modeling Guide* ➤ "How to Create a Pattern View" in the *HP Universal CMDB Modeling Guide*

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):
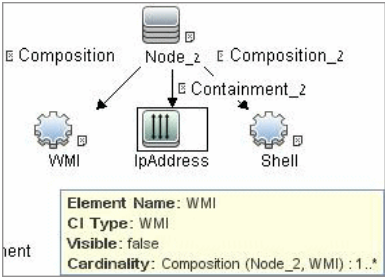
UI Element (A–Z)	Description
<node>	Displays information about the node in the information pane.
<right-click menu>	For details, see "Shortcut Menu Options" in the *HP Universal CMDB Modeling Guide*..
<Toolbar>	For details, see "Toolbar Options" in the *HP Universal CMDB Modeling Guide* .

Information Pane

Displays the properties, conditions, and cardinality for the selected node and relationship.

Important information	Hold the pointer over a node to view information: A small green indicator is displayed next to the tabs that include information:

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 *HP Universal CMDB Modeling Guide*.
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 *HP Universal CMDB Modeling Guide*.
Details	➤ **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 ⬚ is displayed to the right of the selected node/relationship in the Editing pane: ➤ **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 *HP Universal CMDB Modeling Guide*.
Qualifiers	Displays the qualifier conditions defined for the node or the relationship. For details, see "Qualifier Tab" in the *HP Universal CMDB Modeling Guide*.

UI Element (A-Z)	Description
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 *HP Universal CMDB Modeling Guide*.

Part V

Reconciliation

12

Reconciliation

This chapter includes:

Concepts

Tasks

Reference

Concepts

🔷 Reconciliation Overview

Reconciliation is the process of identifying and matching entities from different data repositories (for example, RTSM Discovery, DDMI, ticketing, or BSM). This process is designed to avoid duplicate CIs in RTSM.

Many different data collectors can send CIs to RTSM. In actuality, each different source might be providing information about the same CI. The reconciliation engine is responsible for identifying and matching entities from different data collectors and storing them, without duplicating CIs, in RTSM.

Three main services provide support for the reconciliation engine:

➤ **Data Identification**. Responsible for comparing input CIs, according to reconciliation rules. For details, see "Identification Service" on page 437.

➤ **Data In**. Responsible for inserting data into RTSM. This service decides:

   ➤ whether to merge data into existing CIs in RTSM

   ➤ whether to ignore input CIs in the case of multiple matches

   For details, see "Data In Service" on page 439.

➤ **Merge**. Responsible for merging CIs (used in Federation and Data In flows). Merging is done according to the reconciliation priority definitions. For details, see "Reconciliation Priority" on page 455.

These services operate during reconciliation for inserting data from different sources into RTSM, and during federation for connecting or merging information from different data repositories during TQL query calculations.

The reconciliation engine contains out-of-the-box identification and match criteria rules for most usable and problematic CITs, such as node, running software, and so on.

Stable ID

RTSM now generates stable IDs during CI creation. This means that the ID of the CI is no longer calculated from the CI's properties. This stable ID therefore remains the same when the name, attribute name, or property values (during normalization) change.

Identification Configuration

The reconciliation engine uses XML configuration files that contain identification and match criteria to determine how CIs are identified during federation or data insertion. Configuration files for out-of-the-box CI types are provided when packages are deployed, but you can modify the provided files or create additional files. For details, see "How to Create an Identification Rule Document" on page 443.

The following rules are used during reconciliation:

1 Identification criteria – a set of criteria that defines all possible conditions to find all candidate CIs for matching to a newly introduced CI.

2 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 step 1 (identification). Match verification ends successfully only when all applied verification criteria are true or NA (missing data).

➤ Match validation criteria – an ordered set of criteria that are 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

– NA (missing data) causes reconciliation to proceed to the next criterion. If all validation criterion are NA, then the all candidates left after match verification will be implied as matched.

Identification and Match Criteria Configuration

Due to the discovery method (local or remote), the available credentials (for example, remote access to SNMP or WMI), and specific system security settings (for example, the system responds to a ping), 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.

However, 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)

These node identification criteria show all possible node attributes that can be used for node matching. For example, if there are two nodes with the same HW ID or the same IP address, these nodes are candidates for matching.

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):

   ➤ HW ID with an **equals** operator

   ➤ Network interface with a **contains** operator

   ➤ Node name with an **equals** 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>
```

Reconciliation Services

This section includes:

Identification Service

The Identification service uses identification rules to identify CIs. An identification rule is composed of three criterion sets:

➤ Identification criteria – for two CIs to be the same, one of these criteria must be satisfied.

➤ Match verification criteria – for two CIs to be the same, all the criteria must be satisfied, or there is not enough information to evaluate all of the criteria.

➤ Match validation criteria – for two CIs to be the same, one validation criterion must be satisfied, or there is not enough information to evaluate all of the criteria.

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 above sections, contains one or more conditions. There are two types of conditions:

➤ Attribute conditions – tests whether or not two CIs have the same value (or same value while ignoring case) of the given attribute define for the condition.

➤ Connected CI conditions – tests whether or not the two CIs share the given amount 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 therefore the entire criterion that contains it, returns as unknown.

The identification process is as follows:

1 Must have at least one identification criteria that returns true. If there is at least one identification criteria that returns true, we continue to the next step. Otherwise the two CIs are not the same.

2 Are there contradictions between the CIs? If there is no verification criteria that returns false (all of the verification data returns either true or unknown), continue to the next step. Otherwise, there is a contradiction between the two CIs, and they are not the same.

3 Evaluate the validation criteria one by one and according to their priority:

   a When a validation criterion is satisfied, mark the two CIs as the same.

   b If none of the validation criteria is satisfied, and a validation criterion returns false, the two CIs are unmatched.

   c If none of the validation criteria is satisfied or refuted, evaluate the criteria from the next priority.

   d 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   name = n1, ip_address = ip1, MAC address = m1, os_family = nt

RTSM nodes   ➤ N1 = name=n2

                    ➤ N2 = ip_address=ip1,ip2, MAC address=m1, os_family=nt

                    ➤ N3 = name=n3, MAC address = m1, hw_id = id1, os_family = unix)

1 For each RTSM 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.

Data In Service

After the Identification service runs, the identified data is merged and inserted into the RTSM by the Data In service.

One of the major problems that the Data In service solves is deciding what to do if the input CI matches multiple RTSM CIs. You can:

➤ merge all matched CIs into one

➤ ignore the input CI

The Data In service uses match criteria to make the decision. The process is as follows:

1 Merge the input CI with each matching RTSM CI.

2 For each pair of CIs resulting from step 1, run match criteria (verification and validation criteria).

If at least one pair does not pass the match criteria check, the CIs are not merged. If all pairs pass the match criteria check, the CIs are merged.

3 If the CIs are not merged, the Data In service decides to ignore the input CI. This occurs when the current match criterion causes a pair to fail the match criteria checking, and as a result the service does not merge the CIs.

Multiple Matching Examples

➤ Multiple matching by different identification criteria without conflicts

   ➤ Input bulk data
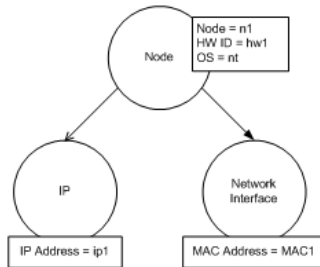
   ➤ Identified data in the RTSM
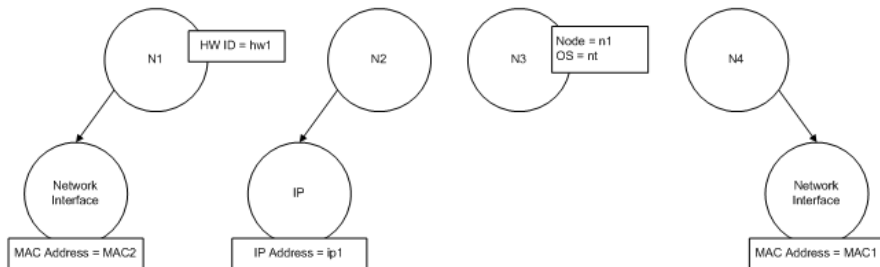
In this example, the input node matches four nodes in the RTSM having different identification criteria, and there are no conflicts with any of the RTSM matched nodes. The process is as follows:

➤ Merge the input CI with each matched CI in the RTSM.
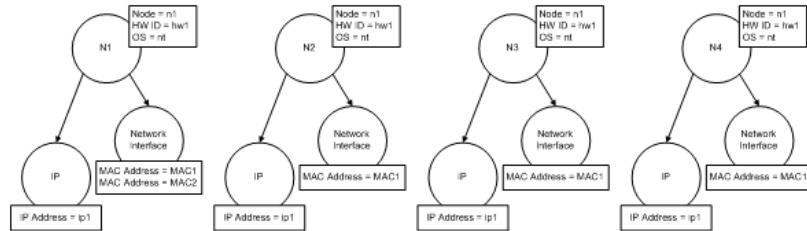
➤ Check for conflicts between the resulting merged CIs. In this example, there is no conflict between the merged CIs. Nodes N2, N3, and N4 are the same CI; therefore, it is obvious that there is no conflict between them. The only difference between nodes N1 and N2 is the additional MAC address in N1. Since the MAC address match validation criterion uses the **contains** operator, there is no conflict between nodes N1 and N2 either.

The decision here is to merge all CIs into one.

➤ Multiple matching by different identification criteria with conflicts

➤ Input bulk data
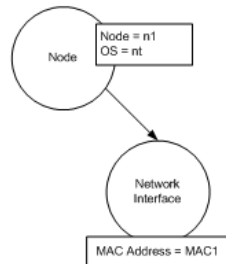
➤ Identified data in the RTSM
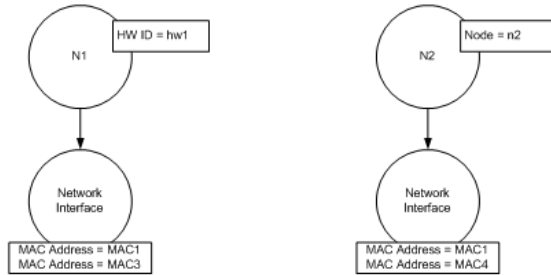
➤ Merge the input CI with each matched CI in the RTSM.
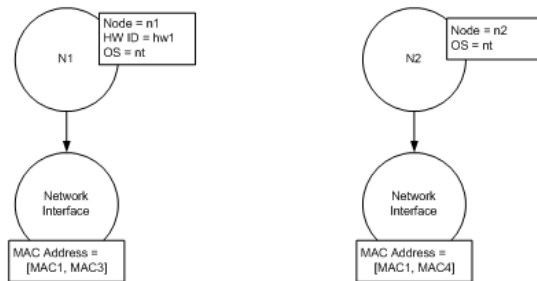
In this example, the input node matches two nodes in the RTSM having different identification criteria, and there are conflicts with the RTSM matched nodes.

➤ Merge the input CI with each matched CI in the RTSM.

➤ Check the conflicts between the resulting merged CIs. In this example, nodes N1 and N2 have conflicting MAC address match criteria.

The decision is to not merge all CIs to one.

The decision of whether to ignore data or pass it on for manual reconciliation depends on the flag setting for the MAC address match criterion.

Merge Service

The merge service is responsible for merging two or more CIs into one CI. This service is used by the Data In service and the Federation service.

Tasks

⚓ How to Add an Identification Rule to an Existing CIT

 1 Go to **Modeling** > **CI Type Manager** > **Details tab** and select **Advanced identification** as the identification method. For details, see "Details Page" in the *RTSM Modeling Guide*.

 2 Click the **Edit** button to open the XML editor. Create the identification rule. For details, see "How to Create an Identification Rule Document" on page 443.

⚓ How to Create an Identification Rule Document

This task describes how to prepare the XML schema for an identification rule file. For details about the schema elements and attributes, see "Identification Rule Schema" on page 446.

The identification rule document is an XML file that describes the required reconciliation data for a specific CI type. This identification rule is applied to the CI type and each of its 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. To do this:

 1 Navigate to **Admin** > **RTSM Administration** > **Modeling** > **CI Type Manager**.

 2 Click the **Details** tab.

 3 Select the information in the Identification field.

Example of the identification section

```
<identification-criteria>
    <identification-criterion>
        <connected-ci-condition ciType="interface" linkType="composition">
            <overlap-operator match-percent="66"/>
            <attribute-condition attributeName="mac_address"/>
        </connected-ci-condition>
    </identification-criterion>
    <identification-criterion>
        <attribute-condition attributeName="name" operator="EqualIgnoreCase"/>
    </identification-criterion>
    <identification-criterion>
        <connected-ci-condition ciType="ip_address" linkType="containment">
            <overlap-operator match-percent="66"/>
            <attribute-condition attributeName="name"/>
            <attribute-condition attributeName="routing_domain"/>
        </connected-ci-condition>
    </identification-criterion>
    <identification-criterion>
        <attribute-condition attributeName="bios_uuid"/>
    </identification-criterion>
 </identification-criteria>
```

In this example:

➤ A 66% match of the mac_address attribute from the connected interfaces CI types is required.

➤ The name attribute is not case sensitive.

➤ The rule requires both the ip_address name and routing_domain to 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 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 field.

➤ Only one priority criterion is given in this example, but there may be many criteria with the same priority.

Reference

🔍 Identification Rule Schema

Element		Attributes
Name and Path	**Description**	
identification-config	The parent element for the identification rule document.	**Name.** description **Description.** A textual description of the identification rule. **Is required.** Optional **Type.** String
		Name. type **Description.** The CI type to which the identification rule will apply. **Is required.** Required **Type.** String
identification-criteria (Identification-config)	The parent element for all the possible identification criteria for the CI type. For details, see "Identification Criteria" on page 433. The identification criteria may contain many **identification-criterion** elements. Can appear at most once.	

Element		Attributes
Name and Path	**Description**	
match (Identification-config)	The parent element for all the possible match criteria for the CI type. For details, see "Match Criteria" on page 434. Can appear at most once.	
multiple-match-resolving (Identification-config)	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.	**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
preferred-property (identification-config > multiple-match-resolving)	This element specifies the property value of the CI that will be preferred when there are multiple matches which cannot be merged.	**Name.** name **Description.** The name of the property. **Is required.** Required **Type.** String
		Name. value **Description.** The value of the property. Is **required.** required **Type.** String
		Name. priority **Description.** The priority of this preferred property. **Is required.** Optional **Type.** Integer

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**.	**Name.** targetType **Description.** Indicates for which CI type 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 **Type.** String
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.	

Element		Attributes
Name and Path	**Description**	

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.
		Name. attributeName
		Description. The name of the attribute.
		Is required. Required
		Type. String

		Name. masterValue **Description.** For the purpose of fulfilling the condition, the value defined here is considered equal to any other value. **Is required.** Optional **Type.** String
		Name. operator **Description.** Specifies whether the equality of attribute values should be case sensitive or not. The default is case sensitive. **Is required.** Optional **Type.** One of the values: Equals or EqualsIgnoreCase
		Name. includeNullValue **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. **Is required.** Optional **Type.** Boolean

Element		Attributes
Name and Path	**Description**	
(cont'd)		**Name**. conditionType **Type**. One of the following values: **approveAndContradict** condition is used for both approving and contradicting CIs (default) or **contradictOnly** condition is used to contradict two CIs.

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.	**Name.** ciType
		
		Description. The type of CI that is assumed to be connected to the CI type to which this rule belongs using the **linkType** attribute.
		
		Is required. Required
		
		Type. String

		Name. linkType **Description.** The type of link that the **ciType** attribute uses to connect to the CI type to which this rule belongs **Is required.** Required **Type.** String
		Name. isDirectionForward **Description.** The direction of the link. Default value is True (from the rule's CI type to ciType). **Is required.** Optional **Type.** Boolean

Element		Attributes
Name and Path	**Description**	
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 434. The verification criteria must contain at least one **verification-criterion** element. Can appear at most once.	

Element		Attributes
Name and Path	**Description**	
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 **Type.** Boolean
		Name. numberOfConflictsToFailIdentification **Description.** The number of conflicting conditions that will cause the current criterion to fail. Default Value: 1. **Is required.** Optional **Type.** Integer
validation-criteria (Identification-config > match)	The parent element for all possible validation criteria for the CI type. For details, see "Match Criteria" on page 434. The validation criteria must contain at least one **validation-criterion** element. Can appear at most once.	

Element		Attributes
Name and Path	**Description**	
validation-criterion (Identification-config > match > validation-criteria)	This element defines a single validation criterion. The criterion may contain many conditions for validation.	**Name.** priority **Description.** The criterion's priority. **Is required.** Required **Type.** Integer
		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 **Type.** Boolean
		Name. numberOfConflictsToFailIdentification **Description.** The number of conflicting conditions that will cause the current criterion to fail. Default Value: 1. **Is required.** Optional **Type.** Integer

13

Reconciliation Priority

This chapter includes:

Concepts

➤ Reconciliation Priority Overview on page 456

Tasks

➤ How to Add Reconciliation Priorities to an Existing CIT on page 457

➤ How to Create a Reconciliation Priority Document on page 457

Reference

➤ Reconciliation Priority Schema on page 459

➤ Reconciliation Priority Manager User Interface on page 460

Concepts

🔹 Reconciliation Priority Overview

Reconciliation Priority (conflict resolution) specifies how matched CIs are merged. You set these priorities in the Reconciliation Priority Manager. For details, see "Reconciliation Priority Window" on page 465.

For details about the reconciliation process and its rules, see "Reconciliation" on page 429.

Reconciliation Priority Configuration

When a CI is matched with another CI, they should be merged. This behavior becomes relevant in the following situations:

➤ During Data In service – to insert an already existing CI into the RTSM.

➤ During Federation – 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.

For details, see "Reconciliation Priority Window" on page 465.

Tasks

⚑ How to Add Reconciliation Priorities to an Existing CIT

1 Create an XML reconciliation file that contains reconciliation priorities. For details, see "How to Create a Reconciliation Priority Document" on page 457.

2 Create a package that contains the XML priorities file. The XML file should be located in a folder called **reconciliationPriority** at the root level in the package. For details, see "How to Create a Custom Package" in the *RTSM Administration Guide*.

3 Deploy the package. For details, see "How to Deploy a Package" in the *RTSM Administration Guide*.

⚑ How to Create a Reconciliation Priority Document

This task describes how to prepare the XML file according to the reconciliation priority schema. For details about the schema elements and attributes, see "Reconciliation Priority Schema" on page 459.

The reconciliation priorities document is an XML file that describes the priorities of integration points in the Data In flow for a specific CI type. The priority is applied to the CI type and each of its descendants, unless one of them has a priority of its own for a given integration point.

You can create a reconciliation priority document from a blank XML document.

Example

```
<reconciliation-priority-config type="node">
    <reconciliation-priority dataStoreName="CMS_Sync" priority="80"/>
    <reconciliation-priority dataStoreName="DDMI_DS" priority="70"/>
    <attributes-reconciliation-priorities>
        <attribute-reconciliation-priorities attribute-name="name">
            <reconciliation-priority dataStoreName="DDMI_DS" priority="100"/>
        </attribute-reconciliation-priorities>
        <attribute-reconciliation-priorities attribute-name="snmp_sys_name">
            <reconciliation-priority dataStoreName="CMS_Sync" priority="50"/>
        </attribute-reconciliation-priorities>
    </attributes-reconciliation-priorities>
</reconciliation-priority-config>
```

In this example:

1 The document handles only two data repositories: CMS_Sync and DDMI_DS. There may be other data repositories that already exist in the RTSM or that will be created afterwards. This means that even though we could have given a data repository the highest priority (100) and the other the lowest priority (1), it is unwise to do so, since this leaves no room to integrate future or existing data repositories to the priority system.

2 We first define a priority value for all attributes of **node**. This is optional, and if omitted defaults to 100.

3 For specific attributes we changed one of the data repositories. The other has the same value as the one defined at the top of the document.

Reference

🔍 Reconciliation Priority Schema

Element		Attributes
Name and Path	**Description**	
reconciliation-priority-config	The parent element of a reconciliation priority section for a specific CI type.	**Name.** type **Description.** The CI type to which the reconciliation priorities will apply. **Is required.** Required **Type.** String
reconciliation-priority (reconciliation-priority-config -OR- reconciliation-priority-config > attributes-reconciliation-priorities)	When this appears under the **reconciliation-priority-config** element, it defines priorities for all attributes in an integration point. When it appears under the **attribute-reconciliation-priorities** element, it defines a priority for a specific attribute. Must appear at least once when it is the child of the **attributes-reconciliation-priorities** element.	**Name.** dataStoreName **Description.** The name of the integration point. **Is required.** Required **Type.** String
		Name. priority **Description.** The priority of the dataStoreName attribute. **Is required.** Required **Type.** String

Element		Attributes
Name and Path	**Description**	
attributes-reconciliation-priorities (reconciliation-priority-config)	The parent element for the section of the document that defines priorities for specific attributes. Can appear at most once.	
attribute-reconciliation-priorities (reconciliation-priority-config > attributes-reconciliation-priorities)	Defines the priorities of integration points for specific attributes of the current CI type.	**Name.** attribute-name **Description.** The name of the attribute for which to define priorities. **Is required.** Required **Type.** String

✎ **Reconciliation Priority Manager User Interface**

This section includes (in alphabetical order):

✎ Add Attribute Dialog Box

The Add Attribute dialog box enables you to select specific attributes and specify a priority override value for each.

To access	Select a CI type in the CI Types tree and click ➕ in the Attribute Overrides area.

User interface elements are described below:

UI Element (A-Z)	Description
Attributes	Enables you to specify an attribute for which you want to specify a priority override.
	Select the **<Show hidden attributes>** check box to include hidden attributes in the displayed list. Hidden attributes are not marked as **Visible** in the Attributes pane of the CI Type Manager. For details, see "Attributes Page" in the *RTSM Modeling Guide*.
	To change the priority of an attribute, do the following:
	➤ Click in the **Priority** field and enter a new value.
	➤ Press **Enter**.
	➤ Click 💾 in the CI Types pane.
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.

✦ CI Types Pane

The CI Types pane displays the list of CI types and attributes that are supported by the selected integration point.

When you select a node in the CI Types tree, all integration points that support the selected item are displayed in the CI Type Overrides area.

If there is a manual override on an item in the tree, that item and all its parent items will be displayed with an asterisk next to the CI type.

User interface elements are described below:

UI Element (A-Z)	Description
	Expands the entire hierarchical tree structure.
	Collapses the hierarchical tree structure.
Tree View	Click Tree View to select the display format of the CI types tree. The following options are available: ➤ 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.

<CI Type> - Reconciliation Priority Overrides Pane

When you select a CI type in the Reconciliation Priority Manager, the Reconciliation Priority Overrides pane lists all integration points that contain the selected item and the priority overrides for those CI types, if any.

Attribute Overrides Area

User interface elements are described below:

UI Element (A-Z)	Description
✚	Opens the Add Attribute dialog box, which enables you to specify attributes for which you want to set overrides. For details, see "Add Attribute Dialog Box" on page 461.
🔁	Resets the value of the selected attribute to its default value.
	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.
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.

UI Element (A-Z)	Description
Priority	Displays the priority that is assigned to a particular attribute. 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.
	To change the priority of an item, do the following:
	➤ Click in the **Priority** field and enter a new value.
	➤ Press **Enter**.
	➤ Click in the CI Types pane.

CI Type Overrides Area

User interface elements are described below:

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	Displays the priority that is assigned to a particular CI Type. 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.
	To change the priority of a CI type, do the following:
	➤ Click in the **Priority** field and enter a new value.
	➤ Press **Enter**.
	➤ Click in the CI Types pane.

⚲ 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 275.

For details about the reconciliation engine, see "Reconciliation" on page 429.

To access	Do one of the following:
	➤ Select **Admin** > **RTSM Administration** > **Data Flow Management** > **Reconciliation Priority.**
	➤ Select **Admin** > **RTSM Administration** > **Data Flow Management** > **Integration Studio** and click 🔧 .
Relevant tasks	➤ "How to Work with Federated Data" on page 255
	➤ "How to Work with Population Jobs" on page 256
	➤ "How to Work with Data Push Jobs" on page 257

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, or to set priorities for all integration points.
	If you have selected a specific integration point, its name is highlighted in the right pane. You can then change the reconciliation priority for that integration point only.

Part VI

Hardening

14

Data Flow Credentials Management

This chapter includes:

Concepts

Tasks

Reference

Concepts

♣ Data Flow Credentials Management Overview

To perform discovery or run integration, you must set up the credentials to access the remote system. Credentials are configured in the Data Flow Probe Setup window and saved in the RTSM Server. For details, see "Data Flow Probe Setup Window" on page 155.

Credentials storage is managed by the Confidential Manager (CM) component. For details, see "Confidential Manager" on page 397.

The Data Flow Probe can access the credentials using the CM client. The CM client resides on the Data Flow Probe and communicates with the CM server, which resides on the RTSM Server. Communication between the CM client and the CM server is encrypted, and authentication is required by the CM client when it connects to the CM server.

The CM client's authentication on the CM server is based on a LW-SSO component. Before connecting to the CM server, the CM client first sends an LW-SSO cookie. The CM server verifies the cookie and upon successful verification, communication with the CM client begins. For details about LW-SSO, see "Configure LW-SSO Settings on the RTSM Server" on page 476.

The communication between the CM client and the CM server is encrypted. For details about updating the encryption configuration, see "Configure CM Communication Encryption on the RTSM Server" on page 477.

Important: The CM authentication uses the universal time defined on the computer (UTC). In order for the authentication to succeed, ensure that the universal time on the Data Flow probe and the UCMDB Server are the same. The server and probe may be located in different time zones, as UTC is independent of time zone or daylight savings time.

The CM client maintains a local cache of the credentials. The CM client is configured to download all credentials from the CM server and store them in a cache. The credentials changes are automatically synchronized from CM server on a continuous basis. The cache can be a file-system or in-memory cache, depending on the preconfigured settings. In addition, the cache is encrypted and cannot be accessed externally. For details about updating the cache settings, see "Configure the CM Client's Cache Mode on the Probe" on page 483. For details about updating the cache encryption, see "Configure the CM Client's Cache Encryption Settings on the Probe" on page 484.

For details on troubleshooting, see "How to Change Confidential Manager (CM) Client Log File Message Level" on page 488.

You can copy credentials information from one RTSM server to another. For details, see "How to Export and Import Credential and Range Information in Encrypted Format" on page 486.

Note: The **DomainScopeDocument** (DSD) that was used for credentials storage on the Probe (in UCMDB version 9.01 or earlier) no longer contains any credentials-sensitive information. The file now contains a list of Probes and network range information. It also contains a list of credential entries for each domain, where each entry includes the credential ID and a network range (defined for this credential entry) only.

This section includes the following topics:

➤ "Basic Security Assumptions" on page 472

➤ "Data Flow Probe Running in Separate Mode" on page 472

➤ "Keeping the Credentials Cache Updated" on page 472

➤ "Synchronizing All Probes with Configuration Changes" on page 472

➤ "Secured Storage on the Probe" on page 474

Basic Security Assumptions

Note the following security assumption:

You have secured the Gateway Server and Probe JMX console to enable access to BSM system administrators only, preferably through localhost access only.

Data Flow Probe Running in Separate Mode

When the Probe Gateway and Manager run as separate processes, the Confidential Manager (CM) client component becomes part of the Manager process. Credentials information is cached and used by the Probe Manager only. To access the CM server on the RTSM system, the CM client request is handled by the Gateway process and from there is forwarded to the RTSM system.

This configuration is automatic when the Probe is configured in separate mode.

Keeping the Credentials Cache Updated

On its first successful connection to the CM server, the CM client downloads all relevant credentials (all credentials that are configured in the probe's domain). After the first successful communication, the CM client retains continuous synchronization with the CM server. Differential synchronization is performed at one-minute intervals, during which only differences between the CM server and the CM client are synchronized. If the credentials are changed on the RTSM server side (such as new credentials being added, or existing credentials being updated or deleted), the CM client receives immediate notification from the RTSM server and performs additional synchronization.

Synchronizing All Probes with Configuration Changes

For successful communication, the CM client must be updated with the CM server authentication configuration (LW-SSO init string) and encryption configuration (CM communication encryption). For example, when the init string is changed on the server, the probe must know the new init string in order to authenticate.

The RTSM server constantly monitors for changes in the CM communication encryption configuration and CM authentication configuration. This monitoring is done every 15 seconds; in case a change has occurred, the updated configuration is sent to the probes. The configuration is passed to the probes in encrypted form and stored on the probe side in secured storage. The encryption of configuration being sent is done using a symmetric encryption key. By default, the RTSM server and Data Flow Probe are installed with same default symmetric encryption key. For optimal security, it is highly recommended to change this key before adding credentials to the system. For details, see "How to Generate or Update the Encryption Key" on page 490.

Note:

➤ Due to the 15 second monitoring interval, it is possible that the CM client, on the Probe side, may not be updated with the latest configuration for a period of 15 seconds.

➤ If you choose to disable the automatic synchronization of CM communication and authentication configuration between the RTSM server and the Data Flow Probe, each time you update the CM communication and authentication configuration on the RTSM server side, you should update all Probes with the new configuration as well. For details, see "Disable Automatic Synchronization of the CM Client Authentication and Encryption Settings Between the RTSM Server and Probes" on page 479.

Secured Storage on the Probe

All sensitive information (such as the CM communication and authentication configuration and the encryption key) is stored on the Probe in secure storage in the **secured_storage.bin** file, located in the **C:\hp\UCMDB\DataFlowProbe\conf\security** directory. This secured storage is encrypted using DPAPI, which relies on the Windows user password in the encryption process. DPAPI is a standard method used to protect confidential data—such as certificates and private keys—on Windows systems. The Probe should always run under the same Windows user, so that even if the password is changed, the Probe can still read the information stored in secure storage.

Viewing Credentials Information (Data Direction: RTSM to BSM)

Passwords are not sent from the RTSM database to the application. BSM displays asterisks (*****) in the password field, regardless of content:
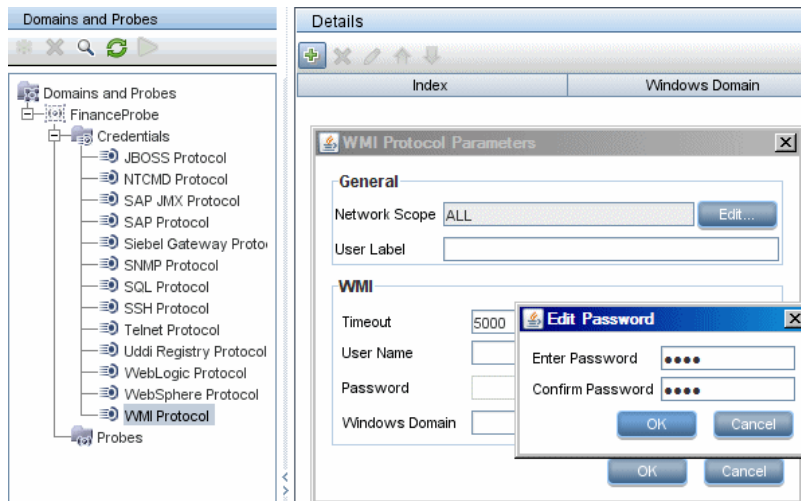
🔵 Updating Credentials (Data Direction: BSM to RTSM)

➤ The communication in this direction is not encrypted, therefore you should connect to the BSM Gateway Server using https\SSL, or ensure connection through a trusted network.

Although the communication is not encrypted, passwords are not being sent as clear text on the network. They are encrypted using a default key and, therefore, it is highly recommended to use SSL for effective confidentiality in transit.

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

Tasks

🔧 How to Configure CM Client Authentication and Encryption Settings on the RTSM Server

This task includes the following steps:

➤ "Configure LW-SSO Settings on the RTSM Server" on page 476

➤ "Configure CM Communication Encryption on the RTSM Server" on page 477

Configure LW-SSO Settings on the RTSM Server

This procedure describes how to change the LW-SSO init string on the RTSM server. This change is automatically sent to Probes (as an encrypted string), unless the RTSM server is configured to not automatically do this. For details, see "Disable Automatic Synchronization of the CM Client Authentication and Encryption Settings Between the RTSM Server and Probes" on page 479.

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

2 Click **UCMDB-UI:name=LW-SSO Configuration** to open the JMX MBEAN View page.

3 Locate the **setInitString** method.

4 Enter a new LW-SSO init string.

5 Click **Invoke**.

Configure CM Communication Encryption on the RTSM Server

This procedure describes how to change the CM communication encryption settings. These settings specify how the communication between the CM client and the CM server is encrypted. This change is automatically sent to Probes (as an encrypted string), unless the RTSM server is configured to not automatically do this. For details, see "Disable Automatic Synchronization of the CM Client Authentication and Encryption Settings Between the RTSM Server and Probes" on page 479.

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

2 Click **UCMDB:service=Security Services** to open the JMX MBEAN View page.

3 Click the **CMGetConfiguration** method.

4 Click **Invoke**.

The XML of the current CM configuration is displayed.

5 Copy the contents of the displayed XML.

6 Navigate back to the **Security Services** JMX MBean View page.

7 Click the **CMSetConfiguration** method.

8 Paste the copied XML into the **Value** field.

9 Update the relevant transport-related settings.

For details about the values that can be updated, see "CM Encryption Settings" on page 496.

Example:

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

10 Click **Invoke**.

🖈 How to Configure CM Client Authentication and Encryption Settings Manually on the Probe

This task includes the following steps:

➤ "Disable Automatic Synchronization of the CM Client Authentication and Encryption Settings Between the RTSM Server and Probes" on page 479

➤ "Configure CM Client Authentication and Encryption Settings on the Probe" on page 480

➤ "Configure CM Communication Encryption on the Probe" on page 481

Disable Automatic Synchronization of the CM Client Authentication and Encryption Settings Between the RTSM Server and Probes

By default, the UCMDB Server is configured to automatically send the CM/LW-SSO settings to all Probes. This information is sent as an encrypted string to the Probes, which decrypt the information upon retrieval. You can configure the UCMDB Server to not send the CM/LW-SSO configuration files automatically to all Probes. In this case, it is your responsibility to manually update all Probes with the new CM/LW-SSO settings.

To disable automatic synchronization of CM/LW-SSO settings:

1 In RTSM, click **Admin** > **RTSM Administration** > **Administration** > **Infrastructure Settings Manager** > **General Settings**.

2 Select **Enable automatic synchronization of CM/LW-SSO configuration and init string with probe**.

3 Click the **Value** field and change **True** to **False**.

4 Click the **Save** button.

5 Restart the RTSM server.

Configure CM Client Authentication and Encryption Settings on the Probe

This procedure is relevant if the RTSM Server has been configured to not send LW-SSO/CM configuration and settings automatically to Probes. For details, see "Disable Automatic Synchronization of the CM Client Authentication and Encryption Settings Between the RTSM Server and Probes" on page 479.

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

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

---

2 Click **type=CMClient** to open the JMX MBEAN View page.

3 Locate the **setLWSSOInitString** method and provide the same init string that was provided for RTSM's LW-SSO configuration.

4 Click the **setLWSSOInitString** button.

Configure CM Communication Encryption on the Probe

This procedure is relevant if the RTSM Server has been configured to not send LW-SSO/CM configuration and settings automatically to Probes. For details, see "Disable Automatic Synchronization of the CM Client Authentication and Encryption Settings Between the RTSM Server and Probes" on page 479.

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

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

---

 2 Click **type=CMClient** to open the JMX MBEAN View page.

 3 Update the following transport-related settings:

Note: You must update the same settings that you updated on the RTSM server. To do this, some of the methods that you update on the Probe may require more than one parameter. To see the current probe configuration, click **displayTransportConfiguration** in the JMX MBEAN View page. For details, see "Configure CM Communication Encryption on the RTSM Server" on page 477. For details about the values that can be updated, see "CM Encryption Settings" on page 496.

---

 a **setTransportInitString** changes the **encryptDecryptInitString** setting.

 b **setTransportEncryptionAlgorithm** changes CM settings on the Probe according to the following map:

   ➤ **Engine name** refers to the <engineName> entry

   ➤ **Key size** refers to the <keySize> entry

➤ **Algorithm padding name** refers to the <algorithmPaddingName> entry

➤ **PBE count** refers to the <pbeCount> entry

➤ **PBE digest algorithm** refers to the <pbeDigestAlgorithm> entry

c **setTransportEncryptionLibrary** changes CM settings on the Probe according to the following map:

➤ **Encryption Library name** refers to the <cryptoSource> entry

➤ **Support previous lightweight cryptography versions** refers to the <lwJCEPBECompatibilityMode> entry

d **setTransportMacDetails** change CM settings on the Probe according to the following map:

➤ **Use MAC with cryptography** refers to the <useMacWithCrypto> entry

➤ **MAC key size** refers to the <macKeySize> entry

4 Click the **reloadTransportConfiguration** button to make the changes effective on the Probe.

For details about the different settings and their possible values, see "CM Encryption Settings" on page 496.

🔧 How to Configure the Confidential Manager (CM) Client Cache

This task includes the following steps:

➤ "Configure the CM Client's Cache Mode on the Probe" on page 483

➤ "Configure the CM Client's Cache Encryption Settings on the Probe" on page 484

Configure the CM Client's Cache Mode on the Probe

The CM client stores credentials information in the cache and updates it when the information changes on the Server. The cache can be stored on the file system or in memory:

➤ **When stored on the file system**, even if the Probe is restarted and cannot connect to the Server, the credentials information is still available.

➤ **When stored in memory**, if the Probe is restarted, the cache is cleared and all information is retrieved again from the Server. If the Server is not available, the Probe does not include any credentials, so no discovery or integration can run.

To change this setting:

1 Open the **DiscoveryProbe.properties** file in a text editor. This file is located in the **c:\hp\UCMDB\DataFlowProbe\conf** directory.

2 Locate the following attribute:
com.hp.ucmdb.discovery.common.security.storeCMData=true

➤ To store the information on the file system, leave the default (**true**).

➤ To store the information in memory, enter **false**.

3 Save the **DiscoveryProbe.properties** file.

4 Restart the Probe.

Configure the CM Client's Cache Encryption Settings on the Probe

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

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

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

---

2 Click **type=CMClient** to open the JMX MBEAN View page.

3 Update the following cache-related settings:

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

---

a **setCacheInitString** changes the file system cache <encryptDecryptInitString> setting.

b **setCacheEncryptionAlgorithm** changes the file system cache settings according to the following map:

➤ **Engine name** refers to the <engineName> entry

➤ **Key size** refers to the <keySize> entry

➤ **Algorithm padding name** refers to the <algorithmPaddingName> entry

➤ **PBE count** refers to the <pbeCount> entry

➤ **PBE digest algorithm** refers to the <pbeDigestAlgorithm> entry

  c **setCacheEncryptionLibrary** changes the cache file system settings according to the following map:

➤ **Encryption Library name** refers to the <cryptoSource> entry

➤ **Support previous lightweight cryptography versions** refers to the <lwJCEPBECompatibilityMode> entry

  d **setCacheMacDetails** changes the cache file system settings according to the following map:

➤ **Use MAC with cryptography** refers to the <useMacWithCrypto> entry

➤ **MAC key size** refers to the <macKeySize> entry

4 Click the **reloadCacheConfiguration** button to make the changes effective on the Probe. This causes the Probe to restart.

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

For details about the different settings and their possible values, see "CM Encryption Settings" on page 496.

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

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

➤ **When exporting credentials information**, you must enter a password (of your choosing). The information is encrypted with this password.

➤ **When importing credentials information**, you must use the same password that was defined when the DSD file was exported.

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

Important: To import credentials information from a UCMDB version 8.02 domainScopeDocument, you must use the **key.bin** file located on the version 8.02 system.

To export credentials information from the RTSM Server:

1 On the RTSM Server, launch the Web browser and enter the following address: **http://localhost:8080/jmx-console**. You may have to log in with a user name and password.

2 Click **UCMDB:service=DiscoveryManager** to open the JMX MBEAN View page.

3 Locate the **exportCredentialsAndRangesInformation** operation. Do the following:

➤ Enter your customer ID (the default is 1).

➤ Enter a name for the exported file.

➤ Enter your password.

➤ Set **isEncrypted=True** if you want the exported file to be encrypted with the provided password, or **isEncrypted=False** if you want the exported file to not be encrypted (in which case passwords and other sensitive information are not exported).

4 Click **Invoke** to export.

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

To import credentials information from the RTSM Server:

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

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

2 Click **UCMDB:service=DiscoveryManager** to open the JMX MBEAN View page.

3 Locate one of the following operations:

➤ Locate the **importCredentialsAndRangesInformation** operation if the file that you are importing was exported from a RTSM Server that is later than version 8.02.

➤ Locate the **importCredentialsAndRangesWithKey** operation if the file that you are importing was exported from a RTSM version 8.02 Server.

4 Enter your customer ID (the default is 1).

5 Enter the name of the file to import. This file must be located in the **c:\hp\UCMDB\UCMDBServer\conf\discovery\<customer_dir>** directory.

6 Enter the password. This must be the same password that was used when the file was exported.

7 If the file was exported from a RTSM version 8.02 system, enter the **key.bin** file name. This file must be located in the **c:\hp\UCMDB\ UCMDBServer\conf\discovery\<customer_dir>** directory, together with the file to be imported.

8 Click **Invoke** to import the credentials.

How to Change Confidential Manager (CM) Client Log File Message Level

The Probe provides two log files that contain information regarding CM-related communication between the CM server and the CM client. The files are:

➤ "CM Client Log File" on page 488
➤ "LW-SSO Log File" on page 489

CM Client Log File

The **security.cm.log** file is located in the **c:\hp\UCMDB\DataFlowProbe\runtime\log** directory.

The log contains information messages exchanged between the CM server and the CM client. By default, the log level of these messages is set to INFO.

To change the log level of the messages to DEBUG level:

1 On the Data Flow Probe Manager server, navigate to **c:\hp\UCMDB\DataFlowProbe\conf\log**.

2 Open the **security.properties** file in a text editor.

3 Change the line:

    loglevel.cm=INFO

to:

    loglevel.cm=DEBUG

4 Save the file.

LW-SSO Log File

The **security.lwsso.log** file is located in the
c:\hp\UCMDB\DataFlowProbe\runtime\log directory.

The log contains information messages related to LW-SSO. By default, the
log level of these messages is set to INFO.

To change the log level of the messages to DEBUG level:

1 On the Data Flow Probe Manager server, navigate to
c:\hp\UCMDB\DataFlowProbe\conf\log.

2 Open the **security.properties** file in a text editor.

3 Change the line:

    loglevel.lwsso=INFO

to:

    loglevel.lwsso=DEBUG

4 Save the file.

🔍 How to Generate or Update the Encryption Key

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

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

Note:

➤ The difference between the methods used to create a key (**generateEncryptionKey**) and update a key (**changeEncryptionKey**) is that **generateEncryptionKey** creates a new, random encryption key, while **changeEncryptionKey** imports an encryption key whose name you provide.

➤ Only one encryption key can exist on a system, no matter how many Probes are installed.

This task includes the following steps:

➤ "Generate a New Encryption Key" on page 491

➤ "Update an Encryption Key on a RTSM Server" on page 492

➤ "Update an Encryption Key on a Probe" on page 493

➤ "Manually Change the Encryption Key when the Probe Manager and Probe Gateway are Installed on Separate Machines" on page 494

➤ "Generate a New Encryption Key" on page 491

Generate a New Encryption Key

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

To generate a new encryption key through the JMX console:

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

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

2 Click **UCMDB:service=DiscoveryManager** to open the JMX MBEAN View page.

3 Locate the generateEncryptionKey operation.

   a In the **customerId** parameter box, enter **1** (the default).

   b For **keySize**, specify the length of the encryption key. Valid values are 128, 192, or 256.

   c For **usePBE**, specify **True** or **False**:

   ➤ **True**: use additional PBE hash cycles.

   ➤ **False:** do not use additional PBE hash cycles.

   d For **jceVendor**, you can choose to use a non-default JCE provider. If the box is empty, the default provider is used.

   e For **autoUpdateProbe**, specify **True** or **False**:

   ➤ **True**: the server distributes the new key to the Probes automatically.

   ➤ **False:** the new key should be placed on the Probes manually.

    f For **exportEncryptionKey**, specify **True** or **False**.

        ➤ **True**: In addition to creating the new password and storing it in secured storage, the Server exports the new password to the file system (**c:\hp\UCMDB\UCMDBServer\conf\discovery\key.bin**). This option enables you to update Probes manually with the new password.

        ➤ **False**: The new password is not exported to the file system. To update Probes manually, set **autoUpdateProbe** to **False** and **exportEncryptionKey** to **True**.

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

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

Update an Encryption Key on a RTSM Server

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

To update an encryption key through the JMX Console:

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

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

2 Click **UCMDB:service=DiscoveryManager** to open the JMX MBEAN View page.

3 Locate the **changeEncryptionKey** operation.

    a In the **customerId** parameter box, enter **1** (the default).

    b For **newKeyFileName**, enter the name of the new key.

    c For **keySizeInBits**, specify the length of the encryption key. Valid values are 128, 192, or 256.

d For **usePBE**, specify **True** or **False**:

> ➤ **True**: use additional PBE hash cycles.

> ➤ **False:** do not use additional PBE hash cycles.

e For **jceVendor**, you can choose to use a non-default JCE provider. If the box is empty, the default provider is used.

f For **autoUpdateProbe**, specify **True** or **False**:

> ➤ **True**: the server distributes the new key to the Probes automatically.

> ➤ **False:** the new key should be distributed manually using the Probe JMX console.

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

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

Update an Encryption Key on a Probe

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

1 Place the encryption key file in the **C:\hp\UCMDB\DataFlowProbe \conf\security** directory.

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

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

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

3 On the Probe domain, click **type=SecurityManagerService**.

4 Locate the **importEncryptionKey** method.

5 Enter the name of the encryption key file that resides in the **C:\hp\UCMDB\DataFlowProbe\conf\security** directory. This file contains the key to be imported.

6 Click the **importEncryptionKey** button.

7 Perform a restart of the probe.

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

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

2 Import the key from the server, using the Probe Manager JMX. For details, see "Generate a New Encryption Key" on page 491.

3 After the encryption key is imported successfully, restart the Probe Manager and Probe Gateway services.

Define Several JCE Providers

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

To change the default JCE provider:

1 Register the JCE provider jar files in the **$JRE_HOME/lib/ext** directory.

2 Copy the jar files to the $JRE_HOME directory:

➤ For the RTSM Server: $JRE_HOME resides at:
   c:\hp\UCMDB\UCMDBServer\bin\jre

➤ For the Data Flow Probe: $JRE_HOME resides at:
   c:\hp\UCMDB\DataFlowProbe\bin\jre

3 Add the provider class at the end of the provider list in the **$JRE_HOME\lib\security\java.security** file.

4 Update the **local_policy.jar** and **US_export_policy.jar** files to include unlimited JCE policies. You can download these jar files from the Sun Web site.

5 Restart the RTSM Server and the Data Flow Probe.

6 Locate the JCE vendor field for the **changeEncryptionKey** or **generateEncryptionKey** method, and add the name of the JCE provider.

Reference

🔍 CM Encryption Settings

This table lists the encryption settings that can be changed using various JMX methods. These encryption settings are relevant for encryption of communications between the CM client and the CM server, as well as for encryption of the CM client's cache.

RTSM CM Setting Name	Probe CM Setting Name	Setting Description	Possible Values	Default Value
cryptoSource	Encryption Library name	This setting defines which encryption library to use.	lw, jce, windowsDPAPI, lwJCECompatible	lw
lwJCEPBECompatibilityMode	Support previous lightweight cryptography versions	This setting defines whether to support previous lightweight cryptography or not.	true, false	true
engineName	Engine name	Encryption mechanism name	AES, DES, 3DES, Blowfish	AES
keySize	Key size	encryption key length in bits	For AES - 128, 192 or 256; For DES - 64; For 3DES - 192; For Blowfish - any number between 32 and 448	256
algorithmPaddingName	Algorithm padding name	Padding standards	PKCS7Padding, PKCS5Padding	PKCS7Padding

RTSM CM Setting Name	Probe CM Setting Name	Setting Description	Possible Values	Default Value
pbeCount	PBE count	The number of times to run the hash to create the key from password (init string)	Any positive number	20
pbeDigestAlgorithm	PBE digest algorithm	Hashing type	SHA1, SHA256, MD5	SHA1
useMacWithCrypto	Use MAC with cryptography	Indication if to use MAC with the cryptography	true, false	false
macKeySize	MAC key size	Depends on MAC algorithm	256	256

🔍 Troubleshooting and Limitations

If you change the default domain name on the UCMDB server, you must first verify that the Data Flow Probe is not running. After the default domain name is applied, you must execute the **DataFlowProbe\tools\clearProbeData.bat script** on the Data Flow Probe side.

Note: Execution of the **clearProbeData.bat** script will cause a discovery cycle on the Probe side once the Probe is up.

15

Data Flow Probe Hardening

This chapter includes:

Tasks

Reference

Tasks

🔧 How to Set the MySQL Database Encrypted Password

This task describes how to encrypt the password for the MySQL database user.

1 Create the Encrypted Form of a Password (AES, 192-bit key)

a Access the Data Flow Probe JMX console. Launch a Web browser and enter the following address: **http://<Data Flow Probe machine name or IP address>:1977**. If you are running the Data Flow Probe locally, enter **http://localhost:1977**.

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

Note: If you have not created a user, use the default user name **admin** and the password **admin** to log in.

---

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

c Locate the **getEncryptedDBPassword** operation.

d In the **DB Password** field, enter the password to be encrypted.

e Invoke the operation by clicking the **getEncryptedDBPassword** button.

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

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

2 Stop the Data Flow Probe

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

3 Run the set_dbuser_password.cmd Script

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

Run the **set_dbuser_password.cmd** script with the new password as an
argument, for example, **set_dbuser_password <my_password>**.

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

4 Update the Password in the Data Flow Probe Configuration Files

a The password must reside encrypted in the configuration files. To
retrieve the password's encrypted form, use the
getEncryptedDBPassword JMX method, as explained in step 1 on
page 500.

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

➤ **appilog.agent.probe.jdbc.pwd**

For example:

```
appilog.agent.probe.jdbc.user = mamprobe
appilog.agent.probe.jdbc.pwd =
66,85,54,78,69,117,56,65,99,90,86,117,97,75,50,112,65,53,67,114,112,65,6
1,61
```

➤ **appilog.agent.local.jdbc.pwd**

5 Start the Data Flow Probe

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

The clearProbeData.bat Script: Usage

The **clearProbeData.bat** script recreates the database user with a password that is provided as an argument to the script.

After you set a password, each time you execute the **clearProbeData.bat** script, it retrieves the database password as an argument.

After running the script:

➤ Review the following file for errors:
C:\hp\UCMDB\DataFlowProbe\runtime\log\probe_setup.log

➤ Delete the following file, as it contains the database password:
C:\hp\UCMDB\DataFlowProbe\runtime\log\probe_setup.log

How to Set the JMX Console Encrypted Password

This task describes how to encrypt the password for the JMX user. The encrypted password is stored in the **DiscoveryProbe.properties** file. Users must log in to access the JMX console.

1 Create the Encrypted Form of a Password (AES, 192-bit key)

a Access the Data Flow Probe JMX console. Launch a Web browser and enter the following address: **http://<Data Flow Probe machine name or IP address>:1977**. If you are running the Data Flow Probe locally, enter **http://localhost:1977**.

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

Note: If you have not created a user, use the default user name **admin** and the password **admin** to log in.

---

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

c Locate the **getEncryptedKeyPassword** operation.

d In the **Key Password** field, enter the password to be encrypted.

e Invoke the operation by clicking the **getEncryptedKeyPassword** button.

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

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

2 Stop the Data Flow Probe

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

3 Add the Encrypted Password

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

appilog.agent.Probe.JMX.BasicAuth.Pwd

For example:

```
appilog.agent.Probe.JMX.BasicAuth.User=admin
appilog.agent.Probe.JMX.BasicAuth.Pwd=-85,-9,-61,11,105,-93,-81,118
```

Note: To disable authentication, leaves these fields empty. If you do so, users can open the main page of the Probe's JMX console without entering authentication.

---

4 Start the Data Flow Probe

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

b Test the result in a Web browser.

🔧 How to Restrict the Data Flow Probe's Access to the MySQL Server

This task describes how to permit access to the Data Flow Probe's MySQL database from the local machine only.

To restrict MySQL access:

Run the following script in a command prompt window or by double-clicking it: **C:\hp\UCMDB\DataFlowProbe\tools\dbscripts\remove_remote_user_access.cmd**.

Any user (other than the root user) trying to connect from a remote computer will now be denied access.

Note: Users who have root credentials to the MySQL database will still be able to access the database from the remote machine.

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

For details, see "How to Enable SSL Between BSM and the Data Flow Probe with Mutual Authentication" on page 515.

.

⚜ How to Enable Authentication on the Data Flow Probe with Basic HTTP Authentication

Important:

➤ The basic authentication method of enabling authentication on the Data Flow Probe is the least preferred method. It is recommended to use mutual authentication security, as it is a much more effective method of security (it combines data encryption and certificate authentication). For details, see "How to Enable SSL Between BSM and the Data Flow Probe with Mutual Authentication" on page 515.

➤ If SSL is not enabled, credentials are transmitted to UCMDB as plain-text.

To set basic authentication:

1 Locate the following file: **C:\hp\UCMDB\DataFlowProbe\conf\ DiscoveryProbe.properties**.

2 Remove the comment markers (#) from the following properties, and enter the relevant credentials:

```
appilog.agent.Probe.BasicAuth.Realm=
appilog.agent.Probe.BasicAuth.User=
appilog.agent.Probe.BasicAuth.Pwd=
```

The credentials should match those defined on the BSM server.

🔧 How to Connect the Data Flow Probe by Reverse Proxy

Perform the following procedure to connect the Data Flow Probe by reverse proxy.

Note: Enabling mutual authentication when using SSL between the BSM Server and the Data Flow Probe is not supported when the connection is made by reverse proxy.

To configure the Data Flow Probe to work against a reverse proxy:

1 Edit the **discoveryProbe.properties** file (located in **C:\hp\UCMDB\DataFlowProbe\conf**).

2 Set the **serverName** property to the reverse proxy server's IP or DNS name.

3 Set the **serverPort** and **serverPortHttps** properties to the reverse proxy server's ports.

4 Save the file.

The following proxy server configuration is required if Data Flow Probes only are connected via a reverse proxy to BSM:

Requests for... on the Reverse Proxy Server	Proxy Request to be Served by:
/mam-collectors	http://[BSM server]/mam-collectors

The following configuration is required if a SOAP adapter is used for replication via a reverse proxy to a secure (hardened) BSM:

Requests for... on the Reverse Proxy Server	Proxy Request to be Served by:
/axis2	http://[BSM server]/axis2

506

Connecting the Data Flow Probe and Web Clients by Reverse Proxy

The following configuration is required if both Data Flow Probes and application users are connected via a reverse proxy to BSM:

Requests for... on the Reverse Proxy Server	Proxy Request to be Served by:
/mam	[BSM server]/mam
/mam_images	[BSM server]/mam_images
/mam-collectors	[BSM server]/mam-collectors
/ucmdb	[BSM server]/ucmdb
/site	[BSM server]/site

How to Control the Location of the domainScopeDocument File

The Probe's file system holds (by default) both the encryption key and the domainScopeDocument file. Each time the Probe is started, the Probe retrieves the domainScopeDocument file from the server and stores it on its file system. To prevent unauthorized users from obtaining these credentials, you can configure the Probe so that the domainScopeDocument file is held in the Probe's memory and is not stored on the Probe file system.

To control the location of the domainScopeDocument file:

1 Open **C:\hp\UCMDB\DataFlowProbe\conf\DiscoveryProbe.properties** and change:

```
appilog.collectors.storeDomainScopeDocument=true
```

to:

```
appilog.collectors.storeDomainScopeDocument=false
```

The Probe Gateway and Probe Manager serverData folders no longer contain the domainScopeDocument file.

For details on using the domainScopeDocument file to harden DFM, see "Data Flow Credentials Management" on page 469.

2 Restart the Probe.

🏵 How to Create a Keystore for the Data Flow Probe

1 On the Probe machine, run the following command:

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

2 Enter a password for the new keystore.

3 Enter your information when asked.

4 When asked **Is CN=… C=… Correct?** enter **yes**, and press ENTER.

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

6 Verify that **client.keystore** is created in the following directory: **C:\HP\UCMDB\DataFlowProbe\conf\security**.

🏵 How to Encrypt the Probe Keystore and Truststore Passwords

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

1 Start Data Flow Probe (or verify that it is already running).

2 Access the Data Flow Probe JMX console: Launch a Web browser and enter the following address: **http://<Data Flow Probe machine name or IP address>:1977**. If you are running the Data Flow Probe locally, enter **http://localhost:1977**.

> **Note:** You may have to log in with a user name and password. If you have not created a user, use the default user name **admin** and the password **admin** to log in.

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

4 Locate the **getEncryptedKeyPassword** operation.

5 Enter your keystore or truststore password in the **Key Password** field and invoke the operation by clicking **getEncryptedKeyPassword**.

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

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

7 Copy and paste the encrypted password into the line relevant to either the keystore or the truststore in the following file: **C:\HP\UCMDB\DataFlowProbe\conf\security\ssl.properties**.

Reference

🔍 Run-time Service Model and Data Flow Probe Default Keystore and Truststore

This section includes the following topics:

RTSM

The files are located in the following directory:
C:\HP\UCMDB\UCMDBServer\conf\security.

Entity	File Name/Term	Password/Term	Alias
Server keystore	server.keystore (sKeyStoreFile)	hppass (sKeyStorePass)	hpcert
Server truststore	server.truststore (sTrustStoreFile)	hppass (sTrustStorePass)	clientcert (default trusted entry)
Client keystore	client.keystore (cKeyStoreFile)	clientpass (cKeyStorePass)	clientcert

Data Flow Probe

The files are located in the following directory:
C:\HP\UCMDB\DataFlowProbe\conf\security.

Entity	File Name/Term	Password/Term	Alias
Probe keystore	MAMKeyStoreExp.jks (pKeyStoreFile)	logomania (pKeyStorePass)	mam
Data Flow Probe uses the **cKeyStoreFile** keystore as the default keystore during the mutual authentication procedure. This is a client keystore that is part of the UCMDB installation.			
Probe truststore	MAMTrustStoreExp.jks (pTrustStoreFile)	logomania (pTrustStorePass)	mam (default trusted entry)
The **cKeyStorePass** password is the default password of **cKeyStoreFile**.			

16

Using SSL with the Data Flow Probe

This chapter includes:

Concepts

➤ Using SSL with the Data Flow Probe Overview on page 514

Tasks

➤ How to Enable SSL Between BSM and the Data Flow Probe with Mutual Authentication on page 515

➤ How to Configure SSL from the Data Flow Probe to the Gateway Server on page 519

Concepts

Using SSL with the Data Flow Probe Overview

This section describes how to configure your HP Universal CMDB platform with the Data Flow Probe and Staging Data Replicator to support communication using the Secure Sockets Layer (SSL) channel.

For introductory and general information on configuring HP Universal CMDB and its data collectors to support SSL, see "Introduction to Hardening the BSM Platform" in the *HP Business Service Management Hardening Guide* PDF.

Tasks

🪓 How to Enable SSL Between BSM and the Data Flow Probe with Mutual Authentication

You can set up authentication for both the Data Flow Probe and BSM (running an RTSM), with certificates. The certificate for each side is sent and authenticated before the connection is established.

Important: The following method of enabling SSL on the Data Flow Probe replaces the procedure for basic authentication, which is deprecated.

This section includes the following topics:

➤ "Prerequisites" on page 515

➤ "Enable Mutual Certificate Authentication" on page 515

Prerequisites

Set up the BSM server with an RTSM, running in SSL. Client certificates are required.

Enable Mutual Certificate Authentication

If the certificate used by the Run-time Service Model Web server is issued by a trusted Certificate Authority (CA), it is most likely that you do not have to perform the following procedure.

During authentication, BSM running an RTSM sends its certificate to the Data Flow Probe client machine, and the Data Flow Probe sends its certificate to BSM running an RTSM.

 1 Download CA root certificate, encoded in base-64, and save it with the following name: **c:\cacert.cer**

 2 Import the Certificate Authority certificate into the DFM Java truststore by running the following command:

```
C:\hp\UCMDB\DataFlowProbe\jre\bin>keytool -import -trustcacerts -alias
ddmTrustedCA -keystore ..\lib\security\cacerts -file c:\cacert.cer
```

 a Type the following keystore password: **changeit**

 b When asked **Trust this certificate?**, enter **yes**.

 3 Create a keystore by running the following command:

```
C:\hp\UCMDB\DataFlowProbe\jre\bin>keytool -genkey -keyalg RSA -alias ddmkey -
keystore
C:\hp\UCMDB\DataFlowProbe\root\lib\security\client.keystore
```

 a Choose your password and enter your details.

 Important: Enter the full hostname for **first and last name**.

 b When asked, **Is CN=... correct?** type **yes**.

 c Press ENTER to set the same password for the key.

 4 Create a certificate request for CA to sign by running the following command:

```
C:\hp\UCMDB\DataFlowProbe\jre\bin>keytool -certreq -alias ddmkey -file c:\ddm.csr  -
keystore
C:\hp\UCMDB\DataFlowProbe\root\lib\security\client.keystore
```

 Enter the keystore password.

 5 Submit the **c:\ddm.csr** file to your Certificate Authority and acquire a signed client certificate in base-64 encoding.

 6 Import the CA certificate into the keystore by running the following command:

```
C:\hp\UCMDB\DataFlowProbe\jre\bin>keytool -import -alias ddmTrustedCA -file
c:\cacert.cer -keystore
C:\hp\UCMDB\DataFlowProbe\root\lib\security\client.keystore
```

Enter the keystore password and when asked **Trust this certificate?**, enter **yes**.

7 Import the client certificate into the keystore by running the following command:

```
C:\hp\UCMDB\DataFlowProbe\jre\bin>keytool -import -alias ddmkey -file
c:\<SIGNED_CERT> -keystore
C:\hp\UCMDB\DataFlowProbe\root\lib\security\client.keystore
```

Note: **<SIGNED_CERT>** is the full path to the certificate acquired in step 5 on page 516 above.

Make sure that the output message is **Certificate** reply **was installed in keystore**.

8 List the contents of the keystore by running the following command:

```
C:\hp\UCMDB\DataFlowProbe\jre\bin>keytool -list -keystore
C:\hp\UCMDB\DataFlowProbe\root\lib\security\client.keystore
```

   a Enter the keystore password.

   b Verify that the output includes both **keyEntry** and **trustedCertEntry**.

9 Change the **ssl.properties** file, located in the **C:\hp\UCMDB\DataFlowProbe\root\lib\security** folder:

   a Update the keystore and truststore file names to point to the files you created previously:

```
# Path to Keystore and Truststore files
javax.net.ssl.keyStore=C:\hp\UCMDB\DataFlowProbe\\root\\lib\\security\\client.keyst
ore
javax.net.ssl.trustStore=C:\hp\UCMDB\DataFlowProbe\\jre\\lib\\security\\cacerts
```

(Note the double backslashes.)

517

    b Update the keystore and truststore passwords:

        ➤ You encrypt the password through the Probe's JMX console: Launch a Web browser and enter the following address: **http://<Data Flow Probe machine name or IP address>:1977**. If you are running the Data Flow Probe locally, enter **http://localhost:1977**.

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

        ➤ Locate the **Type=MainProbe** service and click the link to open the JMX MBEAN View page.

        ➤ Locate the **getEncryptedKeyPassword** operation.

        ➤ Enter your keystore or truststore password in the **Key Password** field and click **getEncryptedKeyPassword**.

        ➤ Open the **ssl.properties** file in the following folder: **C:\hp\UCMDB\DataFlowProbe\root\lib\security**.

        ➤ Copy and paste the encrypted password (numbers separated by commas, for example, 1,2,3,4,5) into the relevant keystore or truststore line of the **ssl.properties** file.

        ➤ Save the file.

10 Update the C:\hp\UCMDB\DataFlowProbe\root\lib\collectors\ DiscoveryProbe.properties file:

    a Change the **appilog.agent.probe.protocol** parameter to **HTTPS**.

    b Make sure the **serverPortHttps** value is **443**.

11 Restart the Data Flow Probe.

⚒ How to Configure SSL from the Data Flow Probe to the Gateway Server

When a session is started between the Data Flow Probe and the Gateway Server, the Gateway Server sends the Probe a server-side certificate that was issued by a Certification Authority (CA) recognized by the Gateway Server. The Data Flow Probe engine should be configured to trust the certificate or the CA that issued it, and to communicate via SSL.

To configure the Data Flow Probe to connect to the Gateway Server using SSL:

1 Prerequisite: Configure HP Universal CMDB to use SSL.

2 Prerequisite: Install the Data Flow Probe. During installation, enter the name of the HP Universal CMDB Gateway server to which the Probe must report results.

3 If you are working with the Certificate Authority, download the current Certificate Authority certificate to your Data Flow Probe server. Save it to a file, for example, C:\ca.cer.

4 Import this certificate into the Data Flow Probe JVM: **C:\hp\UCMDB\DataFlowProbe\jre\bin** with the following values:

keytool -import -trustcacerts -alias <your alias> -keystore ..\lib\security\cacerts -file <file path and name>

5 Enter the password and click **Yes** to confirm.

6 Set the connection parameters in the Data Flow Probe.

➤ Open the file **%discovery root%\root\lib\collectors\ DiscoveryProbe.properties**.

➤ Configure the URL of the HP Universal CMDB server:

serverName = <HP Universal CMDB Gateway server domain name>

Note: The SSL connection may fail if an IP address is used instead of domain name.

➤ Configure the port number to use for HTTPS:

```
# Ports used for HTTP/s traffic
#serverPort = 80
serverPortHttps = 443
```

➤ Set the schema to be used by the Agent to HTTPS:

```
# Can be either HTTP or HTTPS
appilog.agent.probe.protocol = HTTPS
```

➤ Set the name of the HP Universal CMDB server:

```
# Name of the Server machine to which this probe reports
serverName = <server name either of the reverse proxy or the Gateway server>
```

7 Restart the Data Flow Probe.

Index

Index