HP Universal CMDB

For the Windows, Red Hat Enterprise Linux, and Oracle Enterprise Linux operating systems

Software Version: 10.01

Data Flow Management Guide

Document Release Date: December 2012

Software Release Date: December 2012

Legal Notices

Warranty

The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

The information contained herein is subject to change without notice.

Restricted Rights Legend

Confidential computer software. Valid license from HP required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Copyright Notice

© Copyright 2002 - 2012 Hewlett-Packard Development Company, L.P.

Trademark Notices

Adobe™ is a trademark of Adobe Systems Incorporated.

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

UNIX® is a registered trademark of The Open Group.

Documentation Updates

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

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

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

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 Online 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

Contents

Introduction

Chapter 1

Introduction to Data Flow Management

This chapter includes:

Data Flow Management Overview

This section gives an overview about the Discovery Control Panel and the Integration Studio.

This section includes:

- "Integrations" below
- "Discovery" below
- "Data Flow Management Modules" on next page
- "Reconciliation" on page 20

Integrations

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

You can set up the following types of integrations:

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

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

To learn more, see "Integration Studio" on page 179.

Discovery

The Discovery process is the mechanism that enables you to collect information about your IT infrastructure resources and their interdependencies. Discovery automatically discovers and maps

logical application assets in Layers 2 through 7 of the Open System Interconnection (OSI) Model.

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

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

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

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

Data Flow Management Modules

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

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

Integration Studio

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

For more information, see "Integration Studio" on page 179.

Discovery Control Panel

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

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

For more information, see "Introduction to Universal Discovery" on page 238.

Data Flow Probe Setup

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

covers.

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

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

For more information, see "Data Flow Probe Setup" on page 27.

Reconciliation Priority

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

For more information, see "Reconciliation Priority" on page 496.

Adapter Management

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

For more information, see "Adapter Configuration" on page 124.

Universal Discovery Community

The Universal Discovery Community Web site provides you with a convenient way to obtain the latest Discovery and Integration Content Pack. The Content Pack provides all of the out-of-the-box discovery packages and integration adapter required for performing discovery and integrating with external sources.

For more information, see "Universal Discovery Community" on page 24.

Data Flow Probe Status

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

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

For details, see "Data Flow Probe Status" on page 117.

Reconciliation

The Reconciliation process consists of two important steps:

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

different integrations, the CMDB reconciliation engine resolves the conflict by looking at the reconciliation priority assigned to each integration.

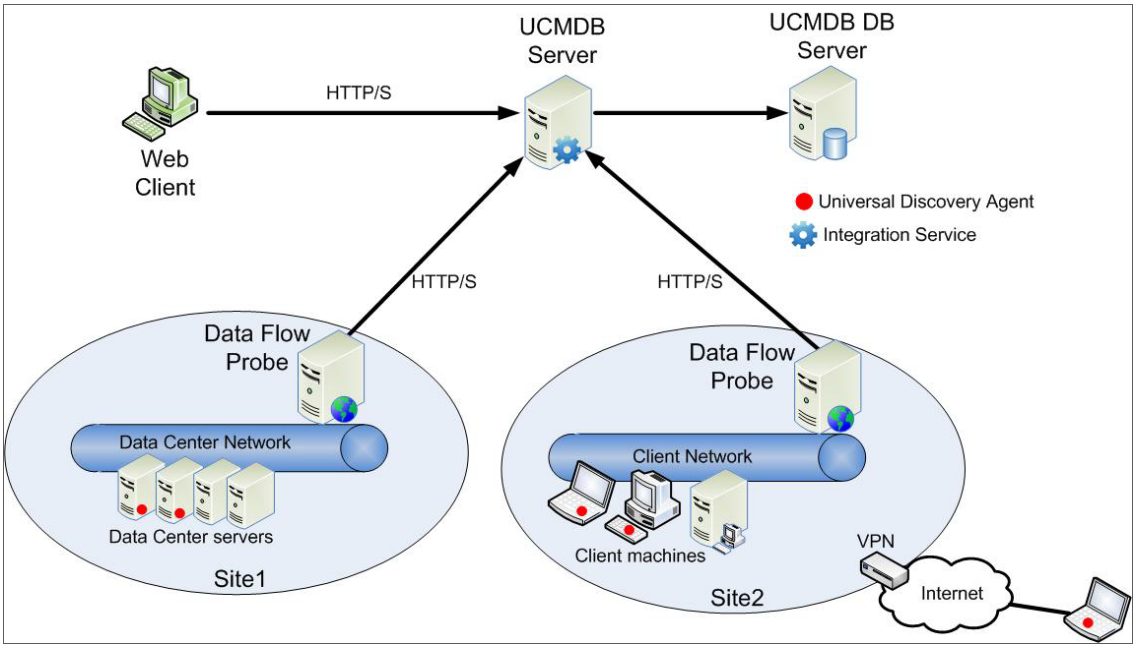
By default, unless you customize the reconciliation priorities within the Reconciliation Priority Manager, the CMDB reconciliation engine uses the last reported value as the most accurate, that is, all integrations have exactly the same priority.

For more information about reconciliation, see "Entity Reconciliation" on page 479.

For details about the Reconciliation Priority Manager, see "Reconciliation Priority Window" on page 502.

Data Flow Management Architecture

Data Flow Management architecture is deployed as follows:



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

Universal Discovery Concepts

This section describes the main topics of Universal Discovery:

Data Flow Probe

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

process.

Passive Discovery Probe

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

Communication Protocols

Discovery of the IT infrastructure components uses protocols such as SNMP, WMI, JMX, Telnet, and so on for communication. For details about each protocol, see the *HP Universal CMDB Discovery and Integration Content Guide*.

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 Create Jython Code in the *HP Universal CMDB 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 *HP Universal CMDB 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 *HP Universal CMDB 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 *HP Universal CMDB 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 correctly, adapters require further context information, which can include an IP address, port information, credentials, and so on.

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

For details on making adapter changes, see "Adapter Management Window" on page 149. For details on creating adapters, see Adapter Development and Writing in the *HP Universal CMDB Developer Reference Guide*

Input Queries

> **Note:** Input queries refer only to discovery-based integrations.

Each discovery-based integration adapter is assigned an input query that is used as follows:

- **The input query defines a minimal set of requirements** for every Trigger CI included in a 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, that is, only IPs with installed SNMP agents can trigger this adapter. This prevents the case where a user could manually create a Trigger CI that adds all IPs as triggers to an adapter.

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

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

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

Discovery Modules

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

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

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

Discovery and Integration Content Packs

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

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

Integration Points

Integration points are entities used to set up UCMDB integrations. Each integration point is created with a selected integration adapter and the additional configuration information required to set up the integration. For details on creating integration points, see "Integration Studio" on page 179.

Discovery Jobs

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

Management Zones

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

You can set up multiple Management Zones to run different instances of a Discovery activity in different Data Centers in your enterprise.

For information, see "Zone-Based Discovery" on page 242.

Discovery Activities

You use one of the discovery activities to discover infrastructure (IPs, nodes), basic software (shallow running software including application servers, databases, and web servers), deep database configuration, and inventory (for example, CPUs, installed software, logical volumes), among other information within Management Zone.

Agent-Based Discovery

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

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

Agentless Discovery

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

Trigger CIs and Trigger Queries

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

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

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

Universal Discovery Community

The Universal Discovery Community (https://hpln.hp.com//group/universal-discovery/) on the HP Live Network provides customers with a convenient way to obtain the latest HP UCMDB

Discovery and Integration Content Packs and related documentation.

Note: You need an HP Passport user name and password to log in to this site.

Data Flow Management Setup

Chapter 2

Data Flow Probe Setup

This chapter includes:

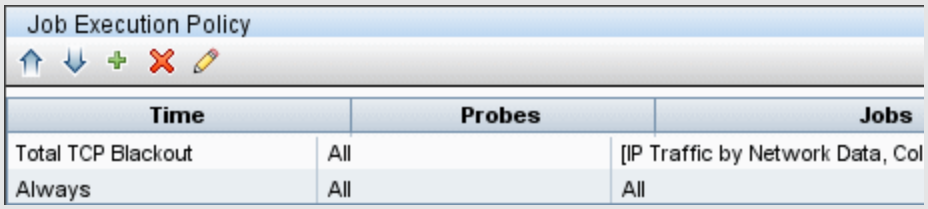
Job Execution Policies

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.

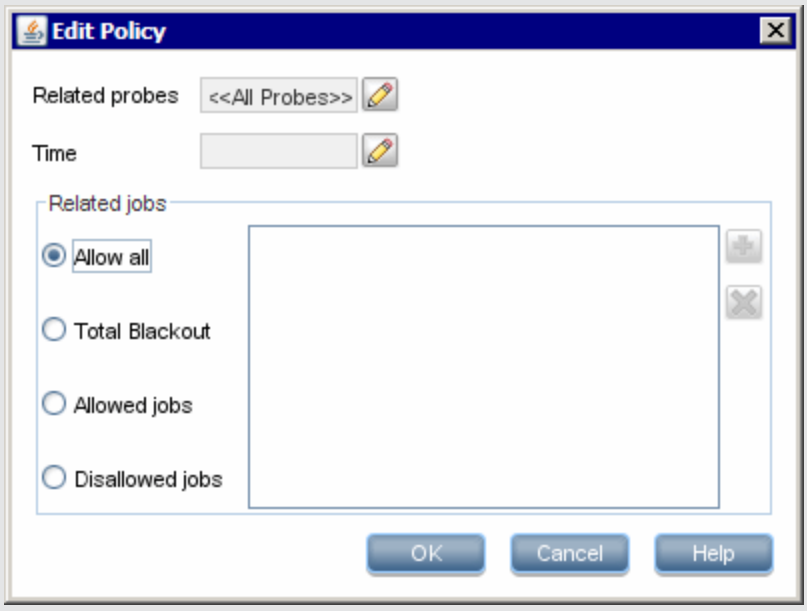
For details on defining a job execution policy, see "New/Edit Policy Dialog Box" on page 66.

Example of Policy Ordering

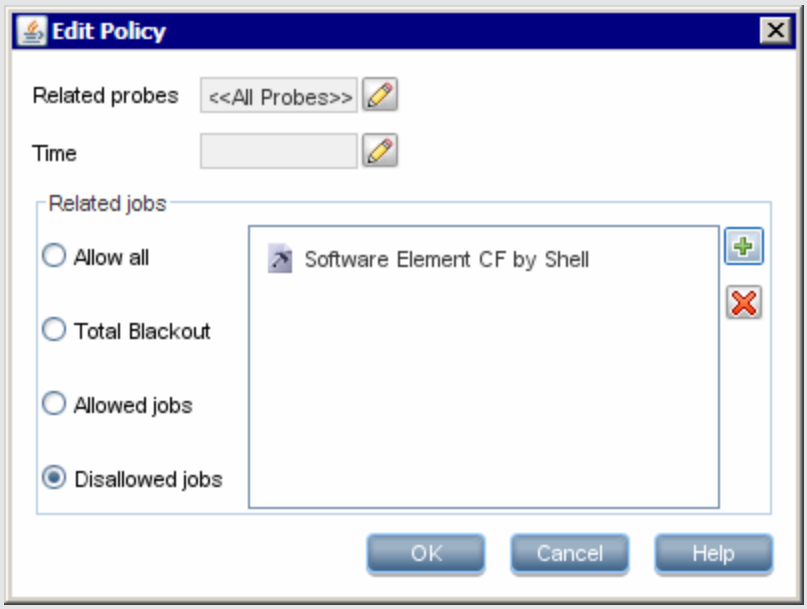
Say there are two policies, **Total TCP Blackout** and **Always** (the out-of-the-box policy). **Total TCP Blackout** does not allow any TCP discovery jobs to run. The policies appear in the list as follows:



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

After discovery or integration, results are processed, each one verifying a different aspect of the outgoing discovery result - class model validation, redundant results validation, and so on. This is called the **result processing chain**.

This section includes:

- "Class Model Data Validation" below
- "Content Data Validation" on next page

Class Model Data Validation

The CIT model resides on the Data Flow Probe (as well as in the CMDB). This enables data validation to take place on the Probe when receiving data from services. Problems are generated for a specific Trigger CI and displayed to the user.

The following validation takes place on the Probe:

- The CIT of the CI is compared to that in the CIT model.
- The CI is checked to verify that all key attributes are present (on condition that the `CmdbObjectId` attribute is not defined).
- The CI's attributes are checked to verify that they are all defined in the CIT.

All invalid attributes raise an error, which reports on a specific CI. When the Probe finds invalid data that is related to the CITs, all data that the Probe has collected on that CI is dropped by the Probe and is not sent to the server.

See also: "Server-Side Data Normalization" on page 506.

For details on attributes, see CI Type Attributes in the *HP Universal CMDB Modeling Guide*.

Content Data Validation

Content that comes out-of-the-box with the Discovery and Integration Content Pack uses standard libraries. However, user-defined packages might not be compatible with the standard APIs and can send invalid data to the UCMDB server.

To provide strong validation for data reported to the UCMDB server, UCMDB allows for additional content data validation before the data is sent to the UCMDB server, and indication of any invalid data. To perform content data validation, you can create validation jython scripts and specify them in the dedicated configuration file, **dataValidationlibs.xml**.

The Content Data Validation module loads and executes sets of jython scripts defined in the **dataValidationlibs.xml** file. The content data validation jython scripts should contain the **ValidateData** function, which is the entry point for data validation execution.

For details about how to configure the content data validation jython scripts, and for some examples, see "Content Data Validation Jython Scripts" on page 57.

To enable or disable Content data validation in UCDMB, see "How to Enable Content Data Validation" on page 42.

Filtering Results

You can filter results sent by the Probe to the HP Universal CMDB server. You would probably need to filter irrelevant data regularly during production runs and specifically when you are testing a limited environment.

There are two levels of filtering: adapter filtering 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 144.
- **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 134.

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.

How to Start the Data Flow Probe

This section explains how to start the Data Flow Probe running on a Windows platform.

Note:

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

This task includes the following steps:

- "Prerequisite" below
- "Start the Probe " below

Prerequisite

- Ensure that the Data Flow Probe is installed on a Windows machine. For details, see the interactive *HP Universal CMDB Deployment Guide*.
- Ensure that UCMDB is installed and running.

Start 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 HP Universal CMDB select **Data Flow Management > Data Flow Probe Setup**. Select the Probe and, in the Details pane, verify that the status is **connected**.

- **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.

How to Stop the Data Flow Probe

- To stop the Probe when it is running as a service, select **Start > Programs > HP UCMDB > Stop Data Flow Probe**.
- To stop the Probe when it is running in a command prompt window (the console), press **CTRL+C**, then **y**.

How to Add a Data Flow Probe

This task describes how to add a Probe to UCMDB.

This task includes the following steps:

- "Prerequisites" below
- "Add a domain to UCMDB" below
- "Add a Data Flow Probe to the new domain" below
- "Add more Probes to the domain – optional" below
- "Define credentials" below

1. ### Prerequisites

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

2. ### Add a domain to UCMDB

   In this step, you create the domain for the new Probe. When you start the Probe, it connects to UCMDB automatically. To verify, select **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 "New/Edit Range Dialog Box" on page 62.

   a. Access the Probe configuration window: **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 67.

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 68.

   c. Select the new Probe and define its range. For details, see "New/Edit Range Dialog Box" on page 62.

4. ### Add more Probes to the domain – optional

   To add more Probes to this domain, repeat step "How to Add a Data Flow Probe" above.

5. ### Define credentials

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

   For details, see "Data Flow Probe Setup Window - Details Pane" on page 69. For a list of protocols, see the *HP Universal CMDB Discovery and Integration Content Guide*.

How to Define Owner Tenants on Data Flow Probes

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

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

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

1. Prerequisite

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

2. On the Data Flow Probe open the **DataFlowProbe.properties** file, located in the Data Flow Probe's installation folder under **..\UCMDB\DataFlowProbe\conf**.

3. Define the owner tenant parameter by adding the following line:

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

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

4. Save the **DataFlowProbe.properties** file.

5. Restart the Data Flow Probe.

6. Result

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

See also

"Discovered CIs and Relationships In a Multi-Tenancy Environment" on page 239

"Integration in a Multi-Tenancy Environment" on page 182

How to Configure Periodic Data Flow Task Updates

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

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

This section includes:

Global Configuration

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

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

To configure global data flow task updates:

1. Select **Administration > Infrastructure Settings Manager**.
2. Select the **General Settings** category.
   a. Locate **Enable periodic update of data flow tasks** parameter and set the value to **true**.
   b. Locate **Periodic data flow task update interval** and **Periodic data flow task update start time** and specify how often (in hours) to update the data flow tasks, and the time (01-24) at which to start the update.

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

Adapter Configuration

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

Note:

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

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

To configure data flow task updates for a particular adapter:

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

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

   Example:

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

Ad Hoc Updates

To run ad hoc updates of data flow tasks:

1. Log in to the JMX console.
2. Run one of the following methods, depending on which is relevant:

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

How to Update the Data Flow Probe's IP Address

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

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

To change the IP address of a Data Flow Probe:

1. ### Update the Probe properties

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

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

  For more details about these properties, see "DataFlowProbe.properties Parameters" on page 45.
- Open the **probeMgrList.xml**, locate the line that starts with `<probeMgr ip=` and update the Probe Manager machine name or IP address, for example:

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

2. **Stop the Probe**
   - To stop the Probe when it is running as a service, select **Start > Programs > HP UCMDB > Stop Data Flow Probe**.
   - To stop the Probe when it is running in a command prompt window (the console), press CTRL+C, then **y**.
3. **Run the clearProbeData script**

   In **C:\hp\UCMDB\DataFlowProbe\tools** run **clearProbeData.bat**.
4. **Restart the Probe**
   - To restart the Probe from the Start window, see "Start the Probe " on page 31.
   - To restart the Probe in a console, see "In a Console" on page 31.

How to Update the Data Flow Probe Memory Size

The Data Flow Probe Memory Size is defined during installation.

This task describes how to change the maximum heap size..

1. Open the **WrapperEnv.conf** located in **C:\hp\UCMDB\DataFlowProbe\bin**
2. Update the following parameters:
   - **set.GATEWAY_MAX_MEM**
   - **set.MANAGER_MAX_MEM**

   Note: For Probes on Linux machine, update only **set.GATEWAY_MAX_MEM**
3. Restart the Data Flow Probe process.

How to Deploy a Data Flow Probe CUP

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

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

1. In Data Flow Management, go to the Data Flow Probe Setup module.
2. Click the **Deploy Probe Update**  button.
3. Select a CUP version to deploy, and click **OK**.

Note:

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

How to a Deploy Data Flow Probe CUP Manually

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

1. **Prerequisite:** To avoid loss of data, deactivate all discovery jobs before running the update.
2. Stop the Data Flow Probe.
3. Copy the Probe Upgrade ZIP file, located in the root folder of the HP Universal CMDB Setup Windows DVD as follows:

   Windows:

File on DVD	**probe-patch-**<*UCMDB version*>**.CUP**<*CUP#*>**-**<*Build_number*>**-windows.zip**
Destination Location	C:\hp\UCMDB\DataFlowProbe\runtime\upgrade\

   Linux:

File on DVD	**probe-patch-**<*UCMDB version*>**.CUP**<*CUP#*>**-**<*Build_number*>**-linux.zip**
Destination Location	/opt/hp/UCMDB/DataFlowProbe/runtime/upgrade

4. Extract the upgrade package:

Operating System	Upgrade Package File
Linux	Run **/opt/hp/UCMDB/DataFlowProbe/tools/upgrade/extractUpgradePackage.sh**
Windows	**C:\hp\UCMDB\DataFlowProbe\tools\upgrade\extractUpgradePackage.bat**

5. Start the Data Flow Probe.
6. In Data Flow Management, in the Data Flow Probe Setup module, verify that the Probe is connected and that the Probe version is updated. For details, see "Data Flow Probes Pane" on page 70.

Note: If this process fails, uninstall the Probe, reinstall a new Probe, and then deploy the relevant Probe CUP.

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

For details on deploying a Probe CUP from the Data Flow Probe Setup module, see "How to Deploy a Data Flow Probe CUP" on page 36.

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

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

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

Note:

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

To align the Data Flow Probe CUP version:

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

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

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

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

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

Example

Consider the following deployment:

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

Aligning the CUP versions will have the following effect:

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

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

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

How to Uninstall Probe CUPs Manually

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

To uninstall a Probe CUP manually:

1. Stop the Probe.
2. Copy **${PROBE_INSTALL}\UninstallCUP\CUP_NUMBER\ probeUninstallCup<*CUP_number*>.zip** to the **${PROBE_INSTALL}\runtime\upgrade** directory.
3. From the command prompt, navigate to the **${PROBE_INSTALL}\tools\upgrade** directory.
4. Run:
   - **Windows: extractUpgradePackage.bat**
   - **Linux: extractUpgradePackage.sh**
5. Ensure that the CUP resource was remove from UCMDB so that it is not deployed again:
   a. In **Administration > Package Manager**, select the **probeUpdate** package, and click **Undeploy Resources**  .
   b. In the Undeploy Package Resources dialog box that opens, if the CUP resource is displayed, select it.
   c. Click **Next** and then **Finish**.

How to 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 126.

1. **Select the CIs to be deleted**
   a. Select an adapter.
   b. In the **Adapter Configuration** tab > **Results Management** pane, 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 153.
   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. **Results**
   To view the deleted CIs, access the Deleted column in the Discovery Results pane. For details, see "Results Pane" on page 293.

How to Configure Number of Connections to Other Machines

This task describes how to configure the number of connections per second that a Data Flow Probe is allowed to create to other machines. You configure these settings in the globalsettings.xml file

which is located in the Adapter Management module under **Resources pane > Packages > AutoDiscoveryContent > Configuration Files.**

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

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

Property	Description
maximumConnectionsPerSecond	Enables limiting the number of new connections per second created by the Probe to other machines. ▪ **0.** Unlimited number of connections allowed. ▪ **> 0.** The maximum number of connections. If this limit is reached, any job trying to create a new connection will wait for a period of time that is determined in the **timeToSleepWhenMaximumConnectionsLimitReached** property (see below) **Default:** 0 (unlimited)
timeToSleepWhenMaximumConnectionsLimitReached	Determines how long (in milliseconds) a job needs to wait until a new connection can be created, assuming the "maximumConnectionsPerSecond" limit has been reached. **Default:** 1000 milliseconds (1 second) **Note:** If **maximumConnectionsPerSecond = 0** this property is ignored.

2. Save your changes.

How to Delete Unsent Probe Results

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

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

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

   Note: If you have not created a user, use the default user name **sysadmin** and the password **sysadmin** 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.

How to Enable Content Data Validation

This task describes how to enable or disable the execution of content data validation.

1. In the **DataFlowProbe.properties** file (located in **c:\hp\UCMDB\DataFlowProbe\conf**), set the **appilog.agent.local.process.result.dataValidation.content** parameter as follows:
   - **true.** Enables content data validation (default)
   - **false.** Disables content data validation
2. Restart the Probe to update the changes.
3. If you are enabling validation, ensure that your content data validation configuration file, **dataValidationlibs.xml**, is defined with the necessary Jython and library scripts. For details, see "Content Data Validation Jython Scripts" on page 57.

For more information about Content Data Validation, see "Content Data Validation" on page 30.

Note: The value given to the **appilog.agent.local.process.result.dataValidation.content** parameter in the DataFlowProbe.properties file can be overridden on an adapter level by adding the **\"enableContentDataValidation\"** parameter to the adapter parameters. If this parameter is absent among the adapter parameters (by default), the value defined in the DataFlowProbe.properties file is used.

Data Flow Probe Process Ports

Data Flow Probe Machine Ports

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

Port	Description
1977	Data Flow Probe's web application port. Used for JMX console and other web services.
1978	If the Data Flow Probe is installed in separate mode (Probe Manager and Probe Gateway are running in separate processes), this port is used by the Probe Manager process for the web application port (Manager's JMX console).
8453	Data Flow Probe's secured web application port. Same as 1977, and is used for the JMX console and other web services if the Jetty HTTPS mode is enabled. Also used to redirect Credential Manager requests when the Data Flow Probe is installed in separate mode.
8454	If the Data Flow Probe is installed in separate mode and Jetty HTTPS mode is enabled, this port is used by the Probe Manager process for the web application port (Manager's JMX console).
1741	Port opened by the Probe Gateway to enable RMI (Remote Method Invocation) between Gateway and Managers.

Port	Description
1742	Port opened by the Probe Manager to enable RMI (Remote Method Invocation) between Gateway and Managers.
80	Opened by a CallHome service for Universal Discovery Agents.

Remote Machine Ports

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

Port	Description
8080	Data Flow Probe uses this port to communicate with the UCMDB server (if the communication is configured to HTTP).
8443	Data Flow Probe uses this port to communicate with the UCMDB server (if the communication is configured to HTTPS).
22	Used for SSH-based discovery.
23	Used for Telnet-based discovery.
80	Used for HTTP, NNM, PowerShell, UDDI, VMware VIM discoveries.
135, 137, 138, 139 + DCOM ports	Used for WMI and NTCMD discoveries.
161	Used for SNMP discovery.
389	Used for LDAP discoveries.
1521, 1433, 6789, 3306, 2048	Used for SQL (Database)-based discoveries.
2738, 7738	Used for Universal Discovery Agent-based discoveries.
443	Used for UDDI, PowerShell discoveries.
280	Used for HP SIM discovery.
1099	Used for JBoss discovery.
5985, 5986	Used for PowerShell discoveries. **Note:** These ports depend on the Microsoft Windows operating system configuration.
3200, 3300-3303, 33xx, where xx is the SAP server instance number	Used for SAP discovery.

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

DataFlowProbe.properties File

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

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

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

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

- **Server Connection Definitions.** Contains parameters that are needed to set up the connection between the server and the Probe, such as the protocol to be used, machine names, default Probe and domain names, time-outs, and basic authentication.
- **Data Flow Probe Definitions.** Contains parameters that define the Probe, such as root folder location, ports, and Manager and Gateway addresses.
- **Probe Gateway Configurations.** Contains parameters that define time intervals for retrieving data.
- **Probe Manager Configurations.** Contains parameters that define Probe Manager functionality, such as scheduled intervals, touching, result grouping, chunking, threading, time-outs, filtering, and reporting multiple updates.
- **I18N Parameters.** Contains parameters that define language settings.
- **Internal Configurations.** Contains parameters that enable DFM to function efficiently, such as thread pool size.

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

DataFlowProbe.properties Parameters

This section describes the DataFlowProbe.properties file parameters.

These include:

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. DownloadingTimeout	Timeout in ms. for download configuration files and userExt files (that is, serverData files).	long	Default: 300000
appilog.agent.probe.protocol	Defines the protocol used to communicate between the Probe Gateway and the 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

Parameter Name (A-Z)	Purpose	Type	Value Description
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.
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 (that is, 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.probe.name	The Probe Gateway name used for identification by the UCMDB server The server uses this name to pass tasks to the appropriate Probe Gateway.	string	Uses the value defined during installation. The default value is the machine name.

Parameter Name (A-Z)	Purpose	Type	Value Description
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
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

Parameter Name (A-Z)	Purpose	Type	Value Description
serverPortHttps	The port number for HTTPS communication.	int	Default: 8443

Data Flow 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 (that is, 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 (that is, **getEncryptedKey Password** operation in **MainProbe** MBean).
appilog.agent.local.jdbc.driver appilog.agent.local.jdbc.uri	Probe Manager database info	string string	**Default:** com.mysql.jdbc.Driver **Default:** jdbc:mysql://localhost/probeMgr?autoReconnect=true
appilog.agent.netflow.jdbc.uri	Netflow database info	boolean	jdbc:mysql://localhost/netflow?autoReconnect=true&jdbcCompliantTruncation=false

Parameter Name	Purpose	Type	Value Description
appilog.collectors.probeLocalUnion	**true**: Probe GW process should also run a Probe Manager on same JVM. **false**: Probe manager runs separately	boolean	**Default:** true
appilog.collectors.ProbeUseSpecificRMIPortFrom	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 separate 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.storeDomainScopeDocument	**true**: Encrypted DomainScope document is stored on file system and internal DB. **false**: Encrypted DomainScope document is retrieved from server each startup and stored only in memory.	boolean	**Default:** true
appilog.collectors.local.ip 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. saveResultsInBKPTable	**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**
appilog.agent.probe. restartProbeAfterJarDownload.interval	Downloaded jar file resources can cause the Data Flow Probe to restart before all the other resources of an adapter package have downloaded. This parameter prevents the restart from occurring.	long	Default: **180000 msec** (3 minutes) **Note:** The delay until a restart on the first resource download (that is, for a first start or after clearing the Probe data) is 10 milliseconds.

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 bool- ean	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.services. maxRemoteProcessesPerJob	The maximum number of remote processes per job that are allowed to run simultaneously.	int	**Default:** 3

Parameter Name	Purpose	Type	Value Description
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
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

Parameter Name	Purpose	Type	Value Description
appilog.agent. local.services.poolThreads appilog.agent.local.services. defaultMAxJobThreads appilog.agent.local.services. adHocMaxThreads	Maximal number of concurrent threads allocated for the multi-threaded job's execution activity. Maximal number of concurrent threads running on a specific job. Maximal number of threads for ad-hoc tasks.	int int int	**Default:** 80 **Default:** 8 **Default:** 20
appilog.agent. local.process. result.data Validation. validLinks	**true** - validate links are legal. **false** - do not validate links.	bool-ean	**Default:** true
appilog.agent. local.process. result. filter Redundant	**true** - filter results which have been already sent to server. **false** - disable filter.	bool-ean bool-ean	Default: **true** Default: **true**
appilog.agent. local.discovery AnalyzerFrom Eclipse	**True:** DiscoveryAnalyzer is executed from Eclipse. **False:** DiscoveryAnalyzer is not executed from Eclipse.	bool-ean	Default: **false**
appilog.agent .local.maxTask ResultSize	Chunk maximal size of results being sent to the server.	int	Default: **20000** **Note:** Lowering this value lowers the number of CIs sent to the CMDB in a single bulk.
appilog.agent. local.probe.restart.interval	Interval (in msec) before auto-restarts of the Probe Manager.	long	Default: **900000**

Parameter Name	Purpose	Type	Value Description
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.filterRedundant** 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.warnOn MultiUpdate	**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. DefaultResultGroupMaxObjs appilog.collectors.probemgr. DefaultResultGroupMinTime	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 long	Default: **5000** Default: **30000** (in ms.) Relation between two keys: **OR**
appilog.agent.probe. touchWindowMechanism.isActive	The touch window defines the period when touch process is allowed . The parameter defines whether the touch window mechanism is active.	bool- ean	Default: **false**
appilog.agent.probe. touchWindowMechanism.startTime	Defines the time, in hours and minutes, when the touch window starts	string	Format: HH:MM Values: 00:00-23:59 Default: **00:00**
appilog.agent.probe. touchWindowMechanism.endTime	Defines the time, in hours and minutes, when the touch window ends	string	Format: HH:MM Values: 00:00-23:59 Default: **23:59**

Parameter Name	Purpose	Type	Value Description
com.hp.ucmdb.-discovery.probe.agents.probemgr.xmlen-richer.activateSecondaryXmlEnricher	Indicates whether the second XML Enricher service is activated for increased scan file processing power. **true.** Both the primary and secondary XML Enricher services process the incoming scan files. **false.** Only the primary XML Enricher service processes the incoming scan files	bool-ean	Default: **false** **Note:** Modifying this value in the **Data-Flow-Probe.properties** file requires restarting the Data Flow Probe. Therefore, it is recommended to activate this feature using the JMX Console. For details, see "How to Increase Scan File Processing Power" on page 353.

I18N Parameters

Parameter Name	Purpose	Type	Value Description
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

Content Data Validation Jython Scripts

The Content Data Validation Jython scripts are divided into main scripts and library scripts. Each "main" script must have the **ValidateData** function which is the entry point for the execution of data validation. The **ValidateData** function has the following parameters:

- **TaskResults.** Provides the API accessing data objects.
- **Environment.** Provides the API for accessing Environment information, such as the Probe Gateway name, the Probe Gateway IP, and the domain name.

The **dataValidationlibs.xml** file is a configuration file where you define which scripts to execute and which to execute as libraries. The file is divided into sections which logically define the data validation execution.

Example of the dataValidationlibs.xml File

```
<datavalidation parserClassName="com.hp.ucmdb.discovery.
library.communication.downloader.cfgfiles.
ContentDataValidationConfigFile">

        <script name="dataValidator1.py">

                <library name="validator1.py"/>

                </script>

        <script name="dataValidator2.py" cit="Node,Process">

                <library name="validator2.py"/>

                <library name="validator3.py"/>

        </script>

</datavalidation>
```

where:

- **validator<x>.py** is a library script.

  Libraries must be ordered according to their dependency. In this example, **validator3.py** uses **validator2.py**, so **validator3.py** appears after first **validator2.py**.

- The **cit** parameter lists the CITs that the script receives for validation. In this example, the **dataValidator2.py** script receives only **Node** and **Process** CITs for validation.

Handling Errors and Warnings

- **addError/addWarning**. Use this API from the TaskResults parameter to attach error/warning to triggered CIs. Bulk is reported to the UCMDB server.
- **raise ContentDataValidationException**. Use to report an error message if the bulk should be discarded.

Example of API Usage

- **Main Script**

```
#dataValidator1.py


import validator1


def ValidateData(TaskResults, Environment):

        logger.info('probe gateway is :', Environment.
getProbeGatewayID())

        logger.info('probe gateway ip is :', Environment.
getProbeGatewayIP())

        logger.info('probe domain is :', Environment.
getProbeManagerDomain())


objectsForUpdate = TaskResults.getResultObjects()

size = objectsForUpdate.size()

  if size > 0:

    for i in range(0, size):

        object = objectsForUpdate.get(i)

        validator1.validate(object, TaskResults)

        if object.getObjectClass() == 'host':

          TaskResults.addError(100, 'host CIT is not in class
model')

  pass
```

- **Library Script**

```
#validator1.py


from com.hp.ucmdb.discovery.library.results.resultprocess import
ContentDataValidationException


def validate(object, TaskResults):

  if object.getAttribute('description') == None:

    TaskResults.addWarning(100, 'No description set for the object
of type ' + object.getObjectClass())
```

```
  if object.getAttribute('host_hostkey') == None:

   // fatal error, all bulk and all previous errors will be removed
from bulk

   // this error will be shown in UI

   raise ContentDataValidationException, 'Attribute host_hostkey is
absent'
```

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.

Log files include:

- "General Logs" below
- "Probe Gateway Logs" on next page
- "Probe Manager Logs" on page 61

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 (that is, the Probe Manager and Probe Gateway are 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

Contains messages that are created following a job execution.

Data Flow Probe Setup User Interface

This section includes:

New/Edit Range Dialog Box

Enables you to set the network range for a Data Flow probe or for a passive discovery 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.

To access	1. Select **Data Flow Management > Data Flow Probe Setup > Domains and Probes > Domain:** 2. **For a Data Flow Probe**: Under Data Flow Probes, select a probe, and in the Ranges pane click the **New range** or **Edit range** button. **For a passive discovery probe**: Under Passive Discovery Probes, select a passive probe, and in the Passive Discovery Integrated Ranges pane click the **New range** or **Edit range** button.
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 Add a Data Flow Probe" on page 32 • "How to Run Module/Job-Based Discovery" on page 275 • "How to Configure Just-In-Time Discovery" on page 476

User interface elements are described below:

UI Element	Description
Definition Type	Choose either IP Range or CIDR. Choose IP Range if you want to use IP addresses to define the probe range; choose CIDR if you want to use the Classless Inter-Domain Routing (CIDR) method to define the probe range. **Available:** New Range dialog box only

UI Element	Description
Range	Enables you to select the range over which the Probe should perform discovery. Depending on which definition type you choose, you define the range either according to IP addresses or according to the CIDR method. Using the CIDR method, each IP address has a network prefix that identifies either an aggregation of network gateways or an individual gateway. The length of the network prefix is also specified as part of the IP address and varies depending on the number of bits that are needed. • **IP Addresses.** Define a range of IP addresses using the following rules: ▪ The IP address range must have the following format: `start_ip_address – end_ip_address` For example: `10.0.64.0 - 10.0.64.57` ▪ The first decimal value (octet) of the start IP and end IP must be identical. For example, **`10`**`.1.2.3 - `**`10`**`.2.3.4.` ▪ 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. ▪ For a passive discovery probe, this range must fall within the range of the Data Flow Probe it is reporting to. • **CIDR method.** Define a range according to the CIDR method as follows: a. Enter the IP address. b. In the drop-down, choose the number of bits (from 1-32) to determine the network prefix. For example, if you enter 192.30.250.00/18, 192.30.250.00 is the network address and 18 means that the first 18 bits are the network part of the address, leaving the last 14 bits for specific host addresses.

UI Element	Description
Type. (Data Flow Probe only)	Defines the IP address lease time setting for the range. **Note:** It is important to select the appropriate IP Address type to ensure that discovery is performed as expected. For more information, see "Range Types" on page 504. • **Data Center**: For permanent or long IP address lease times. • **Client**: For short IP address lease times. **Note:** Mac addresses are not captured during a ping sweep discovery job when the setting is Data Center.
Description. (Optional)	A description about the selected range. **Note:** • Maximum number of characters allowed: 150 • No new lines or tabs may be inserted

UI Element	Description
Excluded IP Ranges	Enables you to define a range of IP addresses to exclude from the IP range specified above. **Note:** • The rules for entering an excluded range are the same as for entering a range. For details, see IP Range above. • When a Probe range is defined in CIDR format, the excluded ranges must still be defined in the IP range format (xxx.xxx.xxx.xxx - xxx.xxx.xxx.yyy)  . **New Excluded IP Range.** Enables you to define a range of IP addresses to exclude, and enter a description about the excluded range if desired.  . **Delete Excluded IP Range.** Deletes an excluded IP range.  . **Edit Excluded IP Range.** Enables you to edit a defined excluded IP range. **Example:** Use this feature to divide a network range into several sub-ranges. 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
Ports	Enables you to define ports over which passive discovery should be performed within the defined IP address range: • **All available ports.** Enables passive discovery over all available ports. • **Selected ports** Enables passive discovery over ports that you select from the Global Ports List. Click  to select ports to monitor. **Available:** When defining an IP address range for a passive discovery probe only.

New/Edit Policy Dialog Box

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

To access	**Data Flow Management > Data Flow Probe Setup > Domains and Probes > Details pane > Job Execution Policy** section. Select an existing policy and click the **Edit Policy** button , or click the **New Policy** button.
See also	• "Job Execution Policies" on page 28 • "Data Flow Probe Setup Window - Details Pane" on page 69

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 modeled 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.

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 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 "Start the Probe " on page 31 or "In a Console" on page 31.

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.

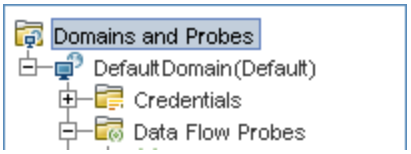
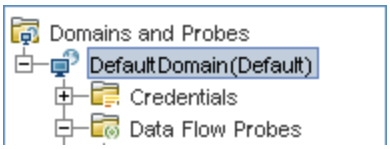
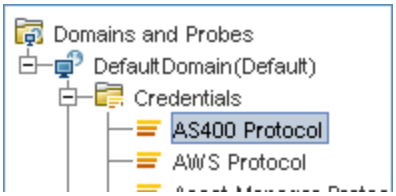
To access	Data Flow Management > Data Flow Probe Setup
Important information	• For details on the Domains and Probes pane, see "Domains and Probes Pane" on page 78. • For details on the Details pane, see "Data Flow Probe Setup Window - Details Pane" below.
See also	Supported Protocols and Supported Agents in the *HP Universal CMDB Discovery and Integration Content Guide*.

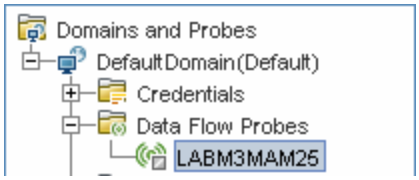
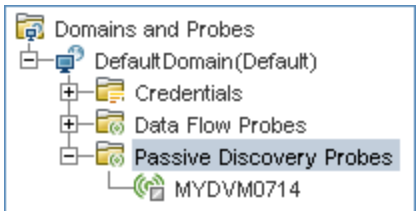
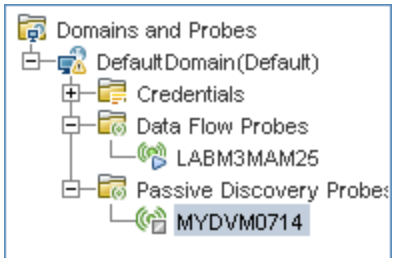
Data Flow Probe Setup Window - Details Pane

Enables you to view the Probes running under all domains and to add an execution policy to jobs.

To access	In the Data Flow Probe Setup window, click an object in the Domains and Probes pane.

Depending on what you select in the Domains and Probes pane, different information is displayed in the Details pane.

If you select...	The information displayed is...
	**Domains and Probes.** You can view details of all Probes and you can define and edit job execution policies. For details, see: • "Data Flow Probes Pane" on next page • "Job Execution Policy Pane" on page 72
	**A specific domain.** You can add a description and view a list of Data Flow Probes and passive discovery probes defined and running in that domain. For details, see: • "Details Pane (Domain)" on page 71 • "Data Flow Probes Pane" on next page • "Passive Discovery Probes Pane" on page 83
	**A specific protocol.** You can add protocol parameters and you can view details on the protocol, including user credentials. For details, see "[Protocol] Pane" on page 73 For a list of supported protocols, see the *HP Universal CMDB Discovery and Integration Content Guide*.

If you select...	The information displayed is...
	**A specific Data Flow Probe.** You can view details of the Data Flow Probe, including range information. You can also add ranges to, or exclude ranges from, the Data Flow Probe, and you can remove a Data Flow Probe from UCMDB. For details, see: • "Details Pane (Probe)" on next page • "Ranges Pane" on page 75
	**Passive Discovery Probes.** You can view and globally configure notification types and verification policies for all passive discovery probes that integrate with the Data Flow Probes of the same domain. For details, see "Passive Discovery Probes Pane" on page 83.
	**A specific passive discovery probe.** Displays the details of a passive discovery probe, including the Data Flow Probe to which it connects, and its IP range information. You can also configure the IP ranges to be monitored by the passive probe, and you can remove a passive probe from the domain. For details, see "Passive Discovery Probe Details Pane" on page 80.

Data Flow Probes Pane

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

To access	In the Domains and Probes pane, do one of the following: • Select **Domains and Probes** • Select **Domains and Probes > *<a domain>***

User interface elements are described below:

UI Element (A–Z)	Description
IP	The main IP address with which the Probe communicates with the UCMDB server.
Last Access Time	The last time that the Probe requested tasks from the server.

UI Element (A–Z)	Description
Name	The name given the Probe when it was added to UCMDB.
Probe Version	The version of the Probe. If the version of the Probe is not compatible with the version of the UCMDB server, this is indicated. Moreover, if the incompatible Probe tries to connect to the UCMDB server, the server sends a shutdown instruction to the Probe. To ensure compatibility, you must upgrade the Probe manually. For details, see the section about manually upgrading the Probe in the *HP Universal CMDB Deployment Guide*.
Status	• **Connected.** The Probe is connected to the server (the Probe connects every few seconds). • **Connected (suspended).** The Probe is connected, but it is suspended such that no jobs can run on the Probe. • **Disconnected.** The Probe is not connected to the server.

Details Pane (Domain)

This pane displays the details of the selected domain.

To access	In the Domains and Probes pane, select **Domains and Probes > <*a domain*>**

User interface elements are described below:

UI Element (A–Z)	Description
Description	The description that was given to the domain when it was defined in UCMDB.
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.

Details Pane (Probe)

This pane displays the details of the selected Data Flow Probe.

To access	In the Domains and Probes pane, select **Domains and Probes > <*a domain*> > Probes > <*a Data Flow Probe*>**

User interface elements are described below:

UI Element (A–Z)	Description
Last time probe accessed UCMDB	The last time that the Probe was accessed on the server machine.
Probe Description	The description given to the Probe when it was added to UCMDB.
Probe IPs	The IPs of the Probe machine. **Note:** If the Probe machine has more than one network card, all the IP addresses are displayed.
Status	• **Connected.** The Probe is connected to the server (the Probe connects every few seconds). • **Connected (suspended).** The Probe is connected, but it is suspended such that no jobs can run on the Probe. • **Disconnected.** The Probe is not connected to the server.
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*.

Job Execution Policy Pane

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

To access	In the Domains and Probes pane, select **Domains and Probes.**
Important information	• The default job execution policy is **Always**. This policy allows all jobs to run on any Probe at any time. • Jobs that have a listening functionality—that is, they do not perform discovery, for example, they listen to SNMP traps—are not included in a policy.
See also	"Job Execution Policies" on page 28

User interface elements are described below:

UI Element (A–Z)	Description
	**Move priority up/down.** Move the priority for 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.
	**New Policy.** Opens the New Policy dialog box, enabling you to add a job execution policy.
	**Remove Policy.** Removes the selected job execution policy. **Note:** If a job affected by the policy is active when the Remove command is executed, UCMDB removes the policy but any of the job's triggers that are currently running remain unaffected.
	**Edit Policy.** Opens the Edit Policy dialog box, enabling you to edit the selected job execution policy.
Jobs	The jobs that are affected by the policy.
Probes	The Probes that are affected by the policy.
Time	The schedule of the policy.

[Protocol] Pane

Enables you to manage protocol connection credentials.

UI Element (A–Z)	Description
	**Create New Connection Details.** Opens the Protocol Parameters dialog box, enabling you to define a connection credential for the selected protocol type. For details, see "Protocol Parameter Dialog Box" on page 85.
	**Remove Connection Details.**Removes the selected connection credential.
	**Edit Connection Details.**Opens the Protocol Parameters dialog box, enabling you to edit the selected connection. For details, see "Protocol Parameter Dialog Box" on page 85.
	**Copy/Move selected credential to another domain.** Enables you to copy/move the selected protocol credential to another domain in the Domains and Probes tree.

UI Element (A–Z)	Description
	**Export Certificate for Manual Agent Deployment.** Enables you to export the Universal Discovery Agent certificate when installing the Universal Discovery Agent manually. For details, see the section about manual Universal Discovery Agent deployment in the *HP Universal CMDB Discovery and Integration Content Guide*. **Available for:** Universal Discovery Protocol only.
	**Move entry up/Move entry down.** Enables you to move credential connections up or down to set the order in which credential sets are attempted. UCMDB tries to connect using all the credential sets in the list with the first set taking priority.
<Protocol connection details>	Displays the defined connection credentials for the protocol type selected in the Domains and Probes pane. The details displayed in this section vary from protocol type to protocol type. For details, see the relevant protocol information as described in the Supported Protocols section in the *HP Universal CMDB Discovery and Integration Content Guide*. All protocol credentials include the following parameters: • **Index.** Indicates the order in which credential instances are selected to make a connection attempt. The lower the index, the higher the priority. **Default:** Credentials are added with an auto-increasing index value. To update the index, use the arrows buttons. • **Scope.** To change the range that a protocol must discover or to select a Probe, click **Edit**. For details, see "Scope Definition Dialog Box" on page 85. **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.

UI Element (A–Z)	Description

<right-click menu>	Choose from the following options:
	• **Edit.** Enables you to enter protocol parameters, such as user name and password, that enable connection to an application on a remote machine.
	• **Edit using previous interface.** Choose this option if:
	  ▪ In a previous version of UCMDB, you added parameters to this protocol that do not exist in this version.
	  ▪ Values in this version cannot be deleted. For example, in this version you cannot configure SQL Protocol credentials with an empty port number. Select this option to open the previous Edit Protocol Parameter dialog box and delete the port number.
	• **Copy/Move to another domain.** Enables you to copy/move the selected protocol credential to another domain in the Domains and Probes tree..
	• **Check credentials.** Opens the Check Credentials dialog box, where you can enter the IP address of the remote machine on which the protocol must run, and specify connection timeout (in milliseconds). The Probe attempts to connect to this IP within the specified timeout and returns an answer as to whether the connection succeeded or not. If the connection is not successful, click **Details** for a description of the error.
	• **Export public certificates.** Opens the Export dialog box, enabling you to export the UD Agent certificate when deploying the UD Agent manually. For details, see the section about manual agent deployment in the *HP Universal CMDB Discovery and Integration Content Guide*.

<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. • **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.

Ranges Pane

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

To access	In the Domains and Probes pane, select **Domains and Probes > *<a domain>* > Probes > *<a Data Flow Probe>***
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 78.

User interface elements are described below:

UI Element (A–Z)	Description
	**New IP Range.** Opens the **New IP Range** dialog box, enabling you to define a new IP range for the selected Probe. For details, see "New/Edit Range Dialog Box" on page 62.
	**Delete IP Range.** Select an IP range and click the button to delete a range from the list. **Note:** You can also delete an excluded IP range.
	**Edit IP Range.** Opens the **Edit IP Range** dialog box, enabling you to edit the selected IP range for the selected Probe. For details, see "New/Edit Range Dialog Box" on page 62. **Note:** You can also edit an excluded IP range.
	**Export Data To File.** Enables you to export the defined ranges in the following formats: • **Excel.** The table data is formatted as an .xls (Excel) file that can be displayed in a spreadsheet. • **PDF.** The table data is exported in PDF format. • **RTF.** The table data is exported in Rich Text Format. • **CSV.** The table data is formatted as a comma-separated values (CSV) text file that can be displayed in a spreadsheet. **Note:** For the CSV formatted table data to display correctly, the comma (,) must be defined as the list separator. In Windows, to verify or modify the list separator value, open Regional Options from the Control Panel, and on the Numbers tab ensure that the comma is defined as the List Separator value. In Linux, you can specify the list separator in the application that opens the CSV file. • **XML.** The table data is formatted as an XML file that can be opened in a text or XML editor. **Tip:** To extract HTML code from the report: ▪ Save the file as HTML ▪ Open the file in an HTML editor ▪ Copy the relevant table into the target file **Note:** Ranges in the CIDR format can also be exported. For an explanation of the CIDR format, see "New/Edit Range Dialog Box" on page 62.

UI Element (A–Z)	Description
	**Import Ranges from CSV File.** Opens the Import Ranges from File dialog box, enabling you to select a CSV file from which to import a set of ranges. Ranges can also be imported according to the CIDR format. For an explanation of the CIDR format, see "New/Edit Range Dialog Box" on page 62. **Note:** Before using this feature, verify that: • the imported file is a valid CSV file The CSV file must be built using exactly the following column names: ▪ **Range.** Specify the range to import. This can be an IP range or in CIDR format. ▪ **Excluded Ranges.** Specify the IP ranges to exclude from the imported range. **Important:** See example below: ○ When defining an excluded IP range, always include the full range in the Ranges column as well. ○ Excluded ranges must always be defined in IP range format, even when excluding the range from a CIDR range. ▪ **Description.** A description of the range ▪ **Type.** The range type: 1 = Client; 0 = Data Center For example: A / B / C / D 1 Range / Excluded Ranges / Description / Type 2 16.60.133.56-16.60.133.75 / / Include IP Range / 1 3 16.60.133.56-16.60.133.75 / 16.60.133.60-16.60.133.65 / Exclude IP Range 1 from IP Range / 4 16.60.133.56-16.60.133.75 / 16.60.133.70-16.60.133.70 / Exclude IP Range 2 from IP Range / 5 16.60.134.56/29 / / Include CIDR / 0 6 16.60.134.56/29 / 16.60.134.56-16.60.134.59 / Exclude IP Range 1 from CIDR / 7 16.60.134.56/29 / 16.60.134.60-16.60.134.61 / Exclude IP Range 2 from CIDR / 8 • the ranges in the CSV file do not conflict with existing ranges, that is, there are no duplicate or overriding ranges.
	**Expand All.** Expands the entire hierarchical tree structure to display all of the defined IP ranges, including the excluded IP ranges.
	**Collapse All.** Collapses the hierarchical tree structure, leaving the top-level IP ranges showing, but hiding excluded IP ranges.
	**Show/Hide Legend.** Shows/Hides the legend for the Ranges pane. •  . Denotes the range of IP addresses included for the selected Probe. •  . Denotes a range of IP addresses to exclude from the defined IP range.

UI Element (A–Z)	Description
<Ranges grid>	The network IP addresses that the Probe uses to discover CIs. For details, see "New/Edit Range Dialog Box" on page 62.

Domains and Probes Pane

Enables you to view, define or edit a domain, connection credentials, Data Flow Probes, and passive discovery probes.

Also enables you to automatically upgrade all the Data Flow Probes with the latest cumulative patch (CUP).

To access	**Data Flow Management > Data Flow Probe Setup**
See also	• "Job Execution Policies" on page 28 • "Data Flow Probe Setup Window - Details Pane" on page 69 • "Passive Discovery Probes Pane" on page 83

User interface elements are described below:

UI Element (A–Z)	Description
	**Add Domain or Probe.** Adds a domain or a Data Flow Probe, depending on what is selected. For details, see "Add New Domain Dialog Box" on page 67 or "Add New Probe Dialog Box" on page 68.
	**Remove Domain or Probe.** Deletes a domain, Data Flow Probe, or passive discovery 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.
	**Reload Domain Information from Server.** Updates all domain, Data Flow Probe, and passive discovery probe information from the server.
	• **Suspend Probe.** Suspends the selected Probe (Data Flow Probe or passive discovery probe) from the UCMDB Server such that no jobs can run. • **Resume Probe.** Resumes the Probe's ability to run discovery and integration jobs. **Note:** When a Probe is suspended, only the ability to run jobs is suspended. All other processes continues to run as usual.

UI Element (A–Z)	Description
	**Deploy Probe Update.** Opens the Deploy Probe Update dialog box, enabling you to automatically update the CUP version of all the Data Flow Probes connecting to the UCMDB Server to the CUP version compatible with the UCMDB CUP version. In the Deploy Probe Update dialog box, navigate to the Probe CUP .zip file. **Note:** • During the CUP deploymentprocess, all compatible Data Flow Probes are automatically restarted. If an integration is running on a Data Flow Probe while it is restarting, the integration stops running, and starts over when the Data Flow Probe restarts. If an integration is almost finished running, or a significant part has already run, to avoid starting the integration over, we recommend letting it complete its run, and, thereafter, updating the CUP.
	**Undeploy Probe Update** Enables you to undeploy CUP versions of the Data Flow Probes connecting to the UCMDB Server, and thereby align them with the CUP version of the UCMDB Server. For details, see "How to Align the Data Flow Probe CUP with the UCMDB Server CUP" on page 38.
<Data Flow Probe status icons>	•  . Indicates that a Probe is connected. •  . Indicates that a Probe is suspended. •  . Indicates that a Probe is disconnected.

Edit Related Probes Dialog Box

Enables you to select specific Probes.

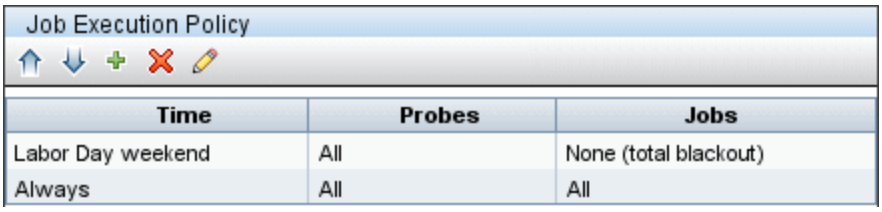
To access	Click the **Related Probes** button  in the Edit Policy dialog box.
See also	"Job Execution Policies" on page 28

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	"New/Edit Policy Dialog Box" on page 66

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.

Passive Discovery Probe Details Pane

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

To access	Select **Data Flow Management > Data Flow Probe Setup.** In the Domains and Probes pane, select a domain, and select a passive probe under **Passive Discovery Probes**.
Important information	The passive discovery probes can be configured to monitor the IP address ranges in the domain of the Data Flow Probe only.
Relevant task	"How to Configure Just-In-Time Discovery" on page 476
See also	• "Just-In-Time Discovery Overview" on page 476 • "Passive Discovery Probes Pane" on page 83

Passive Discovery Probe Details Pane

User interface elements are described below :

UI Element	Description
Name	The name given to the passive discovery probe (RUM Engine) when it was defined in HP RUM.
Data Flow Probe	The name of the Data Flow Probe to which the passive discovery probe reports.
IP	The IP address of the passive discovery probe (RUM Engine) machine.

UI Element	Description
Version	The HP RUM version.
Status	Indicates the status of the passive discovery probe: • **Connected.** The passive discovery probe is connected and available to report information to the Data Flow Probe. • **Suspended.** The passive discovery probe is connected but unavailable to report information to the Data Flow Probe. • **Disconnected.** The passive discovery probe is not connected.
Last access time	The date and time the passive discovery probe was last accessed.

Passive Discovery Ranges Pane

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

User interface elements are described below :

UI Element	Description
Passive Discovery Agent Name	The name of the RUM Probe.
Range	The IP address range defined for the RUM Probe. Information from within this range is reported to the RUM Engine (passive discovery probe). **Note:** The range can be displayed here either according to the IP range format or the CIDR format, as explained in "New/Edit Range Dialog Box" on page 62
Ports	The ports defined for the RUM Probe over which information is reported.

Passive Discovery Integrated Ranges Pane

User interface elements are described below :

UI Element	Description
Use All Ranges Of Data Flow Probe <*Data Flow Probe name*>	Enables passive discovery over all address ranges of the connected Data Flow Probe, over selected ports: • **All available ports.** Enables passive discovery over all available ports. • **Selected ports** Enables passive discovery over ports that you select from the Global Ports List. Click  to select ports to monitor.

UI Element	Description
Use Selected Ranges Of Data Flow Probe <*Data Flow Probe name*>	Enables passive discovery over the Ranges Definition area where you can select existing Data Flow Probe ranges over which to perform passive discovery. See below. **Note:** • Ranges must be a subset of both the connected Data Flow Probe's ranges and Passive Discovery ranges. • Ranges can be displayed here either according to the IP range format or the CIDR format, as explained in "New/Edit Range Dialog Box" on page 62

Ranges Definition Area

User interface elements are described below :

UI Element (A–Z)	Description
	**New Range.** Enables you to define a new range for the passive discovery probe to monitor. **Note:** This range must be a subset of one of the Data Flow Probe's ranges. For details about defining Probe ranges, see "New/Edit Range Dialog Box" on page 62
	**Delete Range.** Enables you to remove a range defined for passive discovery.
	**Select Range** Enables you to select defined ranges for the passive discovery probe to monitor from the ranges defined for the connected Data Flow Probe.
	**Edit Range.** Enables you to modify a selected range. For example, you can select one of the Data Flow Probes ranges, and then exclude some IP addresses from that range for passive discovery.
	**Export Data To File.** **Note:** Not enabled for passive discovery probes.
	**Import Ranges from CSV File.** **Note:** Not enabled for passive discovery probes.
	**Expand All.** Expands the hierarchical tree structure to display all of the defined ranges, including the excluded IP ranges.
	**Collapse All.** Collapses the hierarchical tree structure, hiding excluded IP ranges.

UI Element (A–Z)	Description
	**Show/Hide Legend.** Shows/Hides the legend for the Ranges pane. •  . Denotes a range included for the selected passive discovery probe. •  . Denotes an IP range to exclude from the parent range.
<Ranges grid>	Lists the ranges and ports selected for the passive discovery probe to monitor.

Passive Discovery Probes Pane

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

To access	Select **Data Flow Management > Data Flow Probe Setup.** In the **Domains and Probes** pane, select a domain and select **Passive Discovery Probes.**
Important information	The definitions defined here are valid for all of the passive discovery probes that integrate with the Data Flow Probes of the same domain.
Relevant task	"How to Configure Just-In-Time Discovery" on page 476
See also	"Just-In-Time Discovery Overview" on page 476

Notification Types Pane

Note: By default all types of notifications are enabled.

User interface elements are described below :

UI Element	Description
Report IP notifications	• Reports new IP addresses seen on the network. • Reports unseen IP addresses. ▪ Select the amount of time that the passive probe should wait before triggering a notification that the IP address was not seen. ▪ After this notification is sent, the Data Flow Probe performs a verification. Select an action that should be taken upon verification: ○ set the IP address as a candidate for deletion ○ remove the IP address from UCMDB
Report running software notifications	• Reports new running software seen on the network • Reports unseen running software. ▪ Select the amount of time that the passive probe should wait before triggering a notification that the software is not running. ▪ After this notification is sent, the Data Flow Probe performs a verification. Select an action that should be taken upon verification: ○ set the RunningSoftware CI as a candidate for deletion ○ remove the RunningSoftware CI from UCMDB
Report dependency link notifications	Enables notification of dependency relationships.

Removal Verification Policy Pane

User interface elements are described below:

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

Passive Probes Pane

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

User interface elements are described below:

UI Element (A - Z)	Description
Data Flow Probe	The name of the Data Flow Probe to which the passive discovery probe reports.
IP Address	The IP address of the passive discovery probe (RUM Engine) machine.
Last access time	The date and time the passive discovery probe was last accessed.
Name	The name given to the passive discovery probe (RUM Engine) when it was defined in HP RUM.
Status	Indicates the status of the passive discovery probe: • **Connected.** The passive discovery probe is connected and available to report information to the Data Flow Probe. • **Suspended.** The passive discovery probe is connected but not available to report information to the Data Flow Probe. • **Disconnected.** The passive discovery probe is not connected.
Version	The HP RUM version.

Protocol Parameter Dialog Box

Displays the attributes that can be defined for a protocol.

To access	**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 a description of each protocol, see the *HP Universal CMDB Discovery and Integration Content Guide*.

Scope Definition Dialog Box

Enables you to define ranges of IP addresses 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 316.

UI Element (A–Z)	Description
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 "Ranges Pane" on page 75.

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.** Click to add a Probe to the Selected Probes column.
<	**Remove Selected Probe.** Click to remove 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.

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

Solution. Install the Probe again:

1. (Optional) If you are going to use the same ranges for the Probe in the new domain, export the ranges before removing the Probe. For details, see "Data Flow Probe Setup Window - Details Pane" on page 69.
2. Remove the existing Probe from UCMDB. For details, see the **Remove Domain or Probe** button in "Domains and Probes Pane" on page 78.
3. Install the Probe. For details, see the section about installing the Data Flow Probe in the interactive *HP Universal CMDB Deployment Guide*.

4. During installation, make sure to give the new Probe a different name to the name given to the old Probe, or make sure you delete the reference to Probe from the original domain.

Problem. Discovery shows a disconnected status for a Probe.

Solution. Check the following on the Probe machine:

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

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

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

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

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

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

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

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

Solution: The Probe's CUP version must be the same as UCMDB Server's CUP version. If the CUP versions are not aligned, you must update the Probe's CUP version. To do this, see "How to Deploy a Data Flow Probe CUP" on page 36.

In some cases, the CUP may need to be deployed manually on a Probe. For details, see "How to a Deploy Data Flow Probe CUP Manually" on page 37.

Limitations

- If you reconfigure a Data Flow Probe to work with a different UCMDB server, you must first run the clearProbeData.bat file before you restart the Probe.
- When the Probe is running in separate mode on a machine where both the Gateways and the Manager share same installation folder, the Data Flow Probe CUP must be installed manually. For details, see "How to a Deploy Data Flow Probe CUP Manually" on page 37.
- Data Flow Probe CUPs that were deployed manually can be uninstalled using manual methods only. For details, see "How to Uninstall Probe CUPs Manually" on page 39.

Chapter 3

Universal Discovery Agents

This chapter includes:

Universal Discovery Agent Overview

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

- **Communication**. Performs job scheduling and job execution functions with the Data Flow Probe and with the Scanner.
- **Shell**. Provides a command line interface that provides access to services. The UD Agent uses the Universal Discovery protocol.
- **Software Utilization**. Generates files that contains application utilization data. For more information, see "Software Utilization" on page 338.

The UD Agent generates a **Unique ID** when it is installed on a discovery node. However, if there is a Unique ID already stored on the node, the UD Agent uses the existing Unique ID. Unique ID generation occurs when agent-based and agentless discovery methods are used. Additionally,

generation might also occur when the Inventory Discovery by Scanner job and the Host Connection by Shell job run.

The Unique ID can be utilized as follows:

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

For details about deploying the UD Agent, see "Universal Discovery Agent Deployment" below

Universal Discovery Agent Deployment

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

Deployment Method	Description
Infrastructure Discovery Activity	You can use the Infrastructure Discovery activity to configure and deploy UD Agents. For more information about setting up this activity, see the *HP Universal CMDB Discovery and Integration Content Guide*.
Manual	Third party software distribution tools, scripting, or any remote access technology can be used to deploy and install discovery packages. For more information, see "How to Install Universal Discovery Agent Manually" on page 95.

Supported Platforms

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

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

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

To edit the AgentsSupportMatrix.xml file, see "How to Customize Platforms for Universal Discovery Agent Deployment" on page 93.

Note:

- For a list of out-of-the-box supported platforms and versions for the UD Agent, see the Supported Content section of the *HP Universal CMDB Discovery and Integration Content Guide*. Supported platforms are added based on the growing number of tested platforms and

customer requests.

- Deploying the UD Agent on a platform that is not defined among the supported platforms may result in the UD Agent not functioning properly.

UD Agent Running Modes

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

Running Mode	Description
Complete Install	The UD Agent, software utilization, and Software Identification Tags are installed on the discovery node. **Note:** When you use activities to install discovery packages, this mode is the default.
Software Utilization	Software utilization and Software Identification Tags are installed on the discovery node. Scanners are run manually using third party solutions, scripts, or other remote access technology.

Universal Discovery Agent Certificates

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

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

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

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

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

Using Certificates

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

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

Call Home Overview

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

Note: Call Home is enabled by default.

Traffic Case-Typical

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

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

   - If the Universal Discovery Agent does not receive the acknowledgement message, it sends messages to the Data Flow Probe every hour until an acknowledgement message is received.
   - The acknowledgement message is an HTTP 200 series status message.

3. The Data Flow Probe creates a Node CI, a Call Home Event CI, and a UD Agent CI.
4. The Call Home Event CI triggers the Call Home Processing job.
5. The Call Home Event CI for the Call Home Processing job is sent to the Data Flow Probe.
6. The Call Home Processing job starts.
7. The Call Home Processing job sends a notification message to workflows that are associated with the node and that are waiting to be run. These workflows are also known as **parked workflows**. After the notification message is received, the parked workflow runs. The Universal Discovery Agent continues to send the request message according to the value that is set for the **Call Home Request Frequency** parameter. This parameter is configured when configuring Universal Discovery Agents for deployment. For more information on configuring this parameter, see the section about the Infrastructure discovery activity in the *HP Universal CMDB Discovery and Integration Content Guide*.

Traffic Case-New Node

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

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

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

The acknowledgement message is an HTTP 200 series status message.

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

Traffic Case- Mobile Computer

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

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

FDCC/USGCB Support

Overview

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

Feature Impact

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

Infrastructure Activity. Using this activity to install or upgrade Universal Discovery Agents is not supported. Alternatively, use manual methods to deploy Universal Discovery Agent installation packages to nodes. For details, see "How to Install Universal Discovery Agent Manually" on page 95.

How to Update Security Policy Settings for FDCC

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

This task includes the following steps:

1. "Allow firewall exceptions" on next page
2. "Create firewall exceptions" on next page
3. "Results " on next page

1. Allow firewall exceptions

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

   a. Click **Run** and type **gpedit.msc** to open the Group Policy Editor

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

   c. Double click **"Windows Firewall- Do not allow exceptions"**.

   d. In the **Properties** dialog box, click **Disabled**.

2. Create firewall exceptions

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

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

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

   b. Double click the **"Windows Firewall-Define the Inbound Program Exceptions"**.

   c. In the **Properties** dialog box, click **Enabled**.

   d. Click **Show**.

   e. In the **Show Contents** dialog box, create an entry for the Universal Discovery Agent. Follow the format conventions that are specified in the **Options** pane on the left side.

   > **Note:** Values vary depending on the configuration that you specified when deploying Scanners. The port number of the Universal Discovery Agent is 2738 or 7738. The path of the Universal Discovery Agent is **C:\Program Files\Hewlett-Packard\Discovery Agent\bin32\discagnt.exe**. For more information about Scanners and Scanner parameters, see "Scanner Command Line Parameters and Switches" on page 453.

3. Results

   Verify that the Universal Discovery Agent successfully communicates with the Data Flow Probe by selecting the **Universal Discovery Protocol** in the **Domain and Probes Pane**, and then clicking **Check Credentials**. For more information, see the section on domain credentials in the *HP Universal CMDB Discovery and Integration Content Guide*.

How to Customize Platforms for Universal Discovery Agent Deployment

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

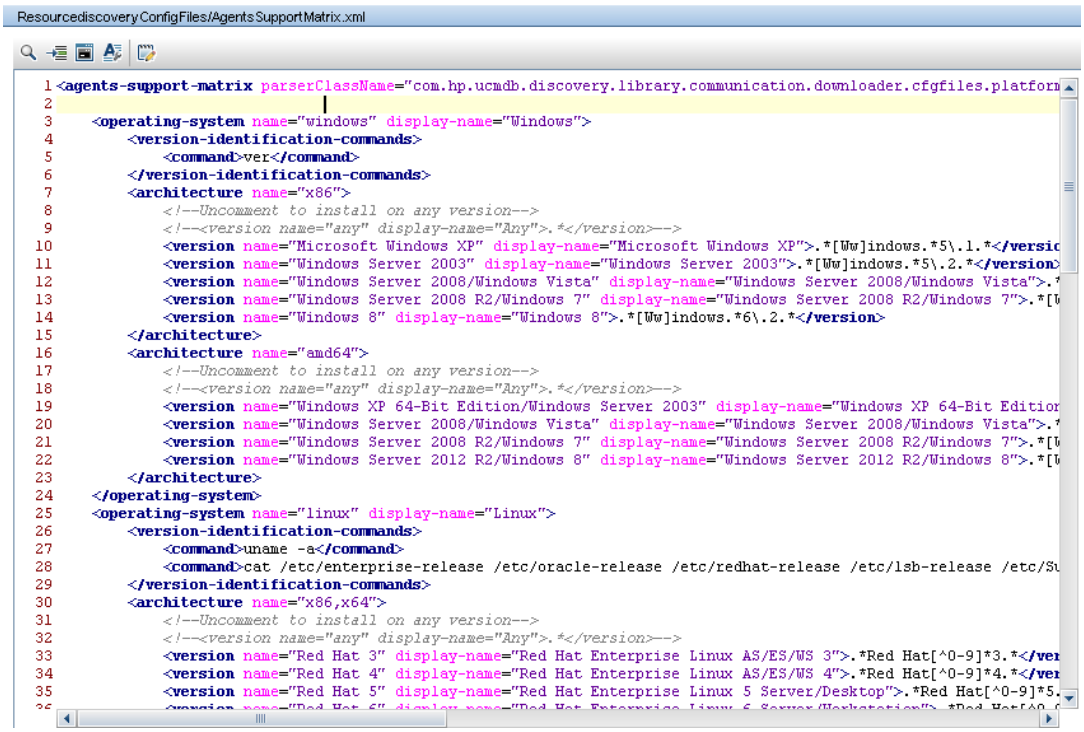
Owing to the large number of platform versions, as well as new platform versions emerging all the time, the configuration file does not include every possible supported platform on which the UD Agent may be installed and function correctly.

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

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

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

   For example:



Note:

- If the relevant operating system or architecture is not listed, create new tags for these.
- To allow support for all versions of a particular architecture of an operating system, under that architecture's tag, uncomment the line: **<version name="any" display-name="Any">.*</version>**

- For a list of out-of-the-box supported platforms and versions for the UD Agent, see the Supported Content section of the *HP Universal CMDB Discovery and Integration Content Guide*.
- For more information about UD Agent deployment, see "Universal Discovery Agent Deployment" on page 89

How to Install Universal Discovery Agent Manually

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

1. **Prerequisite**

   Ensure that the platform of the remote machine on which you want to install the UD Agent is supported.

   For more information, see "Universal Discovery Agent Deployment" on page 89.

   For a list of out-of-the-box supported version, see the Supported Content section of the *HP Universal CMDB Discovery and Integration Content Guide*.

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

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

   For more information, see the section describing exporting packages in the *HP Universal CMDB Administration Guide*.

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

   discoveryResources\ud_agents

   For a mapping of installation files to platforms, see "Universal Discovery Resources for Windows" on page 105 for Windows and "Universal Discovery Resources for UNIX" on page 107 for UNIX.

   Tip:

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

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

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

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

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

- **Attended (Windows only)**

  Copy the UD Agent installation file and certificate using any manual method or remote access technology to the remote Windows machine, and then perform installation by clicking the executable (.MSI) file. For more information on running or configuring this installer, see "Agent Installation Wizard User Interface" on page 100.

- **Unattended (All platforms)**

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

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

  ii. Perform the installation by using command line parameters. For details on parameters for all platforms, see "Universal Discovery Agent Installation Resources" on page 104.

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

  c:\AgentTest>msiexec /i hp-ud-agent-win32-x86-10.01.000.441.msi /quiet SETUPTYPE=Enterprise PORT=7738 TIMEOUT=900 CERTPATH=c:\UDAgentInstall PERIOD=90 SOFTWAREUTILIZATION=ON URL0=15.178.179.124 URL1=15.178.179.125 URL2=15.178.179.126

  Note:

  - For error code information, see platform-specific information at "Universal Discovery Agent Installation Resources" on page 104.
  - If an error occurs, the screen may also display a message with information about the error.

4. (Optional) **Generate Unique IDs for Disk Cloning**

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

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

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

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

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

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

5. **Results**

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

To verify that the Data Flow Probe is able to communicate with the remote UD Agent, go to **Discovery Control Panel > Activity Discovery Status > Progress tab** and make sure that a UDA CI instance was discovered. For more information, see "Zone-Based Discovery View" on page 266.

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

- The UD Agent generates a Unique ID which is stored locally on the discovery node and in UCMDB as follows:
  - **Windows and UNIX**. For more information on where Unique ID is stored, see "Universal Discovery Agent File Locations" on page 110.
  - **UCMDB**. Stored in the ud_unique_id attribute of Node CI.

For more information on Unique ID, see "Universal Discovery Agent Overview" on page 88.

- Software Identification Tag files are created and stored on the discovery node. For more information about Software Identification Tags, see "Hardware and Software Recognition" on page 339

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

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

1. Go to **Data Flow Management > Data Control Panel > Zone-Based Discovery**, and select a Management Zone or create a new one.
2. In the Infrastructure Discovery activity, in the Define Credentials page, ensure that SSH and Universal Discovery protocol credentials are defined, as follows:
   - **SSH protocol:**
     - In the **User Name** and **Password** fields, define credentials for a non-root user for connecting to the host through the SSH network protocol.
     - In the **sudo paths** field, ensure to include the full path to the sudo command on the remote machine. If the path is different on different computers/operating systems, you should provide multiple paths, separated by commas.
     - Enter the **sudo commands**. Ensure that the **agentinstall.sh** and **nohup** commands are included among these commands.

- **Universal Discovery protocol:**
  - In the **sudo paths** field, ensure that the sudo paths defined for the SSH protocol above are also included.
  - In the **sudo commands** field, ensure that the sudo commands defined for the SSH protocol above are also included. Ensure that the **agentinstall.sh** and **nohup** commands are included among these commands.

3. On the Universal Discovery Agent Deployment page:
   a. Select the deployment option: **Install** or **Update**
   b. Clear the **Install UD Agent to run under the root account on UNIX machines** option.

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

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

How to Configure Call Home

This task describes how to configure the Call Home feature.

This task includes the following steps:

1. "Configure the parameters" below
2. "Results" on next page

1. Configure the parameters

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

   - **Infrastructure Discovery Activity**

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

   - **Manual**

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

     Windows
     - **Unattended**. For details on available parameters, see "Universal Discovery Resources for Windows" on page 105 and "Agent Installation Wizard User Interface" on page 100.
     - **Attended**. For details on how to configure, see "Agent Installation Wizard User Interface" on page 100.

UNIX. For details on available parameters, see "Universal Discovery Resources for UNIX" on page 107.

2. Results
   - If you use the activity to configure Call Home, verify that you see configuration values in the **Summary** page of the **Infrastructure Discovery** activity. Then, verify the activity ran successfully by viewing the results summary in **Data Flow Management** > **Discovery Control Panel** > **Zone-Based Discovery**, and select the **Progress** tab. For more information, see "Zone-Based Discovery View" on page 266
   - If you use manual methods to configure Call Home,see the section that describes the traffic case in "Call Home Overview" on page 91

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

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

This task includes the following steps:

1. "Edit the XML file" below
2. "Results " below

1. Edit the XML file
   a. Locate the **AgentConfigurationbyPlatform.xml** file. To do this, choose from the following options:
      - **Data Flow Management** > **Discovery Control Panel** > **Discovery Modules/Jobs**, expand **Tools and Samples**, expand **Universal Discovery Agent Management** and select a job. Under the Properties tab select **AgentConfigurationbyPlatform.xml** and click Edit  . The script editor opens.
      - **Data Flow Management** > **Adapter Management**, expand **Universal Discovery Agent Management**, expand **Configuration Files** and select **AgentConfigurationbyPlatform.xml**. The script editor opens.

   b. In the Script Editor, click Find Text  to open the Find Text dialog box.

      Find the **agent-install-data-folder** and **agent-install-temp-folder** parameters. Replace the **DEFAULT** value with the new value for the parameters you want to modify.

      For more information on the Find Text dialog box, see the section describing the Find Text dialog box in the *HP Universal CMDB Data Flow Management Guide*.

2. Results

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

Agent Installation Wizard User Interface

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

To access	Export this MSI package from the Package Manager. After the resource is deployed, double click **hp-ud-agent-win32-x86-10.01.000.xxx.msi**. For details about how to export the package, see the section describing exporting resources in the *HP Universal CMDB Administration Guide*.
Important Information	• This MSI installer is used for Windows computers only. It is used in attended and unattended manual deployment scenarios. The Windows computer must be running Microsoft Installer version 2.0 or above. For more information on using command line parameters to configure Universal Discovery Agents, see "Universal Discovery Resources for Windows" on page 105. • There are two operational modes that are available-**Complete Installation** mode or **Software Utilization** mode. For more information about these modes, see "Set Up Type Page" below. The mode that you select determines which pages are displayed. • If the Universal Discovery Agent is already installed on the computer, the wizard starts at the "Uninstall Options Page"
Relevant tasks	"How to Install Universal Discovery Agent Manually" on page 95
Wizard map	The Agent Installation Wizard contains: "Set Up Type Page"> "Agent Configuration for Complete Installation Page" > "Software Utilization Page" > "Uninstall Options Page" > "Uninstall Type Page"
See also	"Universal Discovery Agent Overview" on page 88

Set Up Type Page

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

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

User interface elements are described below:

UI Element (A–Z)	Description
Set Up Type	Select a mode of operation: **Complete Install**. This is the default mode and suggested for most client type environments. Universal Discovery Agents are installed on the discovery nodes, and then the Data Flow Probe installs the Scanner on the discovery nodes. Scanner schedules and jobs are managed by the Data Flow Probe. **Software Utilization Only**. Only the Software Utilization software is installed on the discovery node. For more information, see "Software Utilization" on page 338.

Agent Configuration for Complete Installation Page

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

Important information	• The Windows computer must be running Microsoft Installer version 2.0 or later. • This page is displayed only if you selected **Complete Installation** on the **Set Up Page**.
Wizard map	The Agent Configuration Wizard contains: "Set Up Type Page" > **Agent Configuration for Complete Installation Page** > "Software Utilization Page"> "Uninstall Options Page" > "Uninstall Type Page"

UI Element	Description
Port	Select the port that you want to use for communication between the Universal Discovery Agent and the Data Flow Probe. **Note:** This port number should be the same as the port number you specified in the **UD Protocol Parameters** dialog box at **Data Flow Management** > **Data Flow Probe Setup** > **Domains and Probes** > **Domain** > **Credentials**. Additionally, if you change this port number manually after installation, the new port number takes effect only after the Universal Discovery Agent is upgraded.
Time Out	Enter a value that sets a time out threshold. Measured in seconds. **Note:** This parameter is called **Call Home Frequency** in the Infrastructure Discovery activity.

UI Element	Description
Primary Call Home Probe Address	Enter a primary address for the Data Flow Probe server that you want the Universal Discovery Agent to contact for Call Home messages. Enter a URL using one of the following formats: • http://1.1.1.1:80 • http://myhost:80 • myhost **Note**: Separate each entry by using a comma.
Secondary Call Home Probe Address	Enter a secondary address for the Data Flow Probe server that you want the Universal Discovery Agent to contact for Call Home messages. Enter a URL using one of the following formats: • http://1.1.1.1:80 • http://myhost:80 • myhost **Note**: Separate each entry by using a comma.
Certificate Path	Select a credential to use. For more information on exporting certificate files, see "Universal Discovery Agent Certificates" on page 90. **Note:** The path must be a folder that contains the **asctrust.cert** file and **agentca.pem** file.

Software Utilization Page

Enables you to make configurations for the software utilization feature.

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

UI Element (A–Z)	Description
Software Utilization	Select this option if you want to enable this feature. For more information, see "Software Utilization" on page 338.

UI Element (A–Z)	Description
Software Utilization Period	Choose the range to retain the software utilization data: • 31 days • 90 days • 365 days

Uninstall Options Page

Enables you to select options for the uninstall operation.

Important Information	• The Windows computer must be running Microsoft Installer version 2.0 or later. • This page is available only if the Universal Discovery Agent is already installed on the computer.
Wizard Map	The "Agent Configuration Wizard" contains: "Set Up Type Page" > "Agent Configuration for Complete Installation Page" > "Software Utilization Page"> **Uninstall Options Page** > "Uninstall Type Page"

UI Element	Description
Repair	Select this option if you want to install the installation files again. **Note:** All configuration options are preserved.
Remove	Select this option to remove the Universal Discovery Agent.

Uninstall Type Page

Enables you to select the type of uninstall operation.

Important Information	• The Windows computer must be running Microsoft Installer version 2.0 or later. • This page is available only if you selected **Remove** on the "Uninstall Options Page"
Wizard Map	The "Agent Configuration Wizard" contains: "Set Up Type Page" > "Agent Configuration for Complete Installation Page" > "Software Utilization Page" > "Uninstall Options Page" > **Uninstall Type Page**

UI Element	Description
Default	Select this option if you want perform a typical uninstall operation that deletes agent executable files and configuration files. **Note:** • Use this option when upgrading the Universal Discovery Agent. • The Universal Discovery Agent log and software utilization files are not deleted.
Complete	Select this option if you want to perform a complete uninstall and remove most Universal Discovery Agent and scanner files. **Note:** • Use this option when you do not plan on installing the Universal Discovery Agent again. • Temporary files that are associated with the scanner are not deleted.

Discovery Node Disk Requirements

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

Type of Node	Universal Discovery Agent and Scanner	Inventory Data	Utilization Data
Desktop/Workstation/Laptop	25 MB	250 K- 3 MB	5-10 MB

Note:
The value in the **Inventory Data** column greatly varies depending on your selections when you configured and generated the Scanner.

The value in the **Utilization Data** column is estimated for one year of utilization data.

Universal Discovery Agent Installation Resources

The Discovery resources are files that support the deployment and installation of Universal Discovery Agents and Scanners. When using manual methods of deployment you can retrieve these resources by exporting them from **Administration** > **Package Manager** > **UDAgentManagement**. For details, see the section describing exporting packages in the *HP Universal CMDB Administration Guide*.

To export individual resource files, go to **Data Flow Management** > **Adapter Management** > **Resources Pane** > **UDAgentManagement** > **DiscoveryResources** > **UD_Agents**.

Tip: You do not have to export or include XML files in the discovery packages.

Universal Discovery resources are available for the following platforms:

- **Windows**. For details, see "Universal Discovery Resources for Windows" below
- **Mac**. For details, see "Universal Discovery Resources for Mac" on next page
- **UNIX**. For details, see "Universal Discovery Resources for UNIX" on page 107

Universal Discovery Resources for Windows

Resources

Discovery resources for Windows are as follows:

Platform	Resource Name	Description
Windows (x86)	hp-ud-agent-win32-x86-10.01.000.msi	This installer package is required for all installations.
	agentupgrade.cmd	Used when upgrading or migrating DDMI agents to Universal Discovery Agents.

Parameters

You can use parameters in a command line interface to customize the Universal Discovery Agent installation, uninstallation, or upgrade as follows.

c:\AgentTest>msiexec <InstallOption> <Product.msi> /log <UPGRADELOGFILEPATH> [CLEAN=ON] SETUPTYPE=Enterprise PORT=7738 TIMEOUT=900 CERTPATH=c:\ PERIOD=90 SOFTWAREUTILIZATION=ON URL0=15.178.179.124 URL1=15.178.179.125 URL2=15.178.179.126

Parameter Name	Description
InstallOption	Indicates the type of operation. The following options are supported: • **/i**: Installs the Universal Discovery Agent. • **/x**: Uninstalls the Universal Discovery Agent.
Product.msi	Indicates the product file name. For example, **hp-ud-agent-win32-x86-10.01.000.xxx.msi**
UPGRADELOGFILEPATH	Specify a path to save a log file. **Note:** • Only use with the **agentupgrade.cmd** script. • Use together with the **/log** switch.

Parameter Name	Description
CLEAN	Indicates the type of uninstall procedure. Most Universal Discovery Agent files and scanner files are deleted. **Note:** • This parameter must be used together with the uninstall option. • If you do not want to use this option, omit the parameter from the string.
SETUPTYPE	Indicates the operational mode. Type **Enterprise** or **Manual**. **Note:** The **manual** parameter value is called "Software Utilization Plug In Only" in the **Agent Installation Wizard** User Interface.
PORT	Port number for Universal Discovery Agent to use for communication with Data Flow Probe. Type **2738** or **7738**. **Note:** The default value is 2738. If you change this port number manually after installation, the new port number takes effect only after the Universal Discovery Agent is upgraded.
TIMEOUT	Frequency that the Universal Discovery Agent contacts the Data Flow Probe when the Universal Agent sends Call Home messages. Measured in seconds. Default is 86400 seconds. **Note:** This parameter is called **Call Home Frequency** in the Infrastructure Discovery activity.
CERTPATH	Path to install certificate files. Default is the working directory.
PERIOD	Number of days to retain software utilization data. Default is 365 days.
SOFTWAREUTILIZATION	Enable or disable Software Utilization plug in. Use "ON" to enable and "OFF" to disable. Default is "OFF".
URL0|URL1|URL2	IP address for Data Flow Probe that is used for Call Home messages.

Universal Discovery Resources for Mac

Discovery resources for Mac are as follows.

Platform	Resource Name
Mac OS X (x86)	hp-ud-agent-macosx-x86.dmg

Universal Discovery Resources for UNIX

Resources

The following script files are available for manual agent installations and upgrades:

Platform	Resource Name	Description
UNIX	agentinstall.sh	• Installs the Universal Discovery Agent. • Replaces the non-native version of the UD Agent with a version that is packaged in the native operating system version of the discovery node.
	agentupgrade.sh	Upgrades the DDMI agent to a Universal Discovery Agent. However, this version of the UD Agent is not packaged in the native operating system version of the discovery node.

These files are available in the **Package Manager**. For more information on exporting resources, see the section describing exporting resources in the *HP Universal CMDB Administration Guide*.

Additionally,discovery resources for UNIX and the UNIX variants that are also available in the **Package Manager** are as follows:

Operating System	Platform	File Name
HP-UX	ia64	hp-ud-agent-hpux-ia64.depot
	HPPA	hp-ud-agent-hpux-hppa.depot
Linux (Red Hat, SUSE,CentOS, Oracle)	x86,x64	hp-ud-agent-linux-x86.rpm
Linux (Ubuntu)	x86,x64	hp-ud-agent-linux-x86.deb
AIX	POWER	hp-ud-agent-aix-ppc.bff
Solaris	x86	hp-ud-agent-solaris-x86.i86pc
	SPARC	hp-ud-agent-solaris-sparc.sparc
Mac OS X	x86	hp-ud-agent-macosx-x86.dmg

Parameters

You can use parameters in a command line interface to customize the discovery installation as follows:

filename [--help] [--url0 ipaddress] [--url1 ipaddress] [--url2 ipaddress] [--port number] [--timeout seconds] [--cert path] [--usage] [--softwareutilization] [--softwareutilizationonly] [--period days] [--home path] [--upgrade] [--uninstall] [--clean] [--temp] packagename

--isnative

where:

Parameter Name	Description
cert	Path to install certificate files. **Default:** Working directory
clean	Specifies a type of uninstall procedure. Most Universal Discovery Agent files and scanner files are deleted. **Note:** This parameter can only be used together with the **uninstall** and **home** parameters.
filename	The name of the installation file. This is usually **agentinstall.sh**. **Note:** This is a mandatory parameter.
help	Displays help messages.
home	Directory that contains the Universal Discovery Agent log and the software utilization data files. **Default:** HOME directory
packagename	Full path for the package installation file. **Default:** Working directory **Note:** This parameter is required when performing an installation operation.
period	Number of days to retain software utilization data. **Default:** 365 days
port	Port number for the Universal Discovery Agent to use for communication with the Data Flow Probe. Type **2738** or **7738** **Default:** 2738 **Note:** If you change this port number manually after installation, the new port number takes effect only after the Universal Discovery Agent is upgraded.
softwaretutilization	Enables software utilization.
softwareutilizationonly	Enables the Software Utilization plug-in only. **Note:** The Universal Discovery Agent is disabled.

Parameter Name	Description
temp	Directory that contains Universal Discovery Agent and scanner temporary files. **Default:** $TEMP directory.
timeout	Frequency (in seconds) that the Universal Discovery Agent contacts the Data Flow Probe for Call Home. **Default:** 86400 seconds
uninstall	Uninstalls the Universal Discovery Agent. **Note:** When you use this parameter, all other parameters except the **clean** parameter are ignored. Additionally, the **filename** parameter is required.
upgrade	Upgrades the Universal Discovery Agent.
url0|url1|url2	IP address for Data Flow Probe that is used for Call Home messages.
usage	Displays help messages. **Note:** This parameter provides the same information as the **help** parameter.
isnative	Specifies whether a native or non-native Universal Discovery Agent is installed.

Note:

- **Solaris Users Only**: The limit of strings typed in the command line interface is 256 characters.
- Use "udagent" for the **packagename** parameter value. This resource is available in the **Package Manager**.

Universal Discovery Agent Error Codes for UNIX

The following error codes may be returned when using installation or upgrade scripts as follows:

Error Code	Description
1	General error
2	Wrong parameter
3	Not root user
4	File creation error
5	Wrong platform

Error Code	Description
6	Install package error
7	Directory missing
8	File missing
9	File not executable
10	Link startup script error
11	Startup script error
12	Universal Discovery Agent is already installed **Note:** Applicable only when performing an installation operation.

Universal Discovery Agent File Locations

Universal Discovery Agents and supporting files are installed on the discovery node as follows:

Windows

Platform	Installation Files	Data/Utilization Data Files	Unique ID
x86	program files\hewlett-packard\discovery agent	<AgentServiceData>\Hewlett-Packard\Universal Discovery\Data\Perf where <AgentServiceData> is the location of the application data directory for the profile that is used by the UD Agent service. By default, <AgentServiceData> refers to the following if Windows is installed on C drive: • **XP/Server 2003:** C:\Documents and Settings\LocalService\Application Data • **Vista and above:** C:\Windows\system32\config\systemprofile\AppData\Roaming	HKEY_LOCAL_MACHINE\SOFTWARE\Hewlett-Packard\Universal Discovery\V1\Options\UD_UNIQUE_ID
x64	program files(x86)\hewlett-packard\discovery agent	C:\Windows\SysWOW64\config\systemprofile\AppData\Roaming\Hewlett-Packard\Universal Discovery\Data\Perf	HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Hewlett-Packard\Universal Discovery\V1\Options\UD_UNIQUE_ID.

- Certificate files are contained in the same location as program files. For more information, see "Universal Discovery Agent Certificates" on page 90.
- The Perf subdirectory contains most of the utilization data. This applies to all platforms listed.

UNIX

Platform	Installation Files	Data Files	
		Utilization Data Files	Unique ID
Linux /Solaris/HP-UX/Unix	/opt/HP/Discovery	$HOME/.discagnt/Perf	UD_UNIQUE_ID entry in $HOME/.discagnt/aioptionrc
Mac OS X (x86)	/Library/StartupItems/HPDiscoveryAgent	$HOME/.discagnt/Perf	
AIX	/usr/lpp/HP/Discovery	$HOME/.discagnt/Perf	

Note:

- Certificate files are contained in the same location as program files. For more information, see "Universal Discovery Agent Certificates" on page 90.
- The Perf subdirectory contains most of the utilization data. This applies to all platforms listed.
- "$HOME" refers to the home directory of the account that runs the Universal Discovery Agent.
- You can modify the Universal Discovery Agent log and software utilization data files location when you use the **installagent.sh** script. For more information, see "Universal Discovery Resources for UNIX" on page 107.

Software Identification Tags

Tag File Name

When you install the Universal Discovery Agent, a Software Identification Tag file is created and named as follows:

Agent Deployment Mode	File Name
Complete Install	regid.1986-04.com.hp_UD-AgentComplete-10.01.swidtag
Software Utilization	regid.1986-04.com.hp_UD-AgentSoftwareUtlizationOnly-10.01.swidtag

For more information on the deployment modes for the Universal Discovery Agent, see "Universal Discovery Agent Overview" on page 88.

Tag File Location

Operating system vendors can specify where software identification tags are located. If the vendor does not specify a location, software identification tags may be stored as follows:

Platform	Version	Local File Location	Global File Location
Apple Macintosh OS X	Leopard	/Library/StartupItems /HPDiscoveryAgent	/Library/Application Support/regid.1986-04.com.hp
Apple Macintosh OS X	Prior to Leopard		/Applications /HPDiscoveryAgent.app /Contents
UNIX and Linux (Excluding AIX)		/opt/HP/Discovery	/usr/share/regid.1986-04.com.hp/
Windows	XP, 2000, 2003	• **(x32):** C:\Program Files\Hewlett-Packard\Discovery Agent • **(x64):** C:\Program Files (x86) \Hewlett-Packard\Discovery Agent	%AllUsersProfile%\Application Data\regid.1986-04.com.hp
Windows	Vista, Server 2008		%Program Data%\regid.1986-04.com.hp
AIX		/usr/lpp/HP/Discovery	/usr/share/regid.1986-04.com.hp/

Software Identification Tag Attributes

The following attributes are contained in scan files if Software Identification Tags are enabled during discovery:

Field Name	Attribute Name	Description
Entitlement_ required_ indicator	hwOSSoftwareIdTagEntitlementRequiredIndicator	Indicates if an entitlement must match up against this software in order for a successful software reconciliation to occur.
product_title	hwOSSoftwareIdTagProductTitle	Name of software as assigned by the software creator.

Field Name	Attribute Name	Description
product_ version	hwOSSoftwareIdTagProductVersionName, hwOSSoftwareIdTagProductVersionNumber	Textual and numeric version of the software.
software_ creator	hwOSSoftwareIdTagSoftwareCreatorName, hwOSSoftwareIdTagSoftwareCreatorRegid	Software creator that produced the software package, and the creator's domain.
software_ licensor	hwOSSoftwareIdTagSoftwareLicensorName, hwOSSoftwareIdTagSoftwareLicensorDomain	Software licensor that owns the copyright for the software package, and the licensor's domain.
software_id	hwOSSoftwareIdTagSoftwareUniqueId, hwOSSoftwareIdTagSoftwareIdCreatorDomain	Unique ID of the product and the domain name of the tag provider.
tag_creator	hwOSSoftwareIdTagTagCreatorName, hwOSSoftwareIdTagTagCreatorDomain	Name of the tag creator, and the tag creator's domain name.
tag file path	hwOSSoftwareIdTagTagFilePath	Location of the tag file. If the file is located at the root of the application's installation directory, this field will indicate the installation directory of the application. **Tip:** This information may be useful for application teaching. For more information, see "Application Teaching" on page 338.

Field Name	Attribute Name	Description
license linkage	hwOSSoftwareIdTagLicenseLinkageActivationStatus	Licensing level that a software licensor uses to track software status. Every software licensor may have a different set of values. Information may include the following: • **Trial.** Indicates that the software is in a trial mode and this value may include the number of days the trial mode is valid, or that the trial has expired. • **Serialized.** Indicates that the software user has entered a valid serial number during the installation process, however, the software is not activated. • **Fully Licensed.** Indicates that the product is activated. • **Unlicensed.** Indicates that the software is running in a limited mode. Software can enter into this state by one or more of the following: a. A trial period has expired. b. A time-based license has expired. c. Software package contained a serial

Field Name	Attribute Name	Description
		number, however, the software package was not activated in the given timeframe.
	hwOSSoftwareIdTagLicenseLinkageChannelType	Indicates the channel the software was targeted for. Every software licensor may have a different set of values. Information may include the following: • **Volume.** Targeted for volume consumption. • **Retail.** Target for the retail channel. • **OEM.** Targeted for the OEM channel. • **Academic.** Targeted for the education or academic channel.

Field Name	Attribute Name	Description
	hwOSSoftwareIdTagLicenseLinkageCustomerType	Identifies the target customer of the software. Every software licensor may have a different set of values. Information may include the following: • **Government.** Targeted for government customers. • **Corporate.** Targeted for corporate customers. • **Educational.** Targeted for education or academic customers. • **Retail.** Targeted for retail customers.
serial number	hwOSSoftwareIdTagSerialNumber	Unique identifier that may be represented as a combination of numbers, letters, or symbols. The serial number for the software product is a commonly used unique number assigned for identification of a particular title and purchase. **Note:** The value might be the serial number that is run through a one-way hash encryption scheme.

For more information about enabling discovery of Software Identification Tags, see "Hardware Data Page" on page 388.

Chapter 4

Data Flow Probe Status

This chapter includes:

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 **Refresh**  button.

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" below
- "Access Data Flow Probe status" below

1. **Prerequisites**

   Verify that the Probe is enabled and is connected to the HP Universal CMDB server. For details, see "How to Start the Data Flow Probe" on page 31.

2. **Access Data Flow Probe status**

   a. Go to **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 next page.

   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.

Data Flow Probe Status User Interface

This section includes:

[Job Name] Dialog Box

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

To access	In the Progress pane of the Data Flow Probe Status window do one of the following: • Select a job and click the **View job progress**  button • Double-click a job

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 Universal Discovery ran the job. • **Next invocation.** The next time that Universal Discovery is scheduled to run the job. • **Last duration.** The length of time, in seconds, taken to run the job in the previous invocation. This is calculated according to the start time of the first trigger until the end time of the last trigger, even if triggers were added later on. • **Average duration.** The average duration (in seconds) per trigger of the time it took the Probe to run this job. • **Recurrence.** The number of times the job ran via the scheduler (manual runs are not counted).
Discovery Results	For details, see "Data Flow Probe Status Window" below.

Data Flow Probe Status Window

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

To access	**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 discovery results for the domain. • a Probe, you can view details on the Probe (such as the Probe IP), the progress of a job and you can view discovery results.
Relevant tasks	"View Current Status of Discovered CIs" on page 117
See also	"Data Flow Probe Status Overview" on page 117

Domain Browser Pane

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

Details Pane (Domain)

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

User interface elements are described below:

UI Element (A–Z)	Description
Domain Type	• **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. For details on defining domains, see "Add New Domain Dialog Box" on page 67.

Details Pane (Probe)

User interface elements are described below:

UI Element (A–Z)	Description
Refresh	**Refresh.** Displays the most 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 (that is, the date and time of the data displayed in Data Flow Probe Status).
Probe IP	The IP address which the Probe communicates with UCMDB.

UI Element (A–Z)	Description
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 304.
Status	The status of the Probe: • **Connected** The Probe has successfully connected to the server. (The Probe connects every few seconds.) • **Disconnected (being restarted)** The Probe gateway service is restarting. This may be because, for example, the Probe has downloaded a Content Pack Update, or detected a job that is stuck. • **Disconnected (stopped)** The Probe gateway service is stopped by the server administrator. • **Disconnected (reason unknown)** The Probe gateway service is stopped for some other reason. **Note:** If you suspend the Probe via the UI, **(suspended)** is also displayed as part of the status.
Threads	The sum of all threads currently allocated to the running jobs.

Progress Pane

Displays the progress of the jobs on the selected Probe.

User interface elements are described below:

UI Element (A–Z)	Description
	**View Job progress.** Opens the [Job Name] dialog box, enabling you to view the view details of the selected job. **Available:** When a job in the Progress pane is selected. **Tip:** Alternatively, double-click a job to display its details. For details, see "[Job Name] Dialog Box" on page 118.

UI Element (A–Z)	Description
	**View workflow information:** Opens the Workflow Information dialog box, enabling you to view workflow information for a selected job that is dependent on a workflow adapter and that is currently running. This dialog box shows the following information for the job: Trigger CI, current step, workflow status, workflow start time, workflow end time, parking status, current timeout period, and next invocation time. If you double-click on a Trigger CI in the Workflow Information dialog box, a history of all steps that have already been executed during the current execution of the selected job is displayed. The **View workflow information** button is available when a currently running job that is dependent on a workflow adapter is selected in the Progress pane.
Job	The name of the job scheduled to run on the Probe.
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.

Discovery Results Pane

Enables you to view discovery results.

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
	Enables you to retrieve the latest data from the Probe. **Note:** This data is not automatically updated.

UI Element (A–Z)	Description
	**Set Filter.** Enables you to set the time range for which to display discovery results. • **All.** Displays results for all job runs. • **Last Hour/Day/Week/Month.** Choose a period of time for which to display discovery results. • **Custom Range.** Click to open the Change Timeframe dialog box: Enter the date or click the arrow to choose a date and time from the calendar, for the **From** and **To** dates (or click **Now** to enter the current date and time). Click **Last Day** to enter the current date and time in the **To** box and yesterday's date and time in the **From** box. Click **OK** to save the changes.
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.
Filter	The time range set with the **Set Filter** button.
Last updated	The date and time that the results data was updated for a particular Probe.
Updated	The number of CIT instances that have been updated.

Adapter Management

Chapter 5

Adapter Configuration

This chapter includes:

Discovering Running Software

You can discover software (for example, a specific Oracle database) running in your environment.

This section includes the following topics:

- "Discovery Process" below
- "Running Software Default View" on next page

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 UCMDB Server.

Running Software Default View

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

You can configure DFM to discover running software. For details, see "How to Discover Running Software – Scenario" on page 130.

Identifying Running Software by Processes

An application is identified by the existence of one or more running processes which are defined by their names and by command line (optional).

A process can be optionally marked as a key process or as a main process.

An application is identified if the following holds true:

- At least one process was found.
- All processes that are marked as key processes exist.

If an application is identified, a result RunningSoftware CI is created for the application obeying the following rules:

- If none of the processes is marked as a main process, a single RunningSoftware CI will be created, linked to all discovered processes by dependency relationships.
- If there are processes that are marked as main processes, a RunningSoftware CI will be created for each instance of these main processes.

For example, assume that rules are defined for the identification of two applications, **application_a** and **application_b**:

- **application_a** is identified by **proc.exe** and **unique_ proc_a.exe**.
- **application_b** is identified by **proc.exe** and **unique_ proc_b.exe**.

Say that **proc.exe** is found but none of its processes are marked as key or main processes. In this case, **RunningSoftware** CIs are created for both **application_a** and **application_b**. These CIs are linked by a dependency relationship to the same process (that is, **proc.exe**).

Assume too that **unique_proc_a.exe** and **unique_proc_b.exe** are marked as key processes:

- If the **proc.exe** process only is discovered, a **RunningSoftware** CI is not created.
- If **unique_ proc_a.exe** is discovered, **RunningSoftware** CIs are created for **application_a** linked by a dependency link to **unique_ proc_a.exe**. If in addition, **proc.exe** is discovered, it is linked to the same CI. The same holds for **application_b**.

Assume that two instances of **unique_proc_a.exe** are discovered:

- If the process is not marked as a main process, a single **RunningSoftware** CI is created for **application_a** linked to both processes.
- If the process is marked as a main process, two separate **RunningSoftware** CIs are created for **application_a**.

For details on the key field in the Software Identification Rule Editor dialog box, see "Identifying Processes" on page 171.

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.

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 40.

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).

Note: The Data Flow Probe does not wait for the aging mechanism to perform the calculation but immediately sends a deletion request to the server. For details about aging, see "The Aging Mechanism Overview" in the *HP Universal CMDB Administration Guide*.

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.

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 146.
- 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 **containment** relationship is used between a node and an IP address. A laptop machine is allocated a different IP address very often; by deleting the relationship, you prevent the accumulation of old IP addresses attached to this node.

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 Discovery Results pane. For details, see "Data Flow Probe Log Files" on page 59 and "Results Pane" on page 293.
- For details on setting automatic deletion, see "Adapter Configuration Tab" on page 144 in the Results Management pane.

How to Configure Adapter Settings

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

Change the adapter's definitions in the Adapter Management module

Note: This method is recommended.

1. Navigate to **Data Flow Management > Adapter Management**.
2. In the Resources pane, select the adapter file in the **Packages > <package name> > Adapters** folder.
3. Do one of the following:
   - To edit general adapter settings, use the **Adapter Definition** and **Adapter Configuration** tabs. For details, see "Adapter Definition Tab" on page 137 and "Adapter Configuration Tab" on page 144.
   - To define specific settings for the selected adapter, right-click the adapter and select **Edit Adapter Source** from the shortcut menu.

Edit the adapter package and redeploy it using the Package Manager

Export the package to your local drive, edit the package and redeploy it. For information see, "How to Export a Package" and "How to Deploy a Package" in the *HP Universal CMDB Administration Guide*.

Use the JMX Console

1. Launch the Web browser and enter the server address, as follows:
   http://<UCMDB Server Host Name or IP>:8080/jmx-console

   You may have to log in with a user name and password.
2. Under **UCMDB**, click **UCMDB:service=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.

How to Define the Owner Tenant Adapter Parameter

In multi-tenancy environments, all discovered CIs/relationships are assigned an owner tenant. If an owner tenant parameter is defined in the discovery adapter, the discovered CIs/relationships are assigned this owner tenant.

If a job using the adapter has an override defined for this parameter, then the overriding value is assigned to the discovered CI/relationship. For details, see "How to Define the Owner Tenant Parameter in the Discovery Job Properties" on page 240.

This task describes how to define an owner tenant parameter in an adapter.

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

1. Prerequisite

   The owner tenant that you want to define in adapter's parameter must already be defined in UCMDB. For details on creating owner tenants in UCMDB, see "New Tenant/Edit Tenant Dialog Box" in the *HP Universal CMDB Administration Guide*.
2. In the Adapter Management module, select the adapter whose parameter you want to define.
3. Click the **Adapter Definition** tab.
4. In the Adapter Parameters pane, click the **Add**  button:
   a. In the **Name** box, type **defaultOwner**.
   b. In the **Value** box, enter the name of the owner tenant in UCMDB that you want to define in the adapter.
   c. (Optional) Enter a description for the owner tenant parameter.

How to Configure Full Population Run

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

To change the full population value of the UCMDB 9.0x adapter:

1. Open the CmdbAdapter adapter source.
   a. Select **Data Flow Management > Adapter Management > Resources pane > CmdbAdapter.**
   b. Under **Adapters**, right-click **CmdbAdapter**, and select **Edit Adapter Source**.

2. In the source file, locate the following tag:

```
<full-population-days-interval>
    7
</full-population-days-interval>
```

3. Edit the value as follows:

Value	Description
7	Run full population job every 7 days
1	Run full population job each day
0	Always run a full population job
-1	The option is disabled

How to Configure CI Aging Settings

This task explains how to configure the aging mechanism for adapters.

To learn more about aging, see "The Aging Mechanism Overview" in the *HP Universal CMDB Administration Guide*.

To enable aging of CIs:

1. Select the adapter: **Adapter Management > Resources pane > Packages > <adapter>**
2. In the **Adapter Configuration** tab, under **Results Management**, select an **Enable Aging** option as follows:

System Default	Enables aging of CIs using the default aging setting defined in each CI type's attribute settings. For details, see "Configuration Item Properties Dialog Box" in the *HP Universal CMDB Modeling Guide*.
Always Enabled	Always enables aging of CIs discovered by jobs that use this adapter. **Note:** When this option is selected, the default aging setting defined in each CI type's attribute settings is ignored.
Always disabled	Disables aging of CIs discovered by jobs that use this adapter. **Note:** This option overrides the default aging setting defined in each CI type's attribute settings.

3. Save your changes.

How to Define CITs to be Deleted by Java-Based Population Adapters

This task describes how to define CITs to be deleted by population jobs that use Java-based population adapters.

1. Open the population adapter's configuration file.
2. Under the **<taskInfo>** tag, locate the **<remove-cis>** tag.

   If this tag does not exist, create it.
3. Under the **<remove-cis>** tag, add the CITs to be removed using the format in the following example:

```
<remove-cis isEnabled="false">
    <ci-type>link</ci-type>
    <ci-type>object</ci-type>
</remove-cis>
```

4. Save the configuration file.

Note: When defining integration jobs that use the population adapter, to configure the job to delete CITs as defined in the adapter, ensure that the **Allow Integration Job to delete removed data**option is selected . For details, see "New Integration Job/Edit Integration Job Dialog Box" on page 207.

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" below
- "Create a Command Line Rule" on next page
- "Define the Value of an Attribute" on next page
- "Activate the Job" on page 132

1. Prerequisites

Display the Attribute Assignment Rules dialog box:

a. Select **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 143.

> **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 172.

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 170.

d. Click the **Set Attributes** button to open the Attributes Assignment Editor dialog box. For details, see "Attribute Assignment Editor Dialog Box" on page 151.

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 162.

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`.

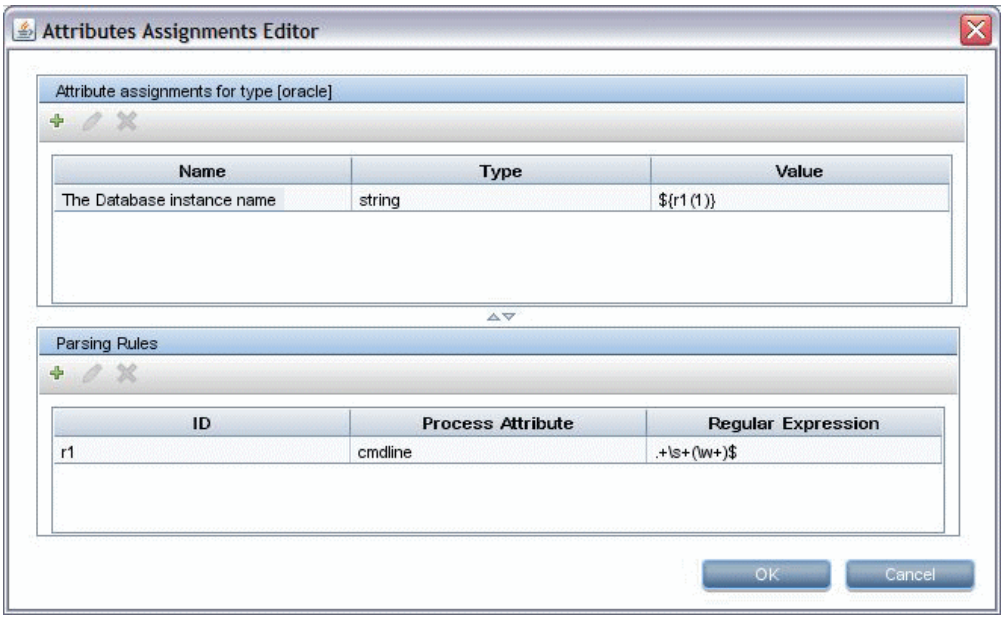
3. Define the Value of an Attribute

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.

That is, 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`.

4. ### Activate the Job

   For details, see "How to Manually Activate Modules/Jobs/CIs" on page 277 and "Discovery Modules/Jobs - Discovery Modules Pane" on page 295.

How to Attach Discovery Documentation to a Discovery Package

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

1. ### Prerequisites

   a. Create the help document in PDF format.

   b. Create a folder called **docs**, and copy your PDF into that folder.

   c. Zip the **docs** folder, and copy it to your local file system.

2. ### Deploy the document on the UCMDB server

   Navigate to **Administration > Package Manager**, and click the **Deploy packages to server** button to deploy the .zip file containing the PDF you want to deploy. For details, see "How

to Deploy a Package" in the *HP Universal CMDB Administration Guide*.

3. **Attach the document to the relevant discovery package**
   a. Navigate to **Data Flow Management > Adapter Management**.
   b. In the **Resources** pane, expand the adapter file: **Packages > <package name> > Adapters** and select the adapter to which to attach the document.
   c. Do one of the following:
      - In the **Adapter Definition** tab, under **Details**, click the **Edit**  button adjacent to the **Content Help** box, and select the help document that you deployed.
      - Right-click the adapter and select **Edit Adapter Source** from the shortcut menu. Look for **RelatedDocument** in the code, and replace the line with:

        `<RelatedDocument>`*`name_of_pdf`*`.pdf</RelatedDocument>`

        where **name_of_pdf** is the name of the help document you deployed.

How to Attach Readme to a Discovery Package

This task describes how to attach an updated or new Readme file to a discovery package.

1. **Prerequisite**

   To attach a Readme file to a discovery package, the package's .zip file must be located somewhere on your local file system.

   If you are updating the Readme file of a discovery package that is already deployed on your UCMDB server, you must export the package's .zip file to your local file system before attaching the updated file. For details on exporting packages, see "How to Export a Package" in the *HP Universal CMDB Administration Guide*.

2. **Add the Readme file to the discovery package's .zip file**
   - Create or update the Readme file, and save it with the name, **Readme.txt**.
   - Copy the **Readme.txt** file into the root of the package's .zip file.

3. **Deploy the package on the UCMDB server**

   Navigate to **Administration > Package Manager**, and click the **Deploy packages to server**  button to deploy the .zip file containing the Readme. For details, see "How to Deploy a Package" in the *HP Universal CMDB Administration Guide*.

How to Filter Probe Results

Global filtering enables you to filter Probe results for all adapters, so that only results of interest to you are sent to the UCMDB Server.

You can also filter specific adapters. For details, see "Adapter Configuration Tab" on page 144.

Note:

- You can use regular expressions in filters.
- Attributes in the filter should be of type **string** only. For details on CI attribute types, see "Attributes Page" in the *HP Universal CMDB 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.
- **Recursive Filtering.** Using global filtering, you can filter out a CI so that it is not included in the filter results. This CI may be a root CI, containing other CIs or relationships. By default, during the filter process, the contained CIs and relationships, as well as any CIs related to them, are added to the filter results—including the root CI. This causes undesired filter results. **Recursive filtering** corrects this by ensuring that if a root CI is filtered out, then any contained CIs or relationships are filtered out too, such that the root CI cannot be found again.

  To enable recursive filtering:

  In the **globalFiltering.xml** file, under the **resultFilters** element, locate the **recursiveFilter** attribute. (If the **recursiveFilter** attribute does not appear, then you must add it.) Set the attribute value to **true**.

  Note: By default, recursive filtering is disabled, that is **recursiveFilter** = **false**.)
- DFM filters first according to the **<includeFilter>** and then applies the **<excludeFilter>** on the results of **<includeFilter>**.

Configure a Filter

Open the **globalFiltering.xml** file. (**Adapter Management module > Resources pane > Packages > DDM Infra > Configuration Files**)

The code in displayed in the View pane:

```
<resultFilters>
    <excludeFilter>
        <vector />
    </excludeFilter>
    <includeFilter>
        <vector />
    </includeFilter>
</resultFilters>
```

- **<excludeFilter>.** When a vector marker is added to this filter, all CIs that match the filter are removed. If this marker is left empty, all results are sent to the server.
- **<includeFilter>.** When a vector marker is added to this filter, all CIs that do not match the filter are removed. If this marker is left empty, all results are sent to the server.

The following example shows an IpAddress CI that has address and domain attributes:

```
<vector>
    <object class="ip_address">
        <attribute name="name"
type="String">192\.168\.82\.17.*</attribute>
        <attribute name="routing_domain"
type="String">DefaultProbe</attribute>
    </object>
</vector>
```

If this vector is defined in **<includeFilter>**, all results **not** matching the filter are removed. The results sent to the server are those where the ip_address matches the regular expression **192\.168\.82\.17.*** and the ip_domain is **DefaultProbe**.

If this vector is defined in **<excludeFilter>**, all results matching the filter are removed. The results sent to the server are those where the ip_address does **not** match the regular expression **192\.168\.82\.17.*** and the ip_domain is **notDefaultProbe**.

The following example shows an ip_subnet CI that has no attributes.

```
<vector>
    <object class="ip_subnet">
    </object>
</vector>
```

Configure a Filter to Ignore Case

You can configure a filter to ignore case by prefixing a regular expression with **(?i)**. For example, **(?i)DefaultProbe** finds **defaultprobe** as well as **DefaultProbe**.

The following example removes all occurrences of the **DefaultdoMain** attribute because the vector code is located in the **<excludeFilter>** section:

```
<resultFilters>
    <excludeFilter>
         <vector>
           <object class="ip_address">
               <attribute name="routing_domain" type="String">(?i)
               DefaultdoMAin</attribute>
           </object>
        </vector>
    </excludeFilter>
    <includeFilter>
        <vector />
    </includeFilter>
</resultFilters>
```

Pre/Post-Scan Script Editor

Enables you to edit pre and post scan scripts in your Management Zones.

To access	• **Adapter Management Module** > **Inventory Discovery** > **Inventory Discovery by Scanner** > then expand the **Global Configuration Files** pane, select the **PrePostScanScriptingConfiguration** file and click **Edit**  . • **Discovery Control Panel** > **Inventory Discovery Activity** > **Preferences tab** > select **Scanner based Inventory Discovery** and click **Edit Script**.
Important information	UI elements are available only when a script file is selected in the left pane.
Relevant tasks	"How to Edit Pre- and Post-Scan Scripts" on page 352

User interface elements are described below:

UI Element	Description
	**Find Text.** Opens the Find Text dialog box, enabling you to find text in the selected script file. For more information, see "Find Text Dialog Box" on page 157.
	**Go to Line.** Opens the Go To Line dialog box, enabling you to jump to a specific line in the script file. Enter the line number and then press **Enter**.
	**Import a File.** Opens the Import File dialog box, enabling you to import a script file.
	**Export to a File.** Opens the Export File dialog box, enabling you to export the selected script to a file.

Pre-Scan and Post-Scan Scripts

The pre-scan and post-scan scripts feature enables you to customize and execute scripts that run on discovery nodes. It expands the capabilities of standard scanner detection by capturing custom data on specific hardware, settings, or applications.

The pre-scan scripts run at scanner start-up before the hardware and software scanning. The post-scan scripts run after the hardware and software scanning is complete.

To see more information on how to edit pre and post scan scripts, see "How to Edit Pre- and Post-Scan Scripts" on page 352.

Note: If you create a post-scan script, you may want to map your captured data to a UCMDB attribute using the Hardware Mapping Configuration tool. To do this, see "How to Map Scan File Attributes to UCMDB" on page 378.

Adapter Management User Interface

This section describes:

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	**Adapter Management > Resources pane > Packages > <adapter>**
Relevant tasks	"Implement a Discovery Adapter" in the *HP Universal CMDB Developer Reference Guide*

User interface elements are described below:

UI Element (A–Z)	Description
Adapter Category	Used to arrange adapters by category.

UI Element (A–Z)	Description
Content Help	The Help document associated with the adapter, in PDF format. To change the Help document associated with the adapter, do one of the following: • Click  and select the relevant PDF file. • Right-click the adapter in the Packages tree and click **Edit adapter source**. Find the following line in the code: `<RelatedDocument>`*name_of_pdf*`.pdf</RelatedDocument>` and change the name of the PDF file. 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 *HP Universal CMDB Developer Reference Guide*. Click the button to choose a CIT to use as the input.
	**Edit Input Query.** Enables you to edit the input query.
	**Remove Input Query.** Enables you to delete the input query.

UI Element (A–Z)	Description
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.) • 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. To define which CIs can be Trigger CIs for jobs that run a specific adapter, see "Input Query Editor Window" on page 158. For more information, see "Trigger CIs and Trigger Queries" on page 24. For an example of an input query definition, see "Example of Input Query Definition" in the *HP Universal CMDB Developer Reference Guide*. **Note:** • Because this field is optional, not all adapters include an Input query. **None** signifies this adapter does not have an Input query definition. • To ensure that the Data Flow Probe is always kept up to date with possible changes to the Trigger CI data, you can configure UCMDB to periodically recalculate the Trigger CI data and send any changes to the Data Flow Probe. For details, see "How to Configure Periodic Data Flow Task Updates" on page 33. This option is disabled by default because it can interfere with performance.
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.

Used Scripts Pane

Displays the scripts used by the selected adapter.

Important Information	Available for Jython adapters only

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

UI Element (A–Z)	Description
	**Move up/Move down.** Enables you to change the order of the scripts. DFM runs the scripts in the order in which they appear here.
	**Add script.** Enables you to add a script to the adapter.
	**Remove script.** Enables you to remove a script from the adapter.
	**Edit.** Enables you to edit the selected script in the Script Editor that opens.
<Scripts>	A list of Jython scripts used by the adapter.

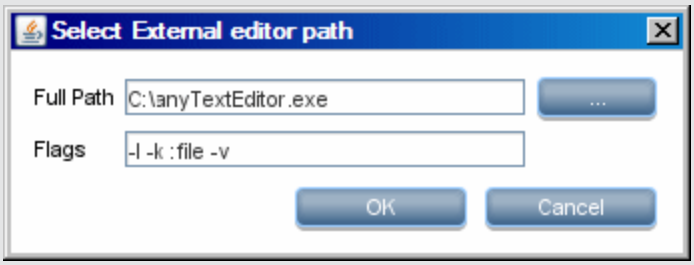
Workflow Steps Pane

Displays only the **workflow** element of the selected adapter script.

Important Information	**Available:** Only for the adapters that contain workflows **Example:** UDAgentManagement adapters

User interface elements are described below:

UI Element (A–Z)	Description
	**Find text.** Enables you to find specific text in the workflow steps. For details, see "Find Text Dialog Box" on page 157.
	**Go to line.** Enables you to jump to a specific line in the workflow steps. In the Go To Line dialog box, enter the line number, and press **ENTER**.
	**Open External Editor.** Opens the workflow steps in an external text editor. **Prerequisite:** Click the **Edit the External Editor Preferences**  button to define the path to an external editor. If no external editor path is defined, you will be prompted to provide one when you try to open the external editor.

UI Element (A–Z)	Description
	**Edit the External Editor Preferences.** Click to edit the external editor preferences. You can run the editor by adding flags to the path. **Note:** You cannot specify the file name. Instead, you can use flags relevant to your external editor to retrieve the file name, such as **:file**. In the following example, **:file** sets the place of the file in relation to the flags.  If no flags are defined, the file name is automatically added to the end of the path.
	**Switch Editor Mode.** Enables you to switch between the default advanced editor and a simple text editor.
Validation Information	Displays if the definition is valid or not: •  . Indicates that the definition is valid. •  . Indicates that there is an error in the definition.

Required Permissions Pane

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

To access	**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 163.

See also	• "Permission Editor Dialog Box" on page 163 • "Discovery Permissions Window" on page 303 • "Viewing Permissions While Running Jobs" on page 274

User interface elements are described below:

UI Element (A–Z)	Description
	**Add.** Opens the Permission Editor dialog box, enabling you to add a permission object. The Permission Editor dialog box opens. For details, see "Permission Editor Dialog Box" on page 163.
	**Edit.** Opens the Permission Editor dialog box, enabling you to edit a selected permission object. For details, see "Permission Editor Dialog Box" on page 163.
	**Remove.** Enables you to delete a selected permission object.
	**Move up/Move down.** Enables you to change the order of the permissions. Select the permission object and click the up or down button. The order given here is the order in which the credentials are verified.
	**Export Data to File.** Enables you to export a permission object in Excel, PDF, RTF, CSV, or XML format. For details, see "Browse Views Mode" in the *HP Universal CMDB 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 required protocol.** Enables you to add a required protocol.
	**Remove required protocol.** Enables you to remove an existing protocol that is no longer required.
<Protocols>	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. For information about the supported protocols, see the *HP Universal CMDB Discovery and Integration Content Guide*.

Discovered CITs Pane

User interface elements are described below:

UI Element (A–Z)	Description
	**Add Discovered CIT.** Opens the Choose Discovered Class dialog box, enabling you to select a CIT to be discovered by the adapter. For details, see "Choose Discovered Class Dialog Box" on page 153.
	**Remove Discovered CIT.** Enables you to remove the CIT from the list of CITs that the adapter discovers.
	**View Discovered CITs as Map.** Opens the Discovered CITs Map window enabling view a graphical map of the CITs and relationships that are discovered by the adapter.
CITs	List of CITs that the adapter discovers.

Global Configuration Files Pane

Enables you to add default configuration files to the adapter, as well as the specific configuration files that the adapter needs.

Important Information	The **applicationsSignature.xml** file contains a list of all applications that DFM attempts to find in the environment. The configuration file **applicationsSignature.xml** opens the Software Library dialog box. For details, see "Software Library Dialog Box" on page 172.
Relevant tasks	"How to Discover Running Software – Scenario" on page 130

User interface elements are described below:

UI Element (A–Z)	Description
	**Add.** Opens the Global Configuration Files dialog box, enabling you to select configuration files that are needed by the adapter.
	**Remove.** Enables you to delete a selected configuration file.
	**Edit.** Opens the selected configuration file in an appropriate editor. For example, the file msServerTypes.xml opens the Script Editor.

Adapter Parameters Pane

User interface elements are described below:

UI Element (A–Z)	Description
	**Add Parameter.** Opens the Parameter Editor dialog box, enabling you to enter details about a new parameter. The value you enter here is assigned to the attribute.
	**Remove Parameter.** Enables you to remove a selected parameter.
	**Edit Parameter.** Opens the Parameter Editor dialog box, enabling you to make changes to the parameter definition.
Name	Each row represents the definitions for one parameter.
Value	Separate values with commas.

Adapter Configuration Tab

Enables you to define additional options relevant to adapter execution and result filtering.

To access	Select a specific adapter in the **Resources** pane and click the **Adapter Configuration** tab.
Important Information	Click the **Save** button to save any changes you make.
See also	"DataFlowProbe.properties File" on page 44

Probe Selection Pane

Enables you to specify which Probe to use with an adapter. For more information, see the section "Override Probe Selection - Optional" in the *HP Universal CMDB Developer Reference Guide*.

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. That is, DFM reports an error (report of a warning does not create a communication log). This is useful when you need to analyze which queries or operations take most of the time, send data for analysis from different locations, and so on. If the job completes successfully, no log is created. When requested (in the Discovery Progress pane), a log retrieved from the Probe is displayed (if a log has been created). For details, see "Discovery Progress Dialog Box" on page 318. **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 "Record DFM Code" in the *HP Universal CMDB 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 **DataFlowProbe.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*.

Results Management Pane

User interface elements are described below:

UI Element (A–Z)	Description
Enable aging	The aging mechanism specifies how long a period must pass in which CIs are discovered, before DFM treats these CIs as no longer relevant and removes them. Choose from one of the following aging options: • **System Default:** Use the system's default value for the Enable Aging attribute of each CI type. • **Always Enabled:** Select this option to always enable the aging mechanism. • **Always Disabled:** Select this option to always disable the aging mechanism. The value you set here is for each CI result that is reported to the UCMDB by the jobs of this adapter. For details on aging, see "The Aging Mechanism Overview" in the *HP Universal CMDB 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).
	Selecting this option enables the **Automatic Deletion** box where you select specific CITs for deletion or as candidates for deletion, if the Data Flow Probe does not find them during its next invocation.
	To select CITs, 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 configuration file, for example:
	`<resultMechanism isEnabled="true">`
	`<autoDeleteCITs isEnabled="true">`
	`<CIT>shell</CIT>`
	`<candidateForDeletionCIT>node</candidateForDeletionCIT>`
	`</autoDeleteCITs>`
	`</resultMechanism>`
	For information about how the Data Flow Probe handles CI deletion, see "Automatically Deleted CIs and Relationships and Candidates for Deletion CIs" on page 126
	Note for Java-based population adapters: In order for CITs to be deleted by the population engine, you must configure the adapter configuration file manually as described in "How to Define CITs to be Deleted by Java-Based Population Adapters" on page 130.

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 the Status of Application Discovery (Rediscover a View)" and "Show Discovery Status and Changes Dialog Box" in the *HP Universal CMDB Modeling Guide*.
Enable reporting of empty values	When selected, the Data Flow Probe reports empty values for discovered properties to UCMDB. **Default:** Enabled
Enable update 'Last Access Time'	When selected, if a CI is touched when a discovery or integration job runs, the **Last access time** property of the CI is updated. This indicates that the CI represents an active component in the system, and prevents the CI from becoming a deletion candidate. For details about the aging mechanism and deletion candidates, see "The Aging Mechanism Overview" in the *HP Universal CMDB Administration Guide*. **Note:** If this option is not selected: • For new CIs, the **Last access time** property is given the same value as the **Create Time** property • For existing CIs, subsequent activations of the job do still update the **LastModifiedTime** property, but the **Last access time** property is not updated. **Use-Case Example** When importing data from an external data source, this data may include meta-data about CIs. If this option is enabled, the CIs are updated with the metadata and their **Last Access Time** value is updated. Disabling this option can be useful if you do not want to affect the aging status or the deletion candidacy of these CIs. In this case, the information is added to the CIs but their Last Access Time remains unchanged.

UI Element (A–Z)	Description
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 CMDB with only the invalid CIs (and their topology) dropped from the results. In the above example, 999 objects would be processed. UCMDB 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	**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 137 • "Global Configuration Files Pane" on page 143 • "Adapter Configuration Tab" on page 144 • "Script Pane" on page 168 • "Resources Pane" on page 164 • "Configuration File Pane" on page 154 • *HP Universal CMDB Discovery and Integration Content Guide*

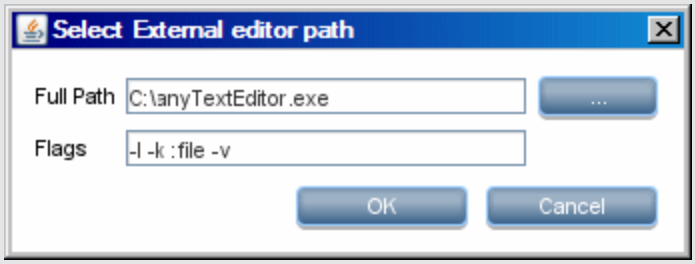
Adapter Source Editor Window

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 164

User interface elements are described below:

UI Element (A–Z)	Description
	**Find text.** Enables you to find specific text in the adapter definition. For details, see "Find Text Dialog Box" on page 157.
	**Go to line.** Enables you to jump to a specific line in the adapter definition. In the Go To Line dialog box, enter the line number, and press **ENTER**.
	**Open External Editor.** Opens the adapter definition in an external text editor. **Prerequisite:** Click the **Edit the External Editor Preferences**  button to define the path to an external editor. If no external editor path is defined, you will be prompted to provide one when you try to open the external editor.

UI Element (A–Z)	Description
	**Edit the External Editor Preferences.** Click to edit the external editor preferences. You can run the editor by adding flags to the path. **Note:** You cannot specify the file name. Instead, you can use flags relevant to your external editor to retrieve the file name, such as **:file**. In the following example, **:file** sets the place of the file in relation to the flags.  If no flags are defined, the file name is automatically added to the end of the path.
	**Switch Editor Mode.** Enables you to switch between the default advanced editor and a simple text editor.
Validation Information	Displays if the definition is valid or not: •  Indicates that the definition is valid. •  Indicates that there is an error in the definition. •  Indicates that the definition could not be validated. **Note:** This may occur due to an internal error while performing the validation. This does not, under any circumstances, harm the process of saving your definition to the server. See **%temp%\UcmdbLog\error.log** for details. For further assistance, contact HP Software Support.

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 130

See also	• "Parse Rule Editor Dialog Box" on page 162 • "Attribute Editor Dialog Box" below • "Software Identification Rule Editor Dialog Box" on page 170

User interface elements are described below:

UI Element (A–Z)	Description
	Click to add a regular expression that determines the attribute of the CI to be discovered, or to add an attribute.
	Click to edit an existing regular expression or attribute.
	Click to delete the regular expression or the attribute.
Attribute assignments for type	For details, see "Attribute Editor Dialog Box" below.
Parsing Rules	For details, see "Parse Rule Editor Dialog Box" on page 162.

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 130
See also	"Parse Rule Editor Dialog Box" on page 162

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.
Type	The type of operation defined for the attribute, for example, Boolean, string, date, and so on.

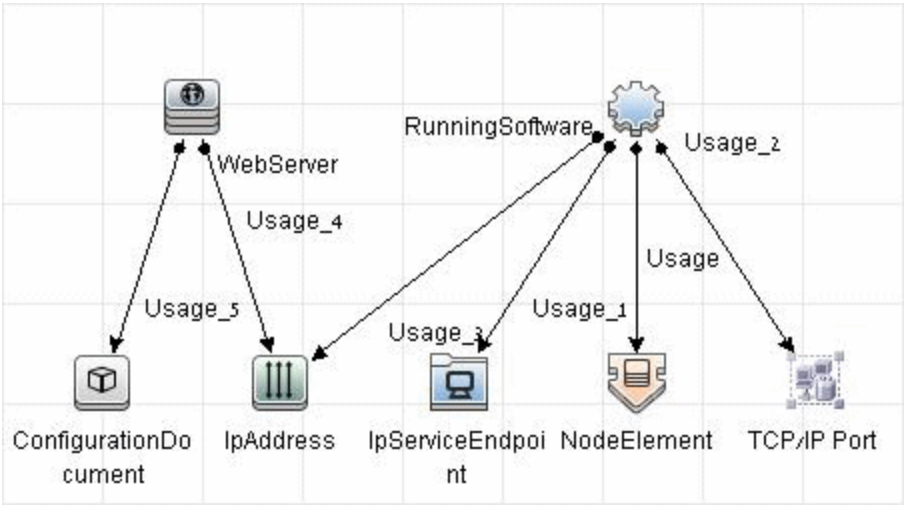
UI Element (A–Z)	Description
Value	The value that replaces the name in the Rule ID field in the Parse Rule Editor dialog box. Use the following syntax for the value: `${<rule ID name>(<group number>)}` For example, **${DB_SID(1)}** means that DFM should search for the Rule ID with the name **DB_SID** and retrieve its regular expression. DFM should then retrieve the code for the first group (**1**). For example, in the regular expression **.+\s+(\w+)$**, the first group is **(\w+)$**, that is, 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	• **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. • **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.

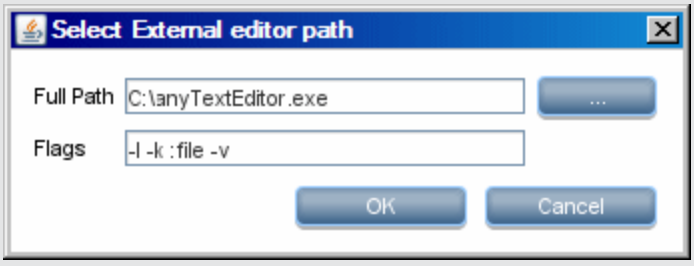
Configuration File Pane

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 Editor is sensitive to the type of file (.xml, .properties, or .groovy) and displays words with context specific meanings as highlighted text. 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 "How to Define Discovery Rules" on page 175 and "Internal Configuration Files" on page 173.

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 157.
	Click to go to a specific line in the configuration file. In the Go To Line dialog box, enter the line number.
	Click to opens the configuration in an external text editor. **Prerequisite:** Click the **Edit the External Editor Preferences**  button to define the path to an external editor. If no external editor path is defined, you will be prompted to provide one when you try to open the external editor.
	**Edit the External Editor Preferences.** Click to edit the external editor preferences. You can run the editor by adding flags to the path. **Note:** You cannot specify the file name. Instead, you can use flags relevant to your external editor to retrieve the file name, such as **:file**. In the following example, **:file** sets the place of the file in relation to the flags.  If no flags are defined, the file name is automatically added to the end of the path.
	Click to toggle between the advanced editor and a simple text editor. You can use the simple editor when the advanced editor causes problems.

UI Element (A–Z)	Description
	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 170

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**.
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 125.
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 (that is, the running software can use any port), select the **All Ports** option.

UI Element (A–Z)	Description
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 (that is, 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 164

User interface elements are described below:

UI Element (A–Z)	Description
	Click to select 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	Click to highlight 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
	• 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	**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.
Important information	To ensure that the Data Flow Probe is always kept up to date with possible changes to the Trigger CI data, you can configure UCMDB to periodically recalculate the Trigger CI data and send any changes to the Data Flow Probe. For details, see "How to Configure Periodic Data Flow Task Updates" on page 33. This option is disabled by default because it can interfere with performance.
See also	• "Trigger CIs and Trigger Queries" on page 24 • "Trigger Query Editor Window" on page 308

User interface elements are described below:

UI Element (A–Z)	Description
<Panes>	• "CI Type Selector Pane" below • "Editing Pane" below • "Information Pane" on next page
Query Name	The name of the adapter's Input query.

CI Type Selector Pane

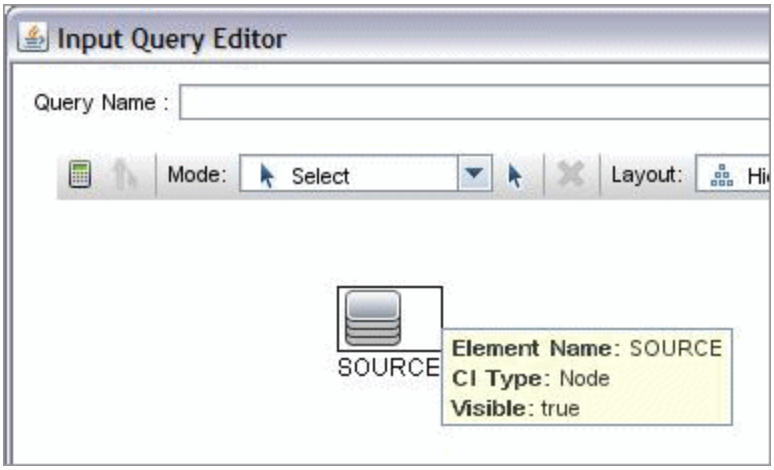
Displays a hierarchical tree structure of the CI Types found in the CMDB. For more details, see "CI Type Manager User Interface" in the *HP Universal CMDB Modeling Guide*.

Note: The number of instances of each CIT in the CMDB is displayed to the right of each CIT.

To access	To create or modify a query, click and drag nodes to the Editing pane and define the relationship between them. Your changes are saved to the CMDB. **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 *HP Universal CMDB Modeling Guide* • "How to Create a Pattern View" in the *HP Universal CMDB Modeling Guide*
See also	"How to Add Query Nodes and Relationships to a TQL Query" in the *HP Universal CMDB Modeling Guide*

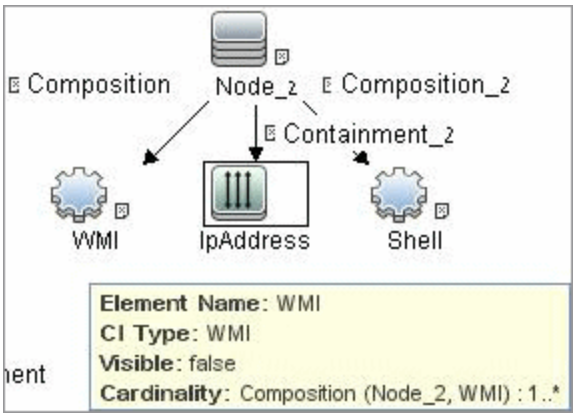
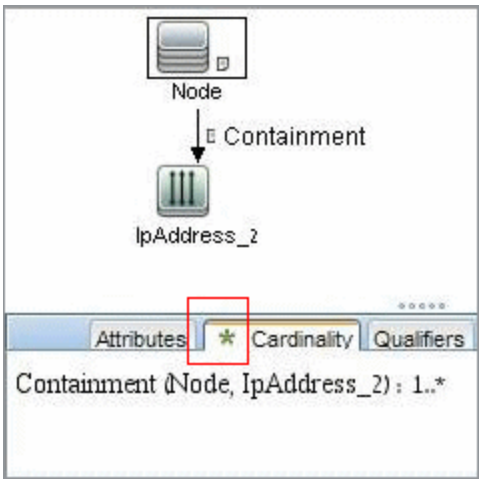
Editing Pane

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 *HP Universal CMDB Modeling Guide*.
<Toolbar>	For details, see "Toolbar Options" in the *HP Universal CMDB Modeling Guide*.

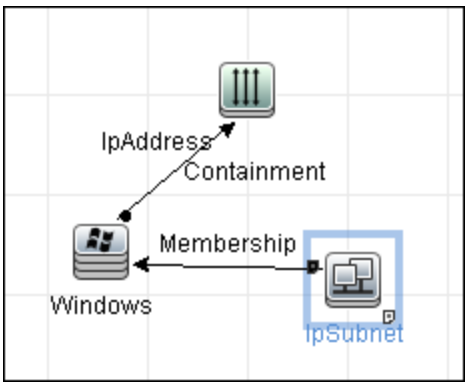
Information Pane

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 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 *HP Universal CMDB Modeling Guide*.

UI Element (A-Z)	Description
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 *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*.
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*.

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 130
See also	• "Attribute Editor Dialog Box" on page 152 • "Software Identification Rule Editor Dialog Box" on page 170

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.
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 171.

Permission Editor Dialog Box

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

To access	**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, that is, if an adapter is changed, the information in this dialog box is not updated.
See also	• "Discovery Permissions Window" on page 303 • "Viewing Permissions While Running Jobs" on page 274 • "Adapter Definition Tab" on page 137 • "Discovery Module/Jobs - Details Tab" on page 292

User interface elements are described below:

UI Element (A–Z)	Description
Operation	The action that is being run.
Permission	Enter a name for the permission, to appear in the Required Permissions pane.
Usage Description	Free text that you enter to describe the permission object and its parameters. This text is usually a general comment on the type of permission object, whereas the description is a more specific comment. For example, you could enter **Permissions for host machines** here, and **Permissions for host machines running on Windows** for a particular row.

Permission Objects and Parameters Pane

UI Element (A–Z)	Description
	Click to open the **Permission Object and Parameter** pane. You can enter more than one object or parameter for each permission. The information you enter in this dialog box appears in the **Required Permissions** pane, in the **Objects and Parameters** column.
	Click to delete a permission object.
	Click to edit an existing permission object.
Context	Specific information about the permission object's environment, for example, Windows or UNIX.
Parameter	The parameters that are needed during the job run. For example, the UNIX permission object `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 activity, and you can import an external resource.

To access	**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 137 and "Adapter Configuration Tab" on page 144. • A script or configuration file: The script editor is displayed. For details, see "Script Pane" on page 168. • An external resource: Information about the file is displayed.
See also	"Package Manager User Interface" in the *HP Universal CMDB Administration Guide*.

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

UI Element (A–Z)	Description
	**Create New Resource.** Enables you to create a resource in a selected package. Select a resource, enter its details, click the ellipsis  button, and select a package to which to add the resource. If you do not select a package, the new resource is created in the **<No Package>** folder: • **New Adapter.** Enter the adapter name. Choose whether it should be used as a discovery adapter or for integration. For integration adapters, choose the integration type from the list of available types. Click **OK**. Edit the adapter. For details, see "Adapter Definition Tab" on page 137 and "Adapter Configuration Tab" on page 144. For details on moving an adapter to a package, see "How to Create a Custom Package" in the *HP Universal CMDB Administration Guide*. For details on creating integration adapters, see "Discovery and Integration Adapters" on page 22. • **New Jython script.** Enter the script name. For details, see "Script Pane" on page 168. • **New Configuration File.** Enter the configuration file name. By default, the file takes an .xml extension. To give the file another extension, for example, `*.properties`, name the file and include the extension. Add the appropriate XML code or other content. For XML files, you can save the file only if it is valid. For details, see "Configuration File Pane" on page 154. • **Import External Resource.** Opens the Select Resources to Import dialog box. **Resources.** Click the ellipsis  to locate the resources that you want to import. You can import more than one file by selecting multiple files at the same time. **Package.** Click the ellipsis  to locate the package that you want to contain the resources. **Path.** Enter a directory path for the resources. • **New Discovery Wizard.** Name the new wizard. By default, the file takes an .xml extension. The file is in template format. • **New Scanner Configuration** Configure the new scanner using the Scanner Configuration Generator wizard. For more information see section about the "Scanner Generator Wizard" on page 384.
	**Delete the Selected Item.** Deletes the resource.
	**Find Resource.** Opens the Find Resource dialog box. For details on filtering, see "Filtering Results" on page 30.
	**Refresh.** Refreshes the list of packages.

UI Element (A–Z)	Description
	**Packages tree.** Displays a list of all packages.
	**Package root.** Displays a list of all resources included in the package. Expand the folders to see available resources: Right-click a resource to do one of the following: • **Save As.** Enables you to clone an existing resource. The new resource includes all attributes of the existing resource. Give the resource a name, and click the ellipsis  button to select a package to which to add the resource. • **Delete**. Enables you to delete the resource. The resource is removed completely from the system. • **Open in Frame.** Enables you to view or edit the resource script in the Script Editor. **Available for**: Configuration files and scripts • **Go to Discovery Job.** Enables you to open the discovery job associated with the selected adapter in the Discovery Control Panel **Available for**: Adapters only. This option is enabled if the adapter is included in a discovery job. • **Go to Integration Point.** Enables you to view and edit the integration point that uses this adapter in the Integration Studio. **Available for**: Adapters only. This option is enabled if the adapter is used by an integration point. • **Edit Adapter Source.** Enables you to view or edit the adapter's XML file in the Adapter Source Editor. For details, see "Adapter Source Editor Window" on page 150. **Available for**: Adapters only.

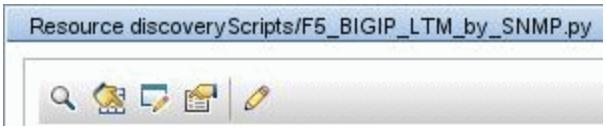
Script Editor Window

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 next page.

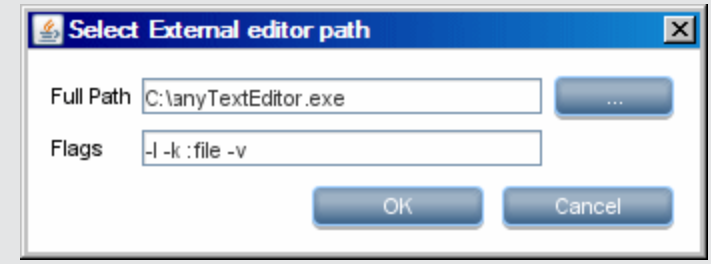
Script Pane

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 *HP Universal CMDB Developer Reference Guide*

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

UI Element (A–Z)	Description
	**Find text.** Enables you to find specific text in the script definition. For details, see "Find Text Dialog Box" on page 157.
	**Go to line.** Enables you to jump to a specific line in the script definition. In the Go To Line dialog box, enter the line number, and press **ENTER**.
	**Open External Editor.** Opens the script definition in an external text editor. **Prerequisite:** Click the **Edit the External Editor Preferences**  button to define the path to an external editor. If no external editor path is defined, you will be prompted to provide one when you try to open the external editor.

UI Element (A–Z)	Description
	**Edit the External Editor Preferences.** Click to edit the external editor preferences. You can run the editor by adding flags to the path. **Note:** You cannot specify the file name. Instead, you can use flags relevant to your external editor to retrieve the file name, such as **:file**. In the following example, **:file** sets the place of the file in relation to the flags.  If no flags are defined, the file name is automatically added to the end of the path.
	**Switch Editor Mode.** Enables you to switch between the default advanced editor and a simple text editor.
	See "Validation Information" on next page. **Note:** This button is displayed when a script contains Framework API errors.
<script definition>	The Jython script used by the package. For details on working with Jython, see "Create Jython Code" in the *HP Universal CMDB Developer Reference Guide*.

UI Element (A–Z)	Description

Validation Information	Displays if the script definition is valid or not:
	•  . For Jython files, indicates that the script definition is valid.
	•  . For Jython files, indicates that the script definition is not valid, and displays the errors in the script.
	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  , then **OK** to update the script.
	The error may occur due to changes in the Framework object's API. For details, see the *HP Universal CMDB Developer Reference Guide*.
	•  . For Jython files, indicates that the script definition could not be validated.
	Note: This may occur due to an internal error while performing the validation. This does not, under any circumstances, harm the process of saving your definition to the server. See **%temp%\UcmdbLog\error.log** for details. For further assistance, contact HP Software Support.

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 > applicationsSignature.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 130
See also	"Global Configuration Files Pane" on page 143

User interface elements are described below:

UI Element (A–Z)	Description
	Click to add attributes to the component. For details, see "Attribute Assignment Editor Dialog Box" on page 151.
	Click to open the Optional Configuration Files dialog box.
	Click to add a process.
	Select a process and click to delete.
	Select a process and click to edit.
Additional Attributes	To add attributes, click the Set Attributes button. For details, see "Attribute Assignment Editor Dialog Box" on page 151.
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 156.
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 Files** pane in the **Adapter Definition** tab. Select **applicationsSignature.xml** and click the **Edit** button.
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 170. 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 130
See also	"Global Configuration Files Pane" on page 143

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.
	Click to define a new software element. For details, see "Software Identification Rule Editor Dialog Box" on page 170.
	Select a software element and click to delete the element.

UI Element (A–Z)	Description
	Select a software element and click to make changes to the element. For details, see "Software Identification Rule Editor Dialog Box" on page 170.
<List of software elements>	List of objects that are software elements.

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 "New/Edit Policy Dialog Box" on page 66. Located in **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 **Data Flow Management > Adapter Management > Packages > AutoDiscoveryContent > Configuration Files**.

Chapter 6

Discovery Rules Engine

This chapter includes:

Discovery Rules Engine Overview

When Universal Discovery discovers data, the Discovery Rules Engine processes the given set of input data, and returns a set of output attribute values.

For example,

- **Input:** A Node contains the string **Cisco** and the string **Version 12.3a**,
- **Output :** The operating system for the Node is recognized as **Cisco IOS Version 12.3(3a)**.

The Data Flow Probe then activates the Rules Engine to fill in additional information on the discovered data.

All discovery jobs use the discovery rules engine. Out of the box rules are applied to data that can be completed by the discovery jobs (sys_object_id, mac_address etc.). Moreover, you can add user-defined rules to the Discovery Rules Engine.

Limitations

- The Discovery Rules Engine completes only empty fields in the UCMDB. It does not overwrite existing values.
- Rules run in a random order. User-defined discovery rules have no priority over out-of-the-box discovery rules. If the input suits more than one rule, the output is returned from the rule that ran first. It is important to ensure that rules are accurate (existing and new rules). If rules are accurate there is no need for prioritization.
- There are no dependencies between rules. A field that was completed using the Discovery Rules Engine cannot be used as input for another rule.

See Also

- For details on the syntax of Discovery Rules, see "Discovery Rules Syntax" on page 1.
- For details on defining new rules, see "How to Define Discovery Rules" on next page.

- For details on viewing out-of-the-box rules, see "How to View Discovery Rules in JMX" on next page.
- To disable the Rules Engine on a particular population adapter, see "How to Disable the Discovery Rules Engine" on next page.
- For details on log files, see "Discovery Rule Engine Log Files" on page 177.

How to Define Discovery Rules

This task describes how to define a new discovery rule in the Discovery Rules Engine.

If you are working on an upgraded version of UCMDB, you can also edit user-defined rules from your previous version.

To learn more about the Discovery Rules Engine, see "Discovery Rules Engine Overview" on previous page.

To add new user-defined discovery rules:

1. Go to **Adapter Management**.
2. In the Resources pane, click **New**  , and select **New Configuration File**.

   Enter a name for the new discovery rule. The name must begin with **ruleEngine/** and end with **.xml**.

   For example: **ruleEngine/myRule.xml**.
3. In the Package field, select **NormalizationRules**.
4. In the Editor pane that opens on the right, enter the new rule.

   An example of valid rules can be found under **NormalizationRules > Configuration Files, in ruleEngine/samples.xml.**
5. Click **OK**.

To edit an existing discovery rule from a upgraded version of UCMDB:

1. Go to **Adapter Management**.
2. In the Resources pane, select the **UserDefinedRules** package.
3. Under **Configuration Files**, select the .xml file for the rule that you want to edit.

   Note:

   - Rules that were defined in previous versions of UCMDB (for example in **oidToHostClass.xml**), can be found under the **UserDefinedRules** package, in the configuration file **UserDefinedOidToHostClass.xml**.
   - Out-of-the-box **OidToHostClass** rules can be found under **NormalizationRules > External resources** in the **ruleEngine/snmp.gz** file.

How to View Discovery Rules in JMX

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

To search for a rule:

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

Command	Description
scanForSNMPRules	Retrieves SNMP discovery rules that apply to the specified input attributes. **Note:** ▪ the **sys_object_id** value must always have a leading "." ▪ Leave empty to ignore
scanForScanFileRules	Retrieves Scan File discovery rules that apply to the specified input attributes. **Note:** Leave empty to ignore
viewNormalizationRuleById	Retrieves discovery rules by ID
viewNormalizationRuleByNiceId	Retrieves discovery rules by user friendly ID (NiceRuleID), **Example:** 4323@SNMP
viewNormalizationRules	Retrieves discovery rule outputs that apply to the specified input attributes **Format:** ▪ Pair attributes in the following format: **attrName;attrValue** ▪ Pairs must be separated by commas. **Example:** Name;HP,Version;10

How to Disable the Discovery Rules Engine

All population adapters are set up, by default, to use the Discovery Rules Engine adapters.

To disable the Discovery Rules Engine for a particular population adapter:

1. In **Adapter Management**, open the population adapter's configuration file (<adapter>.xml).
2. Search for the following parameter: **normalizationRules isEnabled**
   - If you find it, ensure that the value is set to **false**.
   - If you do not find it, add the following line under the **taskinfo** tag: **<normalizationRules isEnabled="false"/>**

Discovery Rule Engine Log Files

The section describes the Discovery Rules Engine log files. These files can be found in <Data Flow Probe Installation>\runtime\log\.

normalization.audit.log

Logs information about the processing of the Discovery Rules Engine.

Level	Description
Information	Audits the number of element processed and the number of CIs that were changed. **Example:** Normalization (OSHV: 8 elements) (Time: 125 ms) (Modified CIs: 1)

normalization.log

Logs detailed information about the processing of the Discovery Rules Engine, enabling you to trace detailed information of the Discovery Rule Engine process.

Level	Description
Error	All discovery rule processing errors.
Information	Logs all levels of information about the processing of the Discovery Rules Engine.
Debug	Logs mainly for debugging purposes.

Basic Troubleshooting. Check this log when you need to analyze why a CI was not enriched by the Discovery Rules Engine.

Performing Integration

Chapter 7

Integration Studio

This chapter includes:

Integration Studio Overview

The Integration Studio is where you manage your UCMDB integration points and connect and share information with external repositories, such as other CMDBs, IT Performance Suite products, or third-party products.

Integration with other products is performed over secure communication channels through Data Flow Probes.

Alternatively, if your remote managed data repositories are accessible from the UCMDB server machine, non-Jython-based integrations can be performed using the HP UCMDB Integration service, enabling the Data Flow Probe resources to be used for other discovery tasks.

Integration points in the CMDB are based on adapters, which are entities that are capable of communicating with external data repositories. A basic set of adapters is provided with the CMDB; however, you can create additional adapters using the Federation Framework SDK. For details, see "Add an Adapter for a New External Data Source" in the *HP Universal CMDB Developer Reference Guide*.

You can also create adapters in the Adapter Management module. For details, see "Resources Pane" on page 164.

For details about how to set up integration points for data integrations, see "Integration Studio Page" on page 206.

Integration points can be of one of the following types:

- "Population" below
- "Federation" below
- "Data Push" on page 182

Population

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

You use population in one of the following scenarios:

- When you need to track changes made by the CMDB at the CI level.
- When a remote repository is not reliable in terms of response time; for example, a network delay prohibits you from setting up run-time federation with the repository.
- When a remote repository does not support federation capabilities (no appropriate adapter exists).

Federation

An integration of Federation type includes data in the CMDB from other sources in such a way that the source of the data still retains control of the data.

You use the CMDB's federation capabilities to extend the scope of the existing Topology Query Language (TQL) capabilities to encompass data that is stored and maintained in an external repository. The ability to include such information is important as it prevents you from having to copy large amounts of data and, instead, bring it into your CMDB only when it is really needed.

Federation also has the benefit that the federated data does not burden the CMDB in terms of capacity; theoretically, you can set up an integration that federates trillions of CIs and relationships. Federated data is fetched at runtime, as requested, which lessens the impact on system performance.

Note: The CMDB does not offer change tracking on federated data because the data does not reside within the CMDB and the CMDB is not notified when external data is modified.

Federated integration creates a federated integration point, which can then be used when defining TQL queries. For details on TQL, see "Topology Query Language" in the *HP Universal CMDB Modeling Guide*.

Note: Federation can be configured in Actual state only, but can be performed in either Actual or Authorized state.

Retrieving Data from Multiple Federated Data Sources

During TQL query calculation, you can retrieve data for the same CIT from several federated data sources. The data is retrieved from the local CMDB, as well as from other federated data sources, according to how you have configured integration points. As data arrives at the CMDB, it is identified and reconciled, with the end result determined according to the configured reconciliation priority given to the various integrations.

Each CI that is retrieved from an external data repository includes an attribute (**Created By**) to show from which federated data source the CI has been retrieved.

For limitations, see "Limitations" on page 219.

Retrieving Attributes from an External Data Repository

- You can retrieve the attributes of a CI from an external data repository, when the core CI data is stored in the CMDB.
- The core data repository must be the CMDB.
- The CIT must be located in a data repository for its attributes to be defined.
- The same attributes can be retrieved from multiple data repositories.
- For details on retrieval options, see the CI Type Retrieval Mode field on the "Federation Tab" on page 196.
- When you configure an integration point to include federated CIs, you must select full federation of a CI or the federation of an attribute alone. You cannot set up two integrations for the same CIT where one is mapped to an external CIT and the other is mapped to that same CIT with an external attribute.
- A CIT can support external attributes if the adapter (which is federating the CIT data) supports mapping information (reconciliation) for this CIT.

Reconciling Information

Federated queries should use the mapping file to reconcile the CI from the CMDB with the attributes from the external data repository.

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

For details on selecting attributes to be included in the federation, see "Federation Tab" on page 196.

For details on how reconciliation is performed, see "Entity Reconciliation" on page 479.

Use Cases

- You need to discover the SMS or Altiris desktops in your system. The desktop CIT is a core CIT and is already synchronized with the CMDB. However, you do not want to store all the desktop data in the CMDB as this is inefficient and unnecessary. It is enough to store core attributes such as name and MAC address in the CMDB, and to define the other details of the desktops as external attributes in two data repositories: SMS and Altiris.
- VMware creates virtual machines that contain a virtual machine monitor (hypervisor) that allocates hardware resources dynamically and transparently. Multiple operating systems can run concurrently on a single physical computer. Since the allocation resources—for example,

memory—are dynamic, DFM cannot discover these resources (DFM runs once every 24 hours and the resource data can change hourly). To enable UCMDB to always be updated with real-time data, the solution is to divide the data into two: the core data of the virtual hosts should be discovered and placed in the CMDB; the resource attributes should be retrieved from the external source. In this use case, the data for these attributes is retrieved from two data repositories: CMDB and VMware.

Data Push

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

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

For limitations on Data Push jobs, see "Limitations" on page 219.

Integration in a Multi-Tenancy Environment

When executing integration queries or jobs in a multi-tenancy environment, all CIs and relationships that are federated or populated from the remote data source are assigned an owner tenant.

If the data source environment is multi-tenancy aware, when you run a query or a job, only the CIs and relationships of those tenants that you have permissions to view are federated or populated. The owner tenant value is brought in with all of the other attributes.

If the data source environment is not multi-tenancy aware, when you run the query or a job, UCMDB automatically assigns a specified owner tenant value to each of the federated/populated CIs and relationships. For details about selecting an owner tenant value to assign to federated/populated CIs and relationships, see "New Integration Point/Edit Integration Point Dialog Box" on page 210.

HP UCMDB Integration Service

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

This enables running non-Jython-based integrations without using Data Flow Probe resources that may be better used for other discovery tasks.

For information on using the HP UCMDB Integration Service to run integrations, see "How to Set Up an Integration Point" on page 186.

Note:

- The HP UCMDB Integration Service must be started on the UCMDB Server.
- If there is a Data Flow Probe installed and running on the UCMDB Server machine, you must first stop the Data Flow Probe before you can start the UCMDB Integration Service. For details, see "How to Check the HP Universal CMDB Integration Service Status" on page 194.
- The HP UCMDB Integration Service on Linux supports the following integrations:
  - HP SIM
  - HP SE
  - HP NNMi
  - EMC Control Center
  - CMS Sync

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 " below
- "Set a reconciliation priority" below
- "View Instances in IT Universe Manager" below
- "View Reports" below

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 186.

2. Set a reconciliation priority

   In the Integration Point pane, right-click the integration, and select **Reconciliation Priority Manager** from the shortcut menu. For more details, see "Reconciliation Priority Window" on page 502.

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 *HP Universal CMDB Modeling Guide*.

4. View Reports

   You can view reports about the integration in the Modeling Studio. For details see the section about reports in the *HP Universal CMDB Modeling Guide*.

How to Work with Population Jobs

This task explains how to schedule population jobs and select the queries that are used to populate the CMDB with data.

This task includes the following steps:

- "Create an integration point" below
- "Set a reconciliation priority" below
- "Run the population job" below
- "Build a view of the population results" below
- "View instances in IT Universe Manager" below
- "View reports" below

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 186.

2. Set a reconciliation priority

   In the Integration Point pane, right-click the integration, and select **Reconciliation Priority Manager** from the shortcut menu. For more details, see "Reconciliation Priority Window" on page 502.

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 197.

   Select the job.

   - To synchronize all data for the first time, click the **Full Synchronization**  button.
   - To synchronize only the data changes since the job last ran, click the **Delta Synchronization**  button.

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 *HP Universal CMDB Modeling Guide*.

5. View instances in IT Universe Manager

   For details about viewing the CI instances, see "Working with Views in IT Universe Manager" in the *HP Universal CMDB Modeling Guide*.

6. View reports

   You can view reports about the integration in the Modeling Studio. For details see the section about reports in the *HP Universal CMDB Modeling Guide*.

How to Work with Data Push Jobs

This task explains how to schedule data push jobs and select the queries that are used to send data from the CMDB to another data repository.

This task includes the following steps:

- "Create an integration point" below
- "Set Reconciliation priority" below
- "Run the Data Push job" below
- "Build a view of Data Push results" on next page
- "View instances in IT Universe Manager" on next page

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 next page.

2. Set Reconciliation priority

   In the Integration Point pane, right-click the integration, and select **Reconciliation Priority Manager** from the shortcut menu. For more details, see "Reconciliation Priority Window" on page 502.

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 197.

   Select the job.

   - To synchronize all data for the first time, click the **Full Synchronization** button.
   - To synchronize only the data changes since the job last ran, click the **Delta Synchronization** button.

   Note:

   - If CIs in a data push job fail, the query is displayed in the Query Status tab with the status: **Passed with failures**. You can drill down to see the errors that occurred and the CIs affected. This error data is saved in the system. When the job runs again to synchronize changes, UCMDB remembers the failed CIs and repushes these as well.
   - You can define a limit on the number sequential CI failures allowed during a running data push job. When this limit is reached, the job automatically stops running, enabling you to troubleshoot the reason for so many failures before waiting for the entire job to end.

     In the Administration module's Infrastructure Setting Manager, select **Integration Settings** and set the value of **Maximum number of data push job failures allowed in a sequence**. The default value for this setting is **20,000**.
   - If, since the last synchronization, you have changed a TQL query (other than changes to conditions on existing nodes), all data is synchronized and the following message is written to the log: **TQL was changed between syncs - performing Full sync!**
   - **High Availability environment:** If a data push job is running, and the UCMDB

Server responsible for write requests becomes unavailable or is changed, the data push job fails. You can wait for the next invocation of the job schedule, or alternatively rerun the data push job manually.

- You can control the way the job handles null value attributes in the Adapter Configuration tab. For details, see "Results Management Pane" on page 146.

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 *HP Universal CMDB Modeling Guide*.

5. View instances in IT Universe Manager

   For details about viewing the CI instances, see "Working with Views in IT Universe Manager" in the *HP Universal CMDB 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" below
- "Create an integration point" below
- "Add the integration jobs and schedule the jobs to run" on next page
- "For a federation-type integration, define the data to be federated" on next page
- "Save the integration point" on next page

1. Prerequisites

   The integration adapter must be correctly configured before setting up the integration.

   - **Pre-configured Integration Adapters:** These are provided out-of-the-box with the product. It is recommended to use the adapters as they come, without any further configuration.

     However, if you do need to modify the adapter configuration, you are encouraged to do this from the Adapter Management module rather than manually. For details about adapter configuration, see "How to Configure Adapter Settings" on page 127.

   - **New External Data Source Adapters:** To configure an adapter for an new external data source, see "Add an Adapter for a New External Data Source" in the *HP Universal CMDB Developer Reference Guide*.

2. Create an integration point

   In UCMDB, select **Data Flow Management > Integration Studio**, and click the **New**

Integration Point button. For user interface details, see "New Integration Point/Edit Integration Point Dialog Box" on page 210.

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 213.

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 *HP Universal CMDB Discovery and Integration Content Guide*.

e. Configure the adapter's protocol credentials, where required. For a list of supported protocols, see the *HP Universal CMDB Discovery and Integration Content Guide*.

f. Select the Probes to use for the integration.

> **Note:** If your remote managed data repositories are accessible from the UCMDB server machine, you can use the UCMDB Integration Service instead of a Data Flow Probe to run non-Jython-based integrations.
>
> In this case, in the **Probe Name** box, select **UCMDB Integration Service**.
>
> If **UCMDB Integration Service** does not appear in the **Probe Name** list, ensure that the UCMDB Integration Service is running on the UCMDB Server machine. For details, see "How to Check the HP Universal CMDB Integration Service Status" on page 194.

g. **For Jython-based 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 207.

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 196.

5. Save the integration point

   When you are finished, click **OK**. The integration point is automatically saved.

How to Save an Integration Point Configuration as an Adapter Default

You can save an integration point configuration as an adapter default. This is useful if you want to use an integration point's configuration to create other integration points with a similar configuration.

This task describes how to save an integration point configuration as an adapter default.

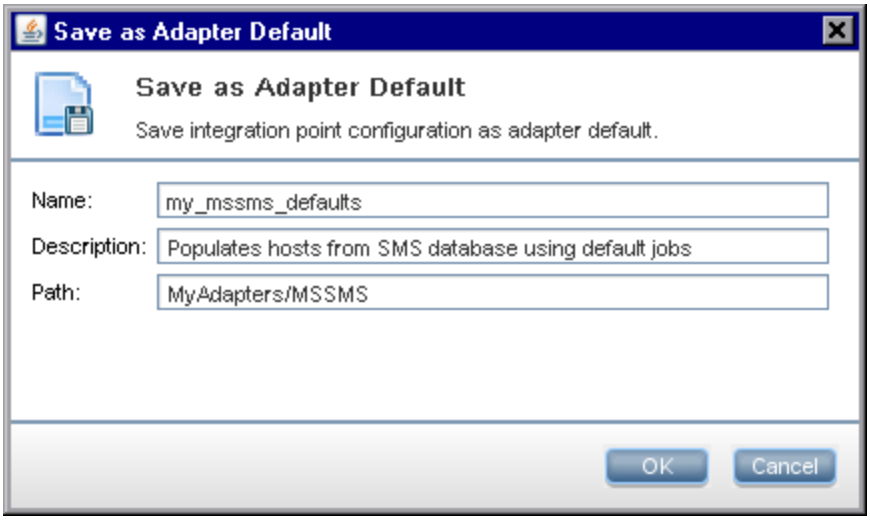
1. **Prerequisites**
   a. Define an integration point based on a particular adapter. For example, MSSMS, based on the Microsoft SMS adapter.
   b. Define population or push jobs and federation details.
   c. Save the integration point.
2. **Save the integration point configuration as an adapter default**
   a. In the Integration Point pane, right-click the integration point that you created, and select **Save as Adapter Default**.
   b. In the Save as Adapter Default dialog box, enter details for the adapter default as follows:
      - **Name and Description.** A name for the adapter default and a description.

        Caution: If you give the adapter default the same name as an existing adapter default, UCMDB treats this as though you are redefining the existing adapter default, and the new definition overwrites the existing definition. If you do not want to overwrite an existing adapter default, give the new adapter default a different name.

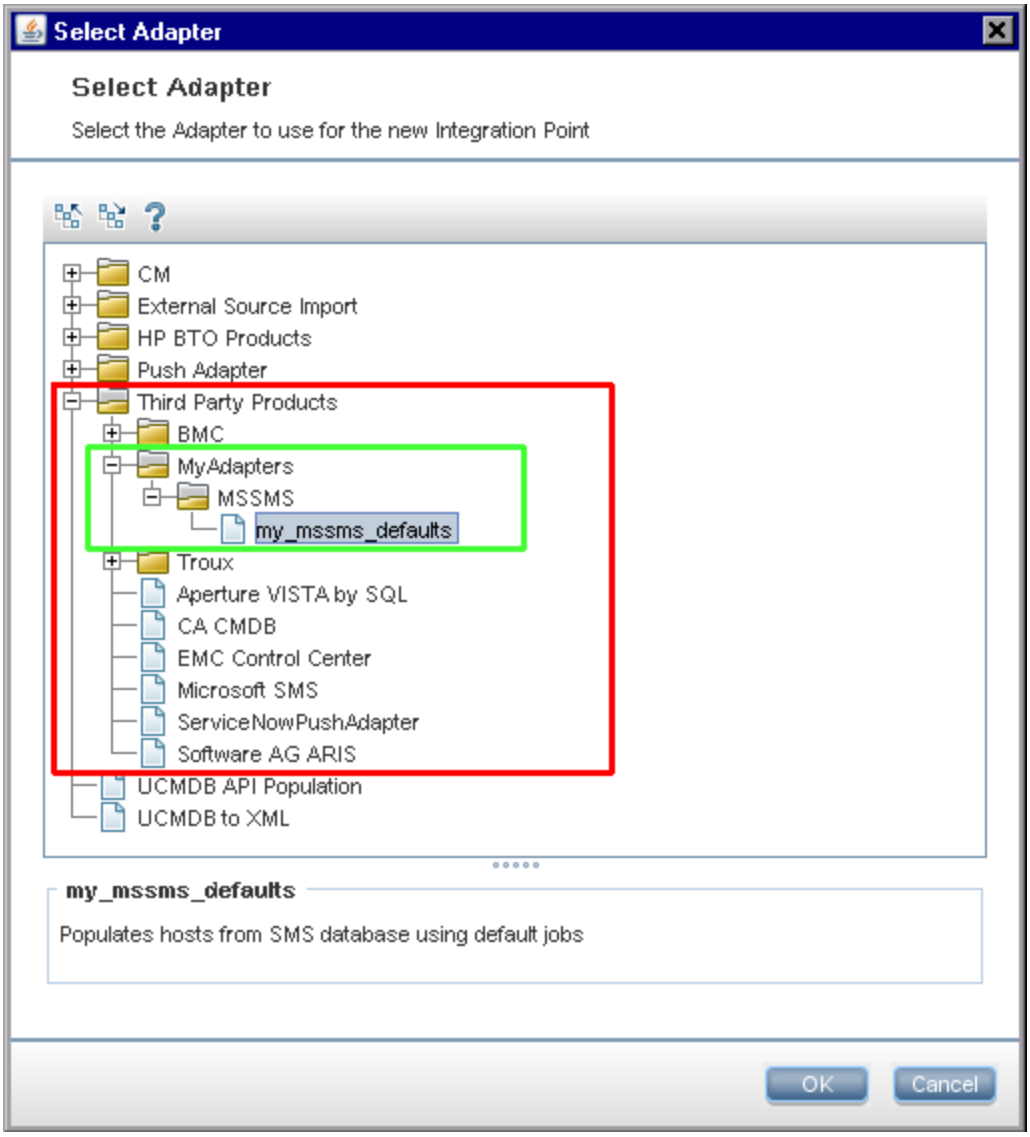
      - **Path.** (Optional) The path to the folder under which your adapter should be displayed in the Select Adapter dialog box (when creating a new integration point). The adapter default is displayed under the same category as the adapter that was originally used to create the integration point, in the path that you define here.

        Note:
        - Use only forward slashes (/) in the path.
        - If you define a new folder in the path, the adapter default is displayed in that folder, under the same category as the original adapter.
        - If you leave the path empty, the adapter default is displayed directly under the same category as the original adapter.

Using the MSSMS integration point example introduced in the Prerequisites section above, you could save this integration point as an adapter default, calling it **my_mssms_defaults** and defining the path as **MyAdapters/MSSMS**.



The next time you create a new integration point, the **my_mssms_defaults** adapter default is displayed under the **Third Party Products** category (because the out-of-the-box Microsoft SMS adapter appears under this category), in the **MyAdapters>MSSMS** folder, as you specified in the path:



3. **Results**
   - When you save the adapter default, integration point parameters that are not related to the connection itself are saved in the adapter default definition.
   - The code for the adapter default is added to the adapter's xml file. To delete the adapter default, see "How to Remove Adapter Defaults" below.

How to Remove Adapter Defaults

To remove an adapter default, you must delete the code that defines it from its base adapter's .xml file.

To remove an adapter default:

1. Locate the adapter on which the adapter default was based. (**Adapter Management > Resources** pane).

   Tip: Alternatively, you can access the adapter from the Integration Point pane by right-clicking the relevant integration point and selecting **Go To Adapter**.

2. Right-click the adapter and click **Edit Adapter Source**.
3. In the adapter's .xml file, locate the following line:

   - **Non-Jython adapters:**
     `<adapterTemplate name="<adapter_default>" description="">`
   - **Jython adapters:**
     `<adapterJythonTemplate name="<adapter_default>" description="">`

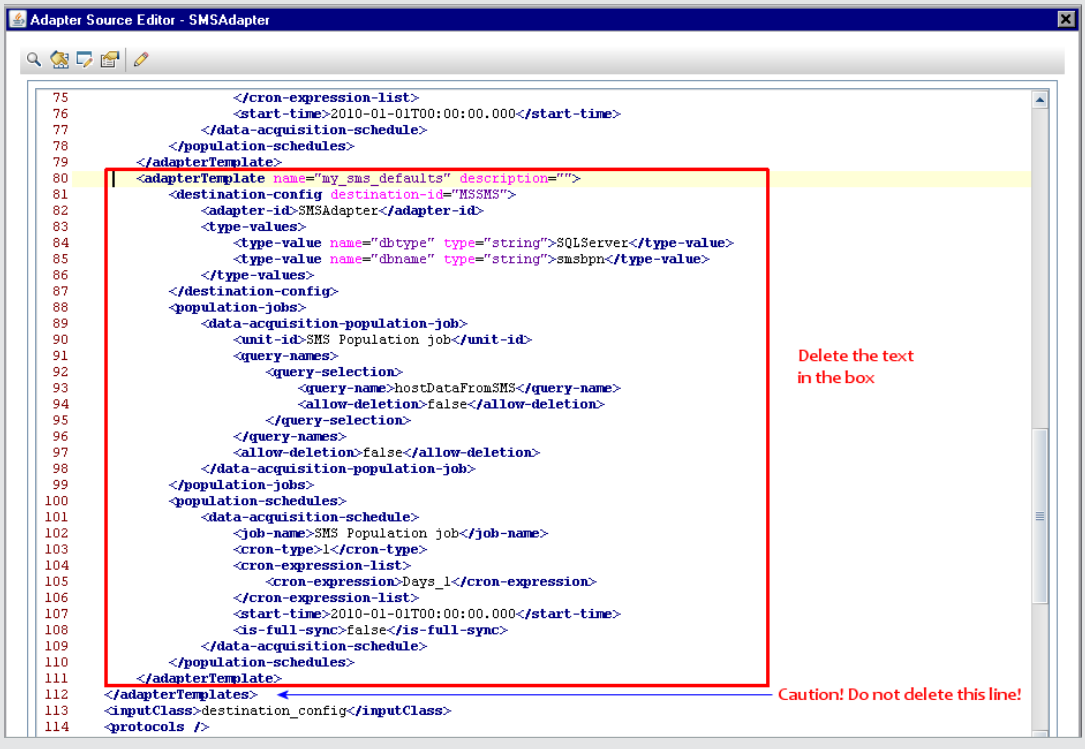
   where **adapter_default** is the name of the adapter default.

4. Delete the all the code from this opening tag to the closing `</adapterTemplate>` (or `</adapterJythonTemplate>`) tag.

   Caution: Do not delete the following line: `</adapterTemplates>`

5. Save your changes.

Example



How to 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 216.

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 to which the package is to be deployed.

This task includes the following steps:

- "Prerequisites" below
- "Change timeout - optional" below
- "Select the integration point" on next page
- "Select the package" on next page
- "View deployment results" on next page
- "View Log files" on next page

1. Prerequisites
   - Verify that the Data Flow Probe is configured correctly and is connected to UCMDB.
   - Verify that the version of UCMDB running on the remote machine is version 9.02 or later.
   - Verify that UCMDB running on the remote machine is up and running.
   - Create the package that must be deployed to the remote machine, and deploy this package to the local UCMDB Server.

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

   - Create an integration point on the local UCMDB Server, that uses the **UCMDB 9.x/10.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.

To change the default: Select **Administration > Infrastructure Settings Manager > Integration Settings > Remote package deploy Timeout**. (The refresh rate indicates when the change takes effect in UCMDB after the value is modified.)

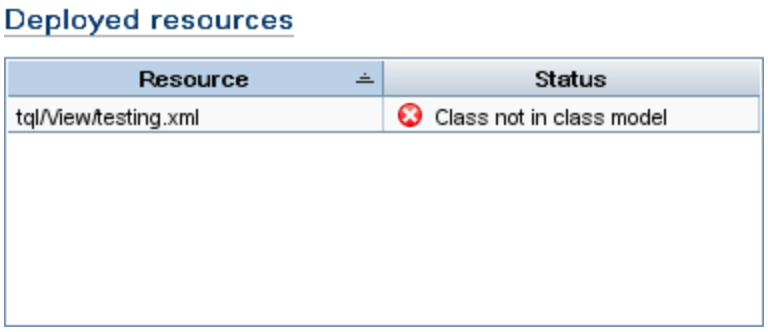
3. Select the integration point
   a. In the Integration Point pane, select the integration point that you created in "Prerequisites" on previous page. For details, see "Integration Point Pane" on page 203.
   b. Click the **Deploy Remote Package** button.
4. Select the package
   a. In the Deploy Remote 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 "Prerequisites" on previous page. For details, see "Deploy Package to Remote Data Repository using <Integration Point>" on page 195.
   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:

6. View Log files

   The following table shows the locations of the log files that record any issues that might arise during deployment:

Location	Log File Name
Remote UCMDB machine, version 9.02 or later	ucmdb-api.log mam.packaging.log
Data Flow Probe	probeTasks.log probe-infra.log adapters.log
Local UCMDB machine	ucmdb-api.log

If a resource fails to deploy, an error is displayed in the Status column as well as in the log file on the remote machine.

How to Check the HP Universal CMDB Integration Service Status

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

To use this service, ensure that it is running on the UCMDB Server machine:

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

To start the service if the service is not running, do the following:

- **Windows:**
  - Select **Start > Programs > HP UCMDB > Start HP UCMDB Integration Service**
  - Select **Start > Control Panel > Administration Tools > Services**, and start the **UCMDB Integration Service**
- **Linux:** Enter the following command:
  /opt/hp/UCMDB/UCMDBServer/integrations/bin/service.sh start

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

To stop the Data Flow Probe:

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

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 197.
- View results for jobs that have run. For details, see "Statistics Tab" on page 200.

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 207

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 203.
Relevant tasks	"How to Deploy a Package to a Remote Data Repository" on page 192

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 *HP Universal CMDB Modeling Guide*.

To access	Select the Federation tab on the Integration Studio page.
Important information	This tab is enabled only when data federation is supported by the adapter on which you are basing your integration point.

User interface elements are described below:

UI Element (A-Z)	Description
	Click to clear all selected items.
	Click to invert the selections.
	Click to expand the entire hierarchical tree structure.
	Click to collapse the hierarchical tree structure.

UI Element (A-Z)	Description
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 CMDB. • **Retrieve the attribute from the UCMDB too.** The attribute can be federated as well as physically retrieved from the CMDB (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 *HP Universal CMDB 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.

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 183 • "How to Work with Data Push Jobs" on page 184
See also	• "Discovery Scheduler Dialog Box" on page 304

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 207.
	**Edit Integration Job.** Enables you to edit an existing integration job.
	**Delete Integration Job.** Deletes the selected integration job from the list.
	**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 Job - Synchronize Changes.** Runs the selected population or data push job and synchronizes only the changes in the data since the last time the job was run. 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. • If CIs in a data push job fail, the query is displayed in the Query Status tab with the status: **Passed with failures**. You can drill down to see the errors that occurred and the CIs affected. This error data is saved in the system. When the job runs again to synchronize changes, UCMDB remembers the failed CIs and repushes these as well. For details, see "Query Status Tab" on page 201.

UI Element (A-Z)	Description
	**Run Job - Synchronize All Data.** Runs a full population or data push job. This job copies or pushes all the relevant data for the job. **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.
	**Stop Running Job.** Stops running the selected job. **Available for:** Data Push jobs only
	**Clear Probe Results Cache.** Clears the cache of all job results for this integration from the Data Flow probe as well as the last time the data was synchronized. The next time you run a synchronization, all the data is synchronized again. **Available for:** Population jobs only
<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 144. **Available for:** Population jobs based on Jython adapters only.
Job Name	Name given to the population or data push job.
Last Synchronization Type	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. **Available for:** Data push jobs only

UI Element (A-Z)	Description
Status	**Population jobs:** • **Waiting for Probe.** The job is waiting to be received by the Probe. • **Did not run.** The job has been received by the Probe but the Probe is not yet ready to run the job. • **Preparing to run.** The Probe is preparing to run the job. **Note:** The status is preceded by another instance of the **Waiting for Probe** status, but this time **Waiting for Probe** indicates that the Probe is now ready to prepare the job for the run. • **Running.** The job is running. • **Completed Successfully.** The job ran successfully. • **Completed.** The job ran successfully but errors or warnings were reported. See details on the errors or warnings in the "Query Status Tab" on next page. • **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**. • **Completed.** The job ran successfully but errors or warnings were reported. See details on the errors or warnings in the "Query Status Tab" on next page. • **Completed Successfully.**. The last run was successful. • **Failed**. The last run was not successful.
Start time / Finish time	The time that the integration job actually started running, and when it finished running. These columns are refreshed every time the job goes into the **Running** state. **Available for:** Population jobs only

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
	Click to refresh the list of CITs.
	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.** Click to open the Change Timeframe dialog box: Enter the date or click the arrow to choose a date and time from the calendar, for the **From** and **To** dates (or click **Now** to enter the current date and time). Click **Last Day** to enter the current date and time in the **To** box and yesterday's date and time in the **From** box. Click **OK** to save the changes. • **By Probe.** To view statistics for a specific Probe, select to open the Choose Probe dialog box. **Available for:** Population jobs only
<Statistics table>	• **CIT.** The name of the discovered CIT. Displayed for population jobs only. • **Query Name.** (Data push jobs only) The name of the query whose data is being pushed. • **Created.** The number of CIs created in the period selected or for the selected Probe. • **Updated.** The number of CIs that were updated in the period selected. • **Deleted.** The number of CIs deleted in the period selected or for the selected Probe. • **Failed.** (Data push only) The number of CIs that were not pushed. **Available for:** Service Manager 9.3 adapter only **Note:** For most adapters, when you repush the same CIs to a remote machine, the CIs are reported as **Created** in the Statistics table. For the Cmdb10xAdapter, AMPushAdapter and genericPushAdapter, the CIs are reported as **Updated** (actual status).
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
	**Refresh.** Refreshes the list of queries.
	**Push Failed Data.** Enables you to repush the selected query/CI manually. **Available:** When a failed query or CI is selected
	**Suppress selected failures/warnings.** Enables you to suppress errors for a selected query/CI. **Available:** When a failed query or CI is selected **Note:** The Suppress feature removes the failed CI from the list of errors. The error is displayed again if the CI fails at the next synchronization attempt.
<Query details>	Displays the details of the selected job's queries: • **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. If a query passed with failures, you can double-click the query to view the errors that occurred and on which CIs they occurred. To repush the query, click the **Push Failed Data**  button. To suppress all the errors for the query, click the **Suppress selected failures/warnings**  button. • **Start Time/Finish Time** The time at which data push for this query started and finished. **Available for:** Data push jobs only
<Errors and warnings>	When you double-click a job that did not complete successfully, the table displays errors and warnings that occurred, the CI type affected, and the number of CIs that failed. Double-click a row to see the CIs that failed due to a particular error. To repush the CIs, click the **Push Failed Data**  button. To suppress all the errors for the selected CI type, click the **Suppress selected failures/warnings**  button. **Available for:** Data push jobs only

UI Element (A–Z)	Description
<Failed CIs>	When you double-click an error or warning, the table displays the exact errors that occurred, the CIs on which they occurred, and when they occurred. To repush the CI, click the **Push Failed Data** button. To suppress all the errors for the selected CI, click the **Suppress selected failures/warnings** button. **Available for:** Data push jobs only

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
	Click to refresh 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 warnings (if the job succeeded with warnings) or the cause for failure if the job failed. • **Severity**. For details, see "Error Severity Levels" in the *HP Universal CMDB 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 CMDB, in which case the CMDB 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 137.

To access	Located in the left pane of the Integration Studio.

Relevant tasks	• "How to Set Up an Integration Point" on page 186 • "How to Save an Integration Point Configuration as an Adapter Default" on page 188 • "How to Deploy a Package to a Remote Data Repository" on page 192
See also	• "Data Push Tab" on page 195 • "Federation Tab" on page 196 • "Population Tab" on page 213

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 210.
	**Edit Integration Point.** Enables you to edit an integration point's properties.
	**Delete Integration Point.** Deletes the selected integration point.
	**Save Integration Point.** Saves the changes you made to the definition of an integration point.
	**Refresh All Integrations.** Refreshes the list of integration points and fully refreshes the selected integration point.
	**Reload supported configuration for adapter.** Refreshes the supported classes and queries of the adapter for the selected integration point.
	**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.

UI Element (A-Z)	Description
<List of integration points>	Displays the list of previously defined integration points. An icon appears next to each integration point indicating its status: •  . Indicates that the integration is deactivated. •  . Indicates that there is an error for one or more of the jobs associated with the integration point. •  . Indicates that there were failures and/or warnings for one or more of the jobs associated with the integration point. •  . Indicates that there were no errors, failures, or warnings for the jobs associated with the integration point or that no job was executed for the integration.

UI Element (A-Z)	Description
<right-click integration point menu>	In addition to some of 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. • **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 502. • **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 192. **Note:** This button is enabled for integration points based on the UCMDB 9.x adapter (which supports package deployment capabilities). •  **Save as Adapter Default.** Opens the Save as Adapter Default dialog box, enabling you to save the configuration of the selected integration point as an adapter default that can be used as a basis for other integration points. Enter a name and description for the adapter default, and specify the path where the default adapter should be saved. For example, to save an adapter default in a user-defined folder, in the **Path** box, enter: **MyAdapters/Default** **Note:** ▪ Use forward slashes (/) to separate folders in the path ▪ If a path is not defined, the default adapter template is saved, by default, under the same category as the adapter that it was based on. • **Edit Integration Resources.** Opens the Adapter Management page where you can edit the adapter resources. Only the resources defined by the adapter as related to integrations are displayed in the **Resources** pane.

Integration Studio Page

This page enables you to create and manage integration points.

To access	Select **Data Flow Management > Integration Studio.**

User interface elements are described below:

UI Element (A-Z)	Description
Integration Point pane	Enables you to create integration points and edit their configuration. For details, see "Integration Point Pane" on page 203.
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 195 • "Federation Tab" on page 196 • "Population Tab" on page 213

New Integration Job/Edit Integration Job Dialog Box

This dialog box enables you to create or edit population and data push jobs and to schedule them to be run at specific times.

To access	Click  on the **Population** or **Data Push** tabs.
Relevant tasks	• "How to Work with Federated Data" on page 183 • "How to Work with Population Jobs" on page 183 • "How to Work with Data Push Jobs" on page 184
See also	"Integration Jobs Pane" on page 197

User interface elements are described below:

UI Element (A-Z)	Description
Name	Enter a name for the job. **Note:** Naming conventions for jobs: • Job names can contain the following characters: `a-z`, `A-Z`, `0-9`, hyphen (-), underscore (_), space ( ) • Job names must not start with a digit • Job names must be limited to a length of 50 characters
Job Definition area	Enables you select integration queries for the job definition. For details, see "Job Definition" on next page. **Available for:** Non-Jython adapters only.

UI Element (A-Z)	Description
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" on next page.

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.
	**Move Query Up/Down.** Enables you to determine the order in which the queries should run.
	**Edit Query Resources.** Opens the Adapter Management page where you can edit the adapter resources. Only the resources defined by the adapter as related to the selected query are displayed in the **Resources** pane.
<Query table>	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.
Allow Integration Job to delete removed data	Enables the deletion of CIs or relationships per job from the local CMDB. **Available for:** Non-Jython-based Population jobs only. For details about defining CITs to be deleted by a Java-based population adapter, see "How to Define CITs to be Deleted by Java-Based Population Adapters" on page 130
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 *HP Universal CMDB 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**.
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 *HP Universal CMDB Modeling Guide*.

UI Element (A-Z)	Description
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.
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 192
See also	**For Multi-tenancy users:** "Integration in a Multi-Tenancy Environment" on page 182

User interface elements are described below

UI Element (A-Z)	Description
Test connection	Enables you to verify Probe connectivity using the parameters provided. **Note:** If you have defined additional Probes, these Probes are tested for connectivity as well.
Additional Probes	Enables you to select additional probes over which to run a data push or federation-type integration. Click ... to select the additional probes. When the integration runs, if additional Data Flow Probes are defined, the server uses the most available Probe. **Available for:** Data push and federation-type integrations only.
Adapter	The adapter for the integration point. Click ... to select an adapter. For details about each adapter, see "Out-of-the-Box Integration Adapters" on page 214. 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 a UCMDB for which authorized state has been defined.
Credentials ID	Enables you to select protocol credentials for relevant adapter integration points. Click ... to open the **Choose Credentials** dialog box. **Note**: Only the required protocols for the selected integration adapter are displayed here. For information about protocols required for each integration adapter see "Required Discovery Protocols Pane" on page 142.

UI Element (A-Z)	Description
Default Owner Name	The name of the owner tenant that should be assigned to the federated or populated CIs and relationships. **Note:** • This field is displayed when creating a federation or population type integration point in a multi-tenancy environment only. • If no owner tenant is specified, but the Data Flow Probe selected for the integration point has an owner tenant, then the Data Flow Probe owner tenant is assigned to all discovered CIs. • The System Owner Tenant is assigned when: ▪ no owner tenant is specified, and no owner tenant is defined on the Data Flow Probe ▪ the data source is not a multi-tenancy environment
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. Clear the check box to deactivate an integration, for example, to set up an integration point without actually connecting to a remote machine. **Note:** New integration points are set as inactive by default.
Probe Name	The name of the Data Flow Probe used to run integration jobs. Do one of the following: • Use the **Auto-Select** option. In this case, the CMDB attempts to choose the correct Probe according to the IP ranges that were defined for the available Probes. • Select the name of a specific Probe to use for these integration jobs. When you manually select a Probe, any ranges that you defined in the Probe settings are ignored. **Note:** If your remote managed data repositories are accessible from the UCMDB server machine, you can use the **UCMDB Integration Service** option to run non-Jython-based integrations, instead of a Data Flow Probe. If **UCMDB Integration Service** does not appear in the **Probe Name** list, ensure that the UCMDB Integration Service is running on the UCMDB Server machine. For details, see "How to Check the HP Universal CMDB Integration Service Status" on page 194. **Note:** A Probe installed on a Linux machine is defined as an Integration Probe and appears in this list.

UI Element (A-Z)	Description
Trigger CI Instance	Displays the CI that is to be used by the new integration point as a trigger during integration with CIs on a remote machine. • **Select Existing CI**. Enables you to select the trigger CI through which data is collected during integration. For details, see "CI Instances Dialog Box" in the *HP Universal CMDB 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 216. To manage or view the trigger CI, right-click the CI. For details on these operations, see "IT Universe Manager Page" in the *HP Universal CMDB 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 *HP Universal CMDB Developer Reference Guide* for details about specific adapters.

Population Tab

This tab enables you to:

- Schedule jobs that populate the CMDB with data from external data repositories. For details, see "Scheduler Definition" on page 209.
- View results for jobs that have run. For details, see "Statistics Tab" on page 200.

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 207

Select Adapter Dialog Box

This dialog box enables you to select from a list of predefined adapters that are provided out of the box.

You also have the option of adding a custom adapter for a new external data repository. For details, see "Add an Adapter for a New External Data Source" in the *HP Universal CMDB Developer Reference Guide*.

The Integration Framework SDK enables you to create new adapters that connect HP Universal CMDB with external products and services. For details, see "Developing Java Adapters" in the *HP Universal CMDB 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 183 • "How to Work with Population Jobs" on page 183 • "How to Work with Data Push Jobs" on page 184
See also	"New Integration Job/Edit Integration Job Dialog Box" on page 207

User interface elements are described below:

UI Element (A-Z)	Description
	Click to collapse the hierarchical tree structure.
	Click to expand the hierarchical tree structure.
	Click to display help about the selected adapter.
<list of adapters>	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 *HP Universal CMDB Discovery and Integration Content Guide*, or by clicking the **Show Content Help**  button for each adapter.

Adapter Name (A-Z)	Description
HP Product Adapters	
AM population and federation	Used to populate and federate data from Asset Manager.
Asset Manager Push Adapter	Used to push data from UCMDB to Asset Manager.

Adapter Name (A-Z)	Description
BSM 9.x	Used to perform a population sync from BSM to UCMDB.
CM KPI Adapter	Used to federate KPI data from Configuration Manager.
CM New Policy Adapter	Used to federate policy data from Configuration Manager.
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 to 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 and push data to HP Service Manager versions 7.1x-9.2x.
ServiceManagerAdapter 9.x	Used to federate data from and push data to HP Service Manager version 9.3 and later.
Storage Essentials	Used to populate CIs and relationships from Storage Essentials.
Systems Insight Manager	Used to populate CIs and relationships from HP SIM.
UCMDB 9.x	Used for populating and federating data from UCMDB version 9.x. For details, see "Multiple Deployments with Version 9.x/10.x CMDBs Using Population" on page 223.
UCMDB 10.x	Used for population and federating data from UCMDB version 10.x. For details, see "Multiple Deployments with Version 9.x/10.x CMDBs Using Population" on page 223.
UCMDB to XML	Used to export the results (CIs and relationships) of TQL queries and convert these to XML files.
Third Party Product Adapters	
Atrium to UCMDB	Used to populate CIs and relationships from Atrium.
CiscoWorks Layer 2	Used to populate server data from CiscoWorks.
CiscoWorks NetDevices	Used to populate network device data from CiscoWorks.
CA CMDB	Used to push CIs and relationships to CA CMDB.
Data Push into Atrium	Used to push CIs and relationships to BMC Atrium.

Adapter Name (A-Z)	Description
EMC Control Center	Used to populate CIs and relationships from EMC Control Center.
Import topology (CSV, Database, Excel, Properties File)	Used to import topology from a specified file type.
Microsoft SMS	Used to populate and federate data from Microsoft SMS.
Service-Now Integration	Used to push CIs and relationships to ServiceNow.
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 to Troux.
Other	
UCMDB API Population	Used to define an integration that specifies the reconciliation priority for data that is added to the CMDB using the CMDB API. For details, see the *HP Universal CMDB 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 (that is, 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 137.
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 210
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 "Report Toolbar Options" in the *HP Universal CMDB 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 "Data Flow Probe Setup Window - Details Pane" on page 69. • 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 78. For details on the protocols, see the *HP Universal CMDB Discovery and Integration Content Guide*.
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 483. • If DFM cannot create the topology, an error message is displayed. Click the link to review the error details in the **ui-server.log** file, located in the following folder: **C:\hp\UCMDB\UCMDBServer\runtime\log**. Then, click **Back** to fix the error and run the wizard again.
Wizard Map	The Topology CI Creation wizard contains: "Topology Preview" > "Define CI: <CI name>" > "Define Credentials" > "Topology Creation" > **"Summary"**

Limitations

This section describes certain limitations on the Integration Studio functionality.

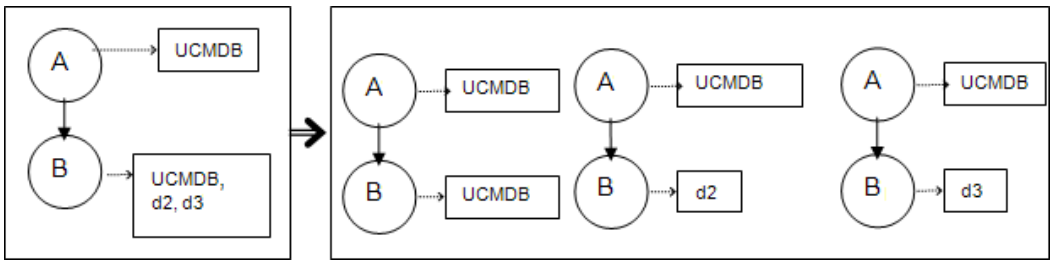
This section includes the following topics:

Limitations on Population Integrations

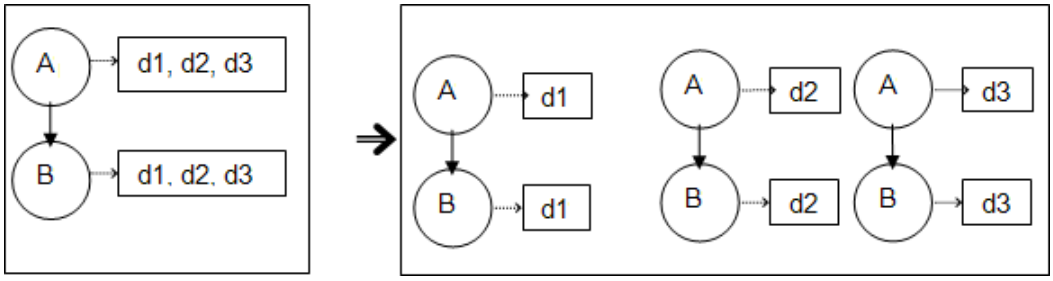
1. When configuring a population job between two CMDBs, verify that the synchronized CITs are the same in the two CMDBs.
2. When modifying a TQL query that is used in a population job, it is recommended to run a differential synchronization before modifying the TQL and a full synchronization after modifying the TQL. The differential synchronization removes any data that is no longer necessary as a result of the updated query, and the full synchronization creates new baseline data on the target system.
3. After a job runs successfully, its status remains **Succeeded** even after the job definition is changed (for example, selecting another TQL query or enabling deletion) and saved.

Limitations on Federation Integrations

1. When a virtual link exists between two data repositories, HP Universal CMDB supports mapping in the following cases only:
   - The UCMDB 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 (UCMDB) and B's data repositories (UCMDB, 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.



2. When changes are made in the Modeling Studio and these changes affect the results of a TQL query, federated CIs in the view are not updated. This is because federated TQL queries are calculated ad-hoc only and are not updated when a view is recalculated. To update the federated CIs, select the view in the CI Selector and click the **Refresh CIs Tree** button. (Note that the recalculation may take a long time.) For details, see "Browse Views Mode" in the *HP Universal CMDB Modeling Guide*.
3. You cannot edit the values of attributes that are configured to be retrieved from both an external data repository and UCMDB during federation.

Limitations on Data Push Integrations

1. After modifying a TQL query that is used in a data push job, it is recommended to run a differential synchronization before modifying the TQL and a full synchronization after modifying the TQL. The differential synchronization removes any data that is no longer necessary as a result of the updated query, and the full synchronization creates new baseline data on the target system.
2. The Universal CMDB cannot push static attributes.

Chapter 8

Integrating Multiple CMDBs

This chapter includes:

Integrating Multiple CMDBs Overview

Multiple CMDBs is a solution that allows setting up a multiple number of CMDBs for delegating the workload and responsibility of the solution to the different CMDBs.

Note: Synchronization between multiple CMDBs of different versions can be performed only between UCMDB versions 9.02 or later.

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 229.

Use Cases – Multiple CMDB Deployments: Discovery-CMS Solution

The Discovery-CMS solution enables the division of the workload and Discovery capacity over more than one CMDB.

- Discovery 1 CMDB
- Discovery 2 CMDB
- The central CMDB acting as the CMS

Both Discovery CMDBs are responsible for running different discovery jobs in the domain, and containing all the discovered topology. The CMS populates the node, interface, and IP from both Discovery CMDBs, and federates the node resource CIs (CPU, file system, and printer) from Discovery 1 CMDB. The CMS federates the node resource CIs (OS user, process, and printer) from Discovery 2 CMDB. When a user runs a view that requests these resources on the CMS, they are brought seamlessly using federation.

Multiple Deployments with Version 9.x/10.x CMDBs Using Population

When you use the UCMDB 9.x or UCMDB 10.x adapter to create an integration point, you are able to synchronize data between different CMDB instances using either population or data push. For details on the data push method, see "Multiple Deployments with Version 9.x/10.x CMDBs Using Data Push" on page 227.

This section includes:

Population from UCMDB 9.x/10.x (CMS Synchronization)

During population, global IDs are synchronized. For details, see "Global ID Synchronization" below below.

For details on population, see "How to Work with Population Jobs" on page 183.

Query Support

In the population flow, the job queries are retrieved from the remote UCMDB.

Two types of queries are supported for population jobs:

- Live queries–all non-federated TQL queries, when they are used for population with the UCMDB 9.x/10.x adapter.

  Live queries require less bandwidth, and cause less load on the source system. There may be a short delay from the time the change is made until the live query mechanism or the population job receives the change (this may take up to several minutes).

  Subgraphs and compound relationships are supported in queries. When using compound relationships, you must select **Show full path between source and target CIs** in the Compound Relationship properties of the query.

- Federated queries–queries that contain at least one federated node or attribute.

  When the UCMDB 9.x/10.x adapter is used, federated queries may also be used for population.

  Federated queries are calculated each time the integration is performed; the entire result set is retrieved and filtered by the Probe.

  The deletion of CIs is not supported. The aging mechanism must be used, since no information about the deletion of CIs or links is populated. For details, see "CI Lifecycle and the Aging Mechanism" in the *HP Universal CMDB Administration Guide*.

  You can create TQL queries for integration. For details, see "Topology Query Language" in the *HP Universal CMDB Modeling Guide*.

Global ID Synchronization

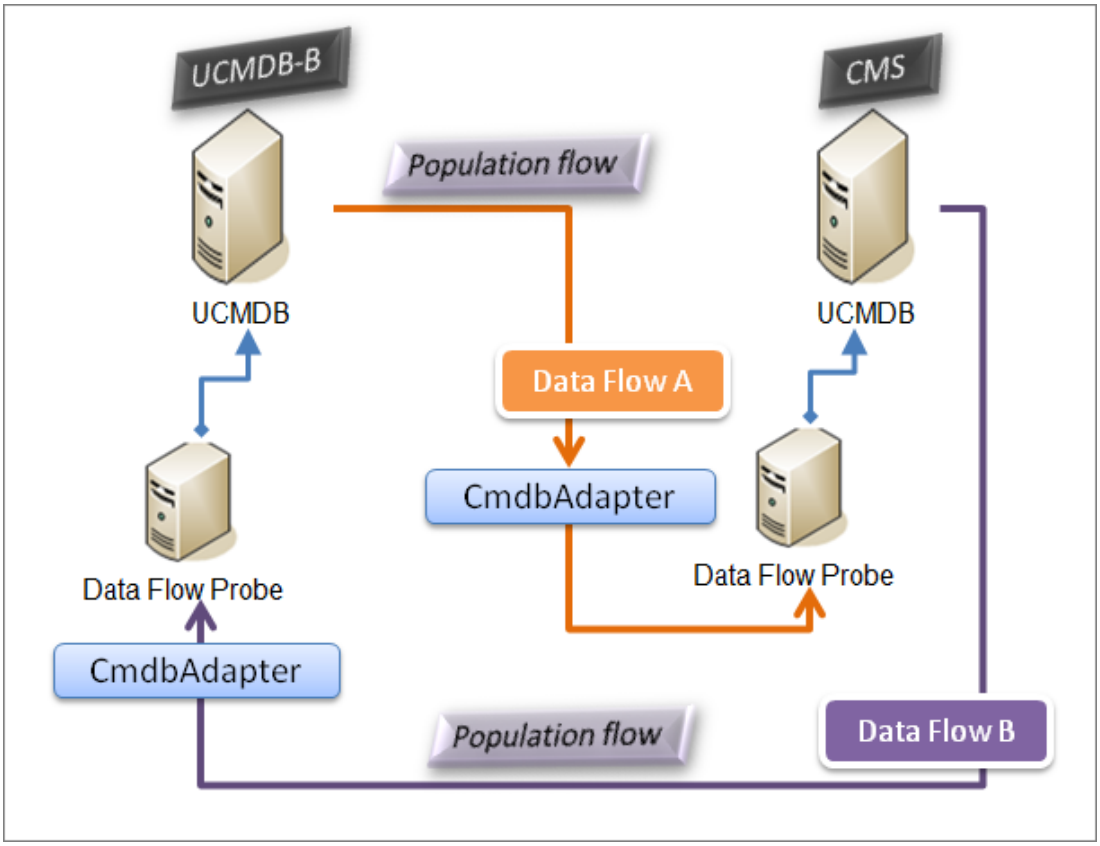
The following examples describe two types of synchronization that can be performed:

- Two-way ID synchronization

  Synchronization of data occurs in both directions between two UCMDB instances.

  The CMS uses the population flow to retrieve data from UCMDB-B, which may be any UCMDB. UCMDB-B uses the population flow to populate data from the CMS.

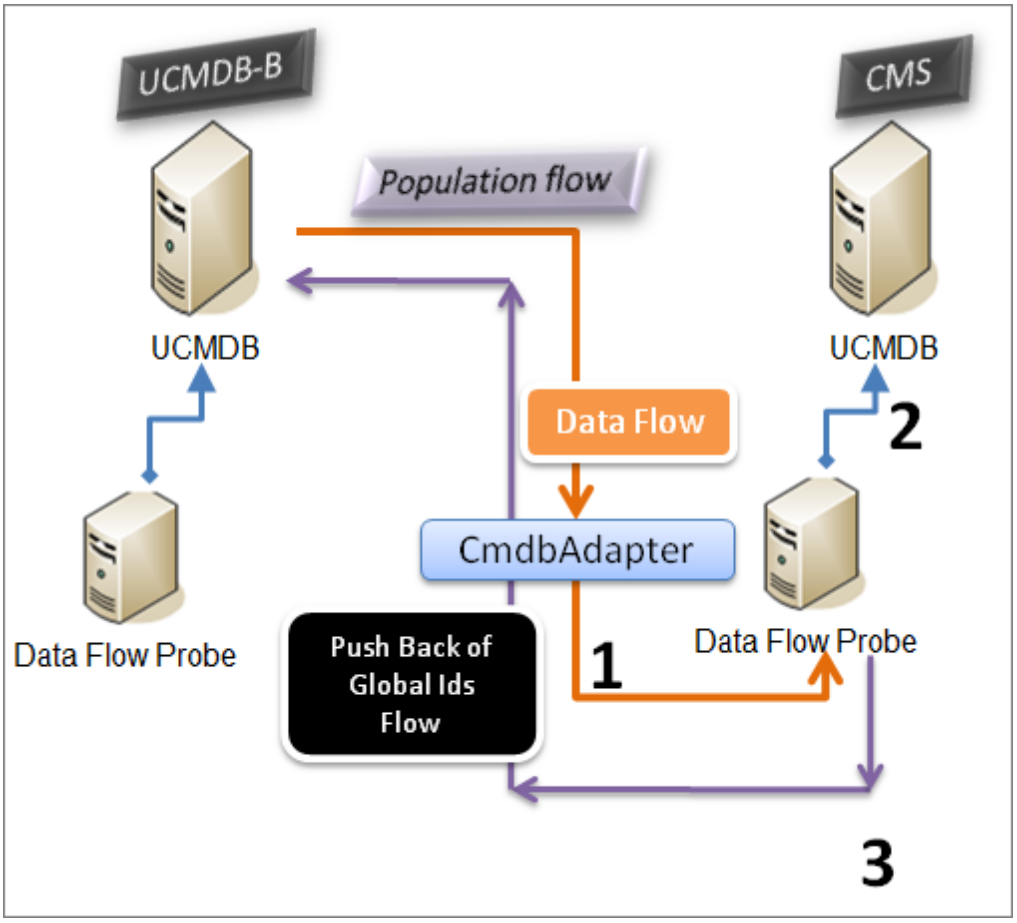
  Because synchronization is performed in two directions, global IDs are also updated on UCMDB-B.



- Pushback of IDs

  The CMS uses the population flow to retrieve data from UCMDB-B. CIs are reconciled with the data in the CMS.

  The global-ID in the CMS for each CI received is pushed back to UCMDB-B.



The default state of this option is disabled.

For details about enabling the pushback of IDs, see "How to Set Up Integrations Between Multiple CMDBs " on page 230.

Automatic Completion of Reconciliation Data

The UCMDB 9.x/10.x adapter automatically retrieves data needed for the reconciliation process of the CIs brought by the population flow. The actual data retrieved is determined by the reconciliation rule defined for the CITs of the TQL query.

For example, if your population TQL query includes a node but does not have any layout selected, the actual data that enters the CMDB is:

- Nodes, with layout
  - name
  - bios_uuid
  - serial_number
  - additional data, according to the defined reconciliation rule
- IP Addresses, with layout

  - name
  - routing_domain
- Interfaces, with layout
  - mac_address
  - interface_name

Note:

- The automatic completion feature may actually synchronize many more CIs or links than you intend.
- The automatic completion feature always retrieves the Global ID.
- By default, if data required for the reconciliation of a particular CI cannot be retrieved (for example, if the data is missing in the source), that CI is ignored without causing the entire job to fail. You can change this behavior in the CmdbAdapter configuration. For details, see "Adapter Configuration Tab" on page 144.

Multiple Deployments with Version 9.x/10.x CMDBs Using Data Push

When you use the UCMDB 9.x or UCMDB 10.x adapter to create an integration point, you are able to synchronize data between different CMDB instances using either population or data push. For details on the population method, see "Multiple Deployments with Version 9.x/10.x CMDBs Using Population" on page 223.

For details on the data push flow for setting up an integration between multiple CMDBs, see "How to Set Up Integrations Between Multiple CMDBs " on page 230.

Limitations

The following limitations apply to the data push method:

- An integration point for data push can only be defined in UCMDB version 10.01.
- The target CMDB must be either UCMDB version 9.05 CUP 9 and later CUPs, or UCMDB version 10.01 (it is not supported for UCMDB version 10.00).
- A single TQL query in the data push flow is limited to 5 million CIs and relationships. This limitation is only for a single query; multiple TQL queries in multiple jobs may exceed this limit.
- Data push is not supported for federated TQL queries.
- Data Push is not supported for virtual links.

In the data push flow, a local TQL query collects data from the local CMDB and pushes this data to the remote CMDB. The adapter filters out any unsupported CITs, relationships, valid-links, or attributes.

Auto Complete Reconciliation

When pushing CIs or relationships to a remote CMDB, any CI or attribute that is needed for reconciliation (according to the remote CMDB reconciliation rules) is automatically added to the CIs

and attributes already requested.

Note: This may cause more data than originally selected in the TQL query to be transferred.

Federation in Version 9.x/10.x CMDBs

Federation allows the CMDB to retrieve data in real time (on-the-fly) from any remote data repository, and combine it with 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 183.

Using the UCMDB 9.x/10.x adapter to federate data from different CMDBs, enables the federation of any CIT in the model. This means that only a small portion of data from the remote CMDBs can be populated, and the rest of the data is federated on demand. This ability enables the delegation of the information to multiple CMDBs, with the CMS always showing the most updated data available and at the same time not overloading its capacity.

A CMS populates the Node, Interface, and IP from a Discovery CMDB (a CMDB whose role is to run Discovery), and defines the CPU, File System, OS, User, Printer, and Process CIs as federated from the same source. When a user runs a TQL query or view that has any federated 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.x/10.x adapter supports the delegation of the federation capabilities, providing the ability to set up a single point for data retrieval (usually the CMS). Any CMDB or service that uses the CMDB's ability to delegate federation uses the CMDB as a virtual black box, and is unaware of whether data comes directly from the CMS or from an external integration.

Note: When you set up a federation flow, be careful not to cause an endless loop. For example, do not set up CMDB-X to federate data from CMDB-Y, and at the same time CMDB-Y to federate data from CMDB-X.

How to Perform Initial Synchronization

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

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

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

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

5. Click **Invoke**.

How to Configure Global ID Generation

1. Launch the Web browser and enter the following address: **http://<CMS server>:8080/jmx-console**.
2. Click **UCMDB:service=Multiple CMDB Instances Services** to open the JMX MBEAN View page.
3. Click one of the following methods and enter values as required:
   - **setAsGlobalIdGenerator** - specifies that the CMDB will act as the global ID generator for all locally existing scopes.
   - **setAsGlobalIdGeneratorForScopes** - specifies the scopes for which global IDs will be generated.
   - **setAsNonGlobalIdGenerator** - stops the CMDB from acting as the global ID generator for all scopes.
4. Click **Invoke**.

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

How to Use SSL with the UCMDB 9.x/10.x Adapter

If the remote UCMDB server uses a certificate signed by a known certificate authority, selecting the HTTPS (SSL) value in the **Protocol** field is sufficient.

If not, add the remote UCMDB server certificate to the local UCMDB JVM Trusted Stores as follows:

1. Export the remote UCMDB self-signed certificate by executing the following command (on the remote server machine):

   ```
   c:\hp\UCMDB\UCMDBServer\bin\jre\bin\keytool.exe -exportcert -
   keystore c:\hp\UCMDB\UCMDBServer\conf\security\server.keystore -
   alias hpcert -storepass 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 Multiple CMDBs

The following steps describe how to create integration points and jobs to integrate between multiple CMDBs

- "Define an integration point" below
- "Define and run a population job" on page 232
- "Define and run a Data Push job" on page 233
- "Select CI types and attributes to be federated" on page 233

1. ### Define an integration point

   a. Navigate to **Data Flow Management > Integration Studio**.

   b. Click the **New Integration Point** button to open the New Integration Point Dialog Box. For details, see "New Integration Point/Edit Integration Point Dialog Box" on page 210.

   Enter the following information:

Name (A-Z)	Recommended Value	Description
Adapter	UCMDB 9.x or UCMDB 10.x	The adapter that is used to integrate between multiple CMDBs.
Additional Probe Name	<user defined>	Additional probes over which to run a federation-type integration. Click ... to select the additional probes. When the integration runs, if additional Data Flow Probes are defined, the server uses the most available Probe.
Credentials	Remote UCMDB	If you must create a new credential protocol, use the Generic Protocol as a basis. For details, see *HP Universal CMDB Discovery and Integration Content Guide*.
Customer Name	<user defined>	The name of the remote UCMDB from which you want to retrieve data.
Default Owner Name	<user defined>	The name of the owner tenant that should be assigned to the federated or populated CIs and relationships. **Note:** ○ This field is displayed when creating a federation or population type integration point in a multi-tenancy environment only. ○ If no owner tenant is specified, but the Data Flow Probe selected for the integration point has an owner tenant, then the Data Flow Probe owner tenant is assigned to all discovered CIs. ○ The System Owner Tenant is assigned when: ○ no owner tenant is specified, and no owner tenant is defined on the Data Flow Probe ○ the data source is not a multi-tenancy environment
Hostname/IP	<user defined>	The name or IP address of the remote CMDB machine.
Integration Description	<user defined>	Free text that describes the integration point.
Integration Name	<user defined>	The name you give to the integration point.

Name (A-Z)	Recommended Value	Description
Is Integration Activated	selected	Select this check box to create an active integration point.
Port	8080	The port listened to by the HP UCMDB API.
Probe Name	<user defined>	The name of the probe on which the population jobs are run. If this field is left empty, UCMDB uses IP ranges to attempt to select the correct Probe.
Protocol	HTTP	Selects the protocol to be used for connecting to the remote CMDB. Valid values are: ○ HTTP ○ HTTPS (SSL)
Push Back Ids	<user defined>	Specifies whether to push back the global IDs after CIs are populated into UCMDB.
Remote Machine State	<user defined>	The state with which you want to connect when integrating with multi-state CMDBs. ○ Actual ○ Authorized ○ Leave this field empty for a single-state UCMDB (default).
Web application Root Context	<user defined>	The root context value of the remote CMDB. If no root context is defined on the remote CMDB, leave this field empty.

c. Click **Save**  .

d. Click **Test Connection** to ensure that the integration point has been successfully created, and then click **OK**.

You can use your integration point with any of the methods described below, population jobs, data push jobs, or federation.

2. ## Define and run a population job

An out-of-the-box integration point already contains population jobs. This step is relevant only when creating additional population jobs.

Select the **Population** tab to define a population job that uses the integration point you defined above. For details, see "New Integration Job/Edit Integration Job Dialog Box" on page 207.

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.
- **For Multi-tenancy users:** When running population with the Cmdb10xAdapter in a multi-tenancy environment, the tenants are automatically synchronized. To receive changes about the tenants (owner and user), **Owner Tenant** and **Consumer Tenants** must be defined in the TQL query layout.

Click the **Run Changes Sync** button to make sure that the integration has been successfully configured.

3. ## Define and run a Data Push job

Select the **Data Push** tab to define a data push job that uses the integration point you defined above. For details, see "New Integration Job/Edit Integration Job Dialog Box" on page 207.

Note:

- When integrating between multiple CMDBs, data push queries must be set up on the local CMDB.
- Select the **Allow Deletion** check box if you want your data push job to allow deletion of CIs and links on the remote CMDB.
- By default, infrastructure CIs and containment relationships are deleted. All other CIs and relationships are retained.
- **For Multi-tenancy users:** When running data push with the Cmdb10xAdapter in a multi-tenancy environment, the tenants are automatically synchronized. To receive changes about the tenants (owner and user), **Owner Tenant** and **Consumer Tenants** must be defined in the TQL query layout.

Click the **Run Changes Sync** button to make sure that the integration has been successfully configured.

4. ## Select CI types and attributes to be federated

a. Navigate to **Data Flow Management > Integration Studio**.

b. Click the **Federation** tab.

c. Select the CI types you want to federate from the source CMDB.

If desired, you can select only attributes to be federated. For details, see "Federation Tab" on page 196.

d. Click **Save Integration** .

Multiple CMDB Integration Troubleshooting and Limitations

Troubleshooting

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

- CMDB server logs
  - fcmdb.log
  - fcmdb.adapters.log
  - error.log
  - cmdb.reonciliation.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 CMDB with additional CIs or links, in order to contain sufficient information to insert the CIs into the CMDB.
- **Problem.** Changes are not populated immediately after a job is run.

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

  Solution. Wait a few minutes for changes to be populated by your next population job.
- **Problem.** CIs are not populated into the CMDB.

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

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

  Check the CMDB reconciliation logs for more information.
- **Problem.** Deletions are not populated.

  Solution:
  - Make sure that you have selected the **Allow Delete** check box in the population job properties.

- Check the query you are running. Deletes are not supported on federated queries, and the aging mechanism must be used.

- **Problem**. Queries that contain compound relationships fail.

  Solution. Select **Show full path between source and target CIs** in the query's Compound Relationship properties.

- **Problem.** Authentication fails.

  Solution. Since the UCMDB 9.x /10.x adapter uses the UCMDB API for connection, set up an integration user to ensure that you provide proper credentials. For details, see "Create an Integration User" in the *HP Universal CMDB Developer Reference Guide*.

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

  The Query settings have been changed manually.

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

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

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

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

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

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

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

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

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

  Check the CMDB reconciliation logs for more information.

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

  Solution:

  - Make sure that you have selected the **Allow Delete** check box in the population job properties.
  - Check the query you are running. Deletes are not supported on federated queries, and the aging mechanism must be used.

- **Problem**. Queries that contain compound relationships fail.

  Solution. Select **Show full path between source and target CIs** in the query's Compound Relationship properties.

- **Problem.** Authentication fails.

  Solution. Since the UCMDB 9.x /10.x adapter uses the UCMDB API for connection, set up an integration user to ensure that you provide proper credentials. For details, see "Create an Integration User" in the *HP Universal CMDB Developer Reference Guide*.

- **Problem.** The Data Push job fails with the message “Remote UCMDB version is not

supported."

Solution. The Data Push flow only supports pushing to UCMDB version 9.05 CUP 9 and later CUPs, or UCMDB version 10.01 (it does not support pushing to UCMDB version 10.00). Upgrade your remote UCMDB or alternatively, run the integration using the population flow.

Limitations

- If the TQL query for a population job (defined on the source) includes CI types or links that do not exist on the target, or links that are not valid, those types or links are ignored in the target data repository.
- Since the UCMDB 9.x/10.x adapter works with the "changes" population engine, if a population flow retrieves federated data, no removals are made in the CMDB, since the federation brings only added or updated data.

Universal Discovery

Chapter 9

Introduction to Universal Discovery

This chapter includes:

Universal Discovery Overview

Universal Discovery enables you to discover components that make up your system. You can discover zones in your environment by running discovery activities is those zones. Alternatively, you can set up and run individual discovery jobs on any node in your environment.

For more information, see:

- "Zone-Based Discovery" on page 242
- "Module/Job-Based Discovery" on page 274

Agent-Based vs Agentless Discovery Overview

Agent-Based Discovery

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

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

Agentless Discovery

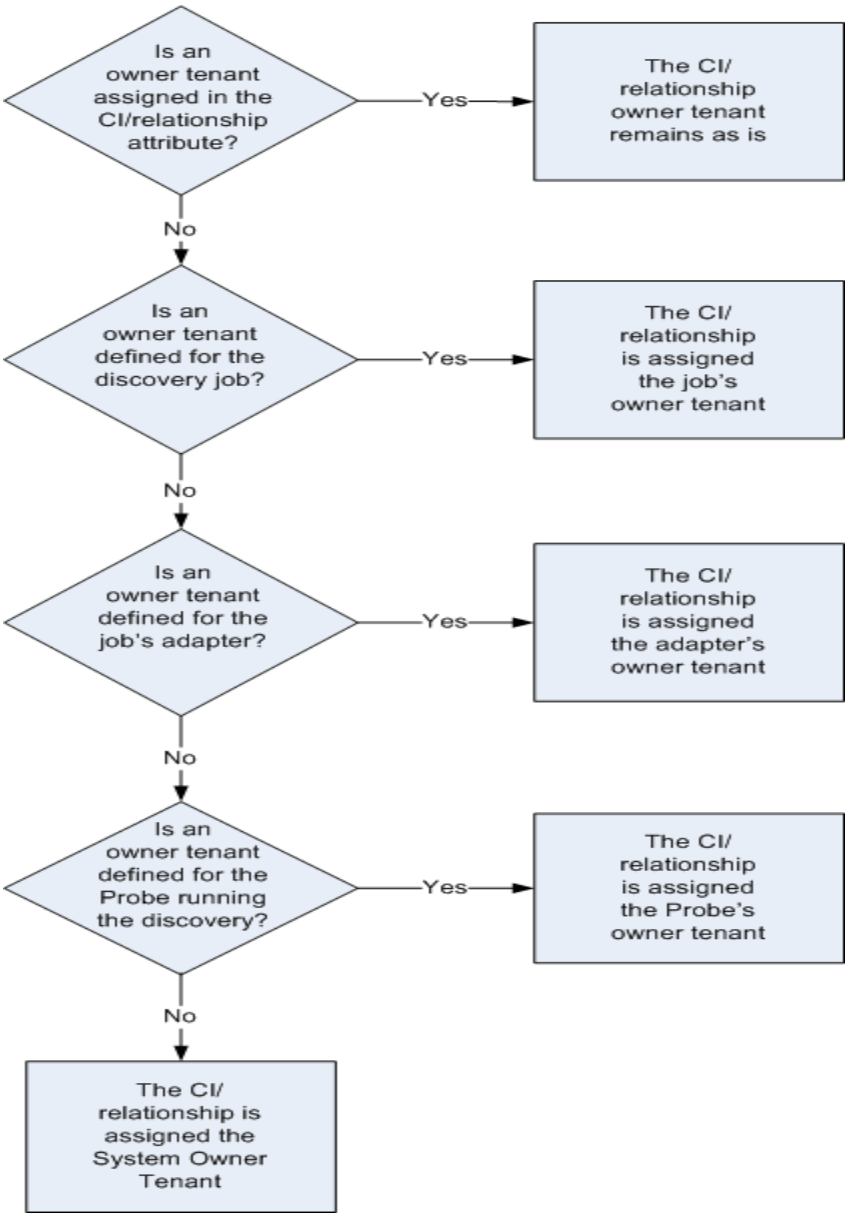
Although agentless discovery does not require the installation of dedicated agents on the servers that are to be discovered, it does depend on native OS or standard agents that are already installed such as SNMP, WMI, TELNET, SSH, NETBIOS, and others. Other discovery capabilities are based on application-specific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

supported protocols, see the *HP Universal CMDB Discovery and Integration Content Guide*.

Discovered CIs and Relationships In a Multi-Tenancy Environment

When running discoveries in a multi-tenancy environment, CIs and relationships that are not directly assigned an owner tenant when discovered, are assigned an owner tenant based on the owner tenant defined in the Data Flow Probe properties, discovery adapter parameters, or discovery job properties.

The following diagram illustrates the mechanism used for assigning owner tenant to discovered CIs/relationships:



- For details about assigning an owner tenant to a Data Flow Probe, see "How to Define Owner Tenants on Data Flow Probes" on page 33
- For details about assigning an owner tenant to an discovery adapter, see "How to Define the Owner Tenant Adapter Parameter" on page 128
- For details about assigning an owner tenant to a discovery job, see "How to Define the Owner Tenant Parameter in the Discovery Job Properties" below

How to Define the Owner Tenant Parameter in the Discovery Job Properties

If you want a discovery job to assign an owner tenant to discovered CIs and relationships other than the owner tenant defined in its adapter's parameters, you can define an override value in the job's properties.

This task describes how to define an override for the owner tenant in the job properties.

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

1. Prerequisite
   - The owner tenant that you want to define in the discovery job's properties must already be defined in UCMDB. For details on creating owner tenants in UCMDB, see New Tenant/Edit Tenant Dialog Box.
   - An owner tenant parameter must be defined in the adapter that the discovery job uses. For details, see "How to Define the Owner Tenant Adapter Parameter" on page 128.
2. In the Discovery Control Panel click the **Discovery Module/Jobs** tab
3. Select the discovery job.
4. In the **Properties** tab, in the **Overrides** area, select check box next to the **defaultOwner** parameter, and enter the name of the owner tenant that is to override the value in the adapter parameter.
5. Click **OK** to save your changes.

See also

"Discovered CIs and Relationships In a Multi-Tenancy Environment" on previous page

Discovery Control Panel

You activate jobs that discover the components of your system from the Discovery Control Panel.

To access	**Data Flow Management > Discovery Control Panel**.
Relevant tasks	• "How to Run Zone-Based Discovery" on page 246 • "How to Run Module/Job-Based Discovery" on page 275

See also	• "Zone-Based Discovery Overview" on page 242 • "Modules/Jobs-Based Discovery Overview" on page 274

User interface elements are described below:

UI Element (A–Z)	Description
Discovery Modules/Jobs tab	Enables you to activate discovery by setting up and run individual discovery jobs. For details, see "Discovery Modules/Jobs View" on page 288 **Note:** This tab is suitable for when you want to run discovery on a particular discovery node rather than within a Management Zone.
Zone-Based Discovery tab	Enables you to activate discovery in a user-friendly way by setting up Management Zones with various discovery activities. For details, see "Zone-Based Discovery View" on page 266.

Chapter 10

Zone-Based Discovery

This chapter includes:

Zone-Based Discovery Overview

Zone-based discovery enables you to:

- Limit the scope of a discovery activity to a sub-set (zone) of the entire network
- Run multiple instances of the same discovery activity on different zones in the network
- Configure each discovery activity instance with different settings (parameters, scheduling)
- Diagnose discovery problems (using the Discovery Troubleshooter)

Definitions

- **Management Zone.** A Management Zone is a region in the network defined by a collection of IP ranges. A region of an organization's infrastructure should be defined as a Management-Zone when you want to discover all the managed objects of the region using the same scheduling policy and parameters.
- **Discovery Activity.** You configure a Discovery activities to perform discovery inside a specific Management Zone. The activities discover infrastructure (IPs, nodes), basic software (shallow running software including application servers, databases, and web servers), deep database configuration, and inventory (for example, CPUs, installed software, logical volumes), among other information. A Discovery activity includes:
  - Discovery parameters that are specific to the type of the Discovery activity
  - A scheduling policy

  For more information on Discovery activities and instructions on how to activate them, see the *HP Universal CMDB Discovery and Integration Content Guide*.

Example: How to Define Management Zones

Organization-X has two data-centers: DC-A and DC-B. Each data center is owned/managed by a different administration group: Admin-Group-A and Admin-Group-B. Each administration group would like to run its own “instance” of a Discovery activity within its data center. On DC-A, you want to discover all machines operating on Windows once every week using the same discovery parameters. Therefore, DC-A should be defined as a Management Zone. On DC-B, you want to discover all the J2EE servers once every day using the same discovery parameters. DC-B should also be defined as a Management Zone.

For details on the Zone-Based Discovery tab, see "Zone-Based Discovery View" on page 266.

For details on creating a Management Zone, see "New/Edit Management Zone Dialog Box" on page 262.

For details on the Discovery Troubleshooter, see "Discovery Troubleshooter" on page 245.

Management Zone Ranking

Management Zone ranking is used when a job's trigger belongs to more than one Management Zone. This could occur when Management Zone ranges overlap, or when a trigger has more than one related IP address and each of these IP addresses belongs to a different Management Zone.

In order to better handle discovery in Management Zones where, for example, overlaps occur, Management Zones can be ranked. When Management Zones are ranked, activities defined in the Management Zones with the highest rank are run in the overlapping IP ranges, while activities in the lower ranking Management Zones do not run in the overlapping IP ranges.

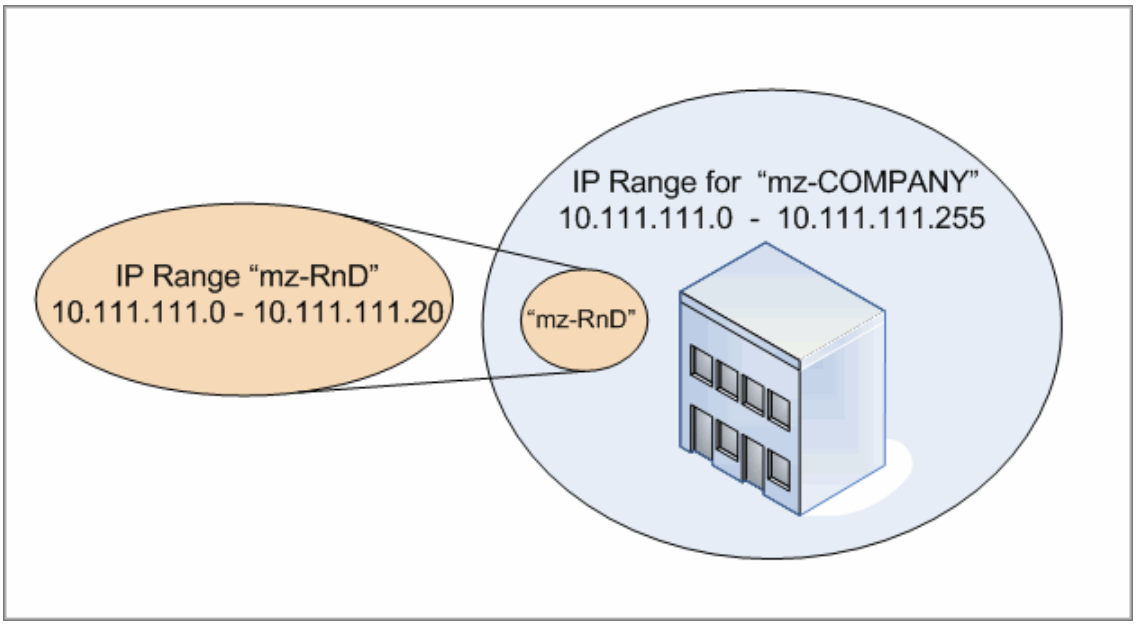
Note: Management Zones with a ranking of level 1 are the highest ranking Management Zones.

The following use-case scenarios demonstrate how ranking comes into play:

Scenario 1: Overlapping Management Zone Ranges

Say you define a large Management Zone, "mz-COMPANY," over IP range 10.111.111.0 - 10.111.111.255, covering all of the desktops in your company. You define an Inventory Discovery activity in mz-COMPANY to scan the desktops in the entire IP range for hardware and installed software.

In the R&D department of the company, discovery needs to be managed differently. Hardware discovery is of no interest to you in this range of IPs but you do want to scan the desktops in this department for installed software, as well as for software utilization. To do this, you define a smaller Management Zone, "mz-RnD", that covers the IP range of the R&D desktops only: 10.111.111.0 - 10.111.111.20. You define an Inventory Discovery activity to scan for installed software and for software utilization.



When you activate the activities in both Management Zones:

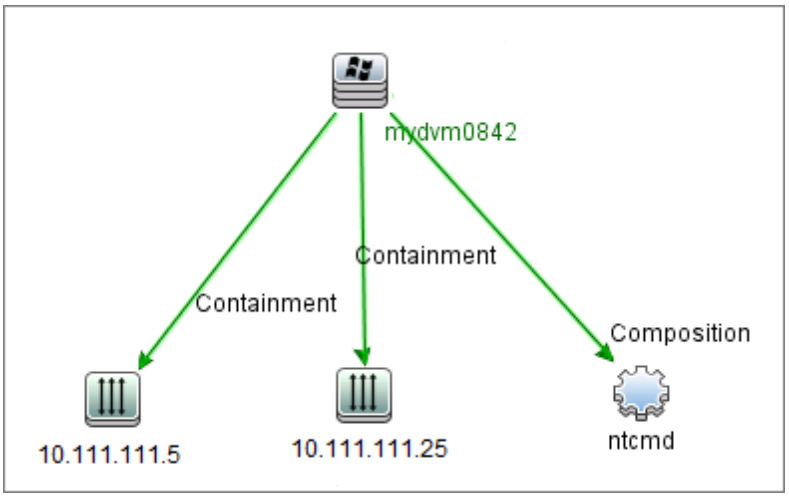
- the results for mz-COMPANY include data about hardware and installed software discovered on all desktops in mz-COMPANY's range
- the results for mz-RnD include data about installed software discovered on the desktops in mz-RnD's range, as well as information about software utilization.

Notice how both sets of discovery results include information about the installed software on the desktops in the overlapping range 10.111.111.0 - 10.111.111.20.

Because mz-RnD requires a more specialized discovery, you can assign mz-RnD a ranking of 1, and lower the ranking of mz-COMPANY to 2. This way, because mz-RnD has a higher ranking than mz-COMPANY, only the discovery activities defined for mz-RnD will run in the overlapping IP range, 10.111.111.0 - 10.111.111.20. Discovery activities defined for mz-COMPANY will run in mz-COMPANY's remaining IP range—10.111.111.21 - 10.111.111.255.

Scenario 2: Discovery Node has multiple IP Address in different Management Zones

Using the scenario above, say the desktop, Node **mydvm0842**, has multiple IP addresses, including 10.111.111.5 and 10.111.111.25. Note that both of these IP addresses belong to mz-COMPANY, but 10.111.111.5 belongs to mz-RnD as well.



Only one of these IP addresses is recorded in the Protocol CI in the Application IP attribute, which **mydvm0842** then uses for communicating with the Data Flow Probe and for determining which Management Zone **mydvm0842** will belong to.

If IP address 10.111.111.5 is selected, the activities from mz-RnD are used for discovery because mz-RnD has a higher ranking.

Note: In the case of multiple IP addresses on a node, the IP address selected for communication with the node is that which determines which Management Zone the discovery node will belong to. In the scenario above, if 10.111.111.25 is selected, even though the Management Zone it belongs to, mz-COMPANY, is lower ranking than mz-RnD, mz-COMPANY's activities will still run on the node, and may lead to unexpected discovery results. This is because the second IP address, 10.111.111.5, that was not selected for communicating with the node, is not taken into account for ranking purposes.

It is strongly recommended to define your Management Zones in such a way that if a discovery node has multiple IP addresses, all of the IP addresses are included in the same Management Zone. For details about defining Management Zones, see "New/Edit Management Zone Dialog Box" on page 262.

Discovery Troubleshooter

It is possible that after running discovery, you will not find a particular CI in the discovery results. There are various types of errors that can occur that would cause this to happen. The Discovery Troubleshooter allows you to search for the missing CI, and even if you are unable to locate the missing CI, the Discovery Troubleshooter also detects and lists errors that occurred during the discovery process. By attempting to solve these errors, this can lead you to the missing CI.

Currently the Discovery Troubleshooter allows you to locate missing Running Software CIs. When invoking the Discovery Troubleshooter, you are requested to enter the IP of the target host you are looking for and choose a detection method before searching for the missing running software CI. If the Discovery Troubleshooter does not initially succeed in connecting to the target host, it allows you to rerun discovery with a different detection method. If the Discovery Troubleshooter does succeed in connecting to the target host, it lists all the running software currently connected to the detected Node CI. If the CI you are looking for is not in the list, the Discovery Troubleshooter lets

you update available application signatures, which may provide a more extensive list of all running software connected to the detected Node CI and enable you to find the missing CI.

Note: The Discovery Troubleshooter can be run on a Management Zone only after the Infrastructure and Basic Software Configuration discovery activities have been run on that Management Zone.

See also: "Discovery Troubleshooter Wizard" on page 252

How to Run Zone-Based Discovery

This task describes a recommended workflow for running discovery in a Management Zone.

This task includes the following steps:

1. ## Prerequisites

   Verify that the Data Flow Probe is installed.

   (UNIX only) If you want to specify the locations of data or temporary folders when installing Universal Discovery Agent, see "How to Specify Data and Temp Folder Locations when Installing or Updating the Universal Discovery Agent for UNIX" on page 99.

2. ## Create a Management Zone

   a. In Data Flow Management, go to **Discovery Control Panel > Zone-Based Discovery tab**, click the **New**  button, and select **New Management Zone**.

   b. In the New Management Zone dialog box that opens:

   - Enter a name for the Management Zone. **This field is mandatory**.

     Note: Naming conventions for Management Zones:

     - The name can contain the following characters: `a-z`, `A-Z`, `0-9`, hyphen (-), underscore (_), and space ( )
     - The name is not case sensitive, for example, mz1/mZ1/Mz1 are all the same
     - The name must not start with a digit
     - The name must be limited to a length of 50 characters

   - Select a method for defining ranges for the Management Zone. You can use full Data Flow Probe ranges or define partial ranges for the Management Zone. For more information on the differences between these two options and on the user interface, see "New/Edit Management Zone Dialog Box" on page 262.

> **Note:** In order to get predictable discovery results, we recommend that when defining the ranges for your Management Zones, they are configured in such a way so that all related IP addresses for a particular discovery node belong to the same Management Zone.
>
> If IP addresses belonging to one discovery node span more than one Management Zone, and the Management Zones are ranked at different levels, unpredictable discovery results may occur. This is because the IP address that was selected to communicate with the discovery node is used to determine which Management Zone the discovery node belongs to, and that address may not always belong to the Management Zone with the highest rank.

c. (Optional) Configure settings for the Management Zone. For details, see "How to Configure Global Settings for Management Zones" on page 251.

> **Note:** These settings override the global Management Zones configuration settings.

3. Set up and activate discovery activities

   In the Management Zone:

   a. Set up and activate the **Infrastructure Discovery Activity**.

      For agent-based discovery, you must ensure that the Universal Discovery (UD) Agent is installed on the node being discovered. You can configure the Infrastructure Discovery activity to install the UD Agent automatically. For more information, see the section describing the Infrastructure Discovery activity in the *HP Universal CMDB Discovery and Integration Content Guide*.

      Alternatively, if you want to install the UD Agent manually, follow the instructions described in "How to Install Universal Discovery Agent Manually" on page 95

   b. Set up and activate other activities required for discovering the Management Zone. For more information, see the *HP Universal CMDB Discovery and Integration Content Guide*

4. Results

   - To verify the discovery ran successfully, select the Management Zone in the Management Zones tree and, in the **Discovery Status** pane, click the **Results** tab.

     For more information, see "Discovery Results Tab/Pane" on page 324.

     If you do not find a particular CI in the discovery results, you can run the Discovery Troubleshooter to search for the missing CI. For more information about running the Discovery Troubleshooter, see "Discovery Troubleshooter Wizard" on page 252

     > **Note:** The Discovery Troubleshooter can be run in a Management Zone only after the Infrastructure and Basic Software Configuration discovery activities have run in that Management Zone.

   - The following events occur as a result of installing the Universal Discovery Agent:
     - The UD Agent generates a Unique ID which is stored locally on the discovery node and in UCMDB as follows:

- **Windows and UNIX.** For more information on where Unique ID is stored, see "Universal Discovery Agent File Locations" on page 110.
- **UCMDB**. Stored in the **ud_unique_id** attribute of Node CI.

For more information on Unique ID, see "Universal Discovery Agent Overview" on page 88.

- Software Identification Tag files are created and stored on the discovery node. For more information about Software Identification Tags, see "Hardware and Software Recognition" on page 339.

How to Create a Discovery Activity Template

This task describes how to create a Discovery Activity Template; a collection of jobs which you define. Once you have created the template, users can create new custom activity types based on the template, and edited to suit individual requirements.

For more information about discovery activities see "Universal Discovery Overview" on page 238, and see the section about Universal Discovery Activities in the *HP Universal CMDB Discovery and Integration Content Guide*.

See also "How to Create a Custom Discovery Activity from a Template" below.

To Create a Discovery Activity Template

1. Go to **Data Flow Management > Discovery Control Panel > Zone-Based Discovery > Management Zones**.
2. Select any Management Zone.
3. Click the  button, or right-click any Management Zone.
4. Select **New Discovery Activity > Templates > New Discovery Activity Template**.

   The **New Discovery Activity Template** wizard starts.
5. Type a name for the template and click **Next**.

   The **Select Discovery Jobs** page appears.
6. Click the  button.

   The **Select jobs** dialog box appears.
7. Select the jobs to include in the activity.

   Note: Click the  button to display the **Find jobs** dialog box if required.
8. Click **Finish** to save the template.

How to Create a Custom Discovery Activity from a Template

This task describes how to create a custom Discovery Activity from a previously created template.

For more information about discovery activities see "Universal Discovery Overview" on page 238, and see the section about Universal Discovery Activities in the *HP Universal CMDB Discovery and Integration Content Guide*.

See also "How to Create a Discovery Activity Template" on previous page.

To Create a Custom Discovery Activity from a Template

1. Go to **Data Flow Management > Discovery Control Panel > Zone-Based Discovery > Management Zones**.
2. Select the appropriate Management Zone.
3. Click the  button.
4. Select **New Discovery Activity > Templates > <template name>**.

   The **New Discovery Activity** wizard starts.
5. Type a name for the activity and click **Next**.

   The **Select Activity Jobs** page appears.The jobs included in the template are listed under Selected Jobs.
6. Edit the activity, if required. (This step is optional.)
   a. To add a job, click the  button. The **Select jobs** dialog box appears. Select the required jobs.

      Note: Click the  button to display the **Find jobs** dialog box if required.

   b. To remove a job, select the job in the **Selected jobs** list and click the  button.
   c. To override the parameters for a job, select the job in the **Selected jobs** list. The parameters appear in the **Job Parameters** pane. Select **Override** for the parameter you want to override, and type the replacement value in the **Value** column.

      After editing the activity, click **Next**.
7. Schedule the discovery.

   Edit the entries on the **Schedule Discovery** page to match your requirements, then click **Next**.
8. Review the summary.

   Verify the entries on the **Summary** page. If required, select the **Activate activity** option.
9. Click **Finish** to save the activity. The activity appears in the Management Zone.

How to Rank Management Zones

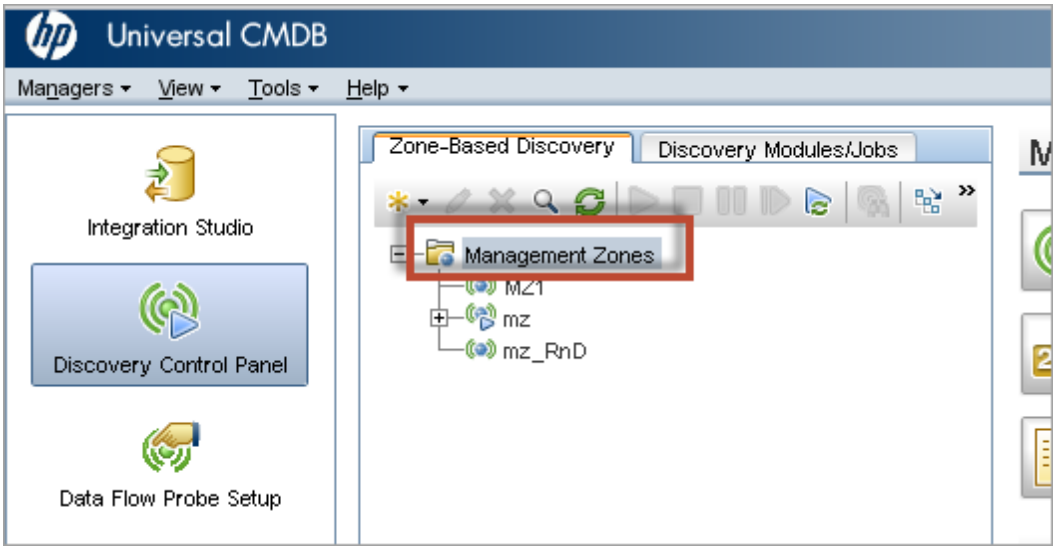
Management Zone ranking is used when a job's trigger belongs to more than one Management Zone. This could occur when Management Zone ranges overlap, or when a trigger has more than one related IP address and each of these IP addresses belongs to a different Management Zone.

Note: As noted when defining ranges for your Management Zones, if you are aware of a discovery node having multiple IP addresses, we recommended that all of these IP addresses are included in the ranges of only one Management Zone. If IP addresses belonging to one discovery node span more than one Management Zone, and the Management Zones are ranked at different levels, unpredictable discovery results may occur.

For more information and an example, see "Management Zone Ranking" on page 243.

This task describes how to assign ranks to Management Zones.

1. In the Zone-based Discovery view, in the Managements Zones tree, select the Management Zones root.



2. In the Management Zone Actions pane on the right, click **View/Edit Management Zone Ranks**  .

   The Management Zone Ranking dialog box opens:

   - The Ranks tree displays all the defined Management Zones.

     Note: By default, when Management Zones are created, they are ranked at level 1.

   - When you select a Management Zone in the tree, the right pane displays the Management Zones whose IP ranges overlap with the selected Management Zone.
   - The IP ranges of the selected Management Zone are displayed in the lower area of the right pane.

     Note: The ranges displayed in the lower area of the right pane belong to the Management Zone selected in the Ranks tree, and not to Management Zones selected in the overlapping Management Zones area.

3. To assign a different ranking to a Management Zone, select the Management Zone in the Ranks tree and click the **Rank Higher** / **Rank Lower** button.

How to Configure Global Settings for Management Zones

This task describes how to set global settings for Management Zones.

Note: This task is optional. Management Zones can be used with the default values assigned to global settings without any changes by the user.

For more information on global settings for management zones, see "Global Settings Dialog Box" on page 258.

1. In the Discovery Control Panel, click the **Zone-Based Discovery** tab.

   Ensure that the root node of the Management Zone tree is selected.

2. In the Management Zone Actions section, click **View/Edit Global Settings** .

   The Global Settings dialog box opens. This dialog box presents the following three types of global settings:

   - General Settings
   - Application Signatures
   - Ports

3. In the left pane, select **General Settings** (selected by default upon initial entry to this dialog box).

   You can configure here the following global settings:

   - Maximum Probe Connections Per Second
   - Shell Bandwidth Limit
   - Shell Default Command Timeout
   - SQL Query Timeout
   - SSH Log Level

   To change a value for a general setting:

   a. Either select in the list and click **Properties** , or double-click it in the list.

   b. In the Properties window that opens, assign a new value and click **Save**.

4. Select **Application Signatures** in the left pane (if you want to change application signatures).

   Here you can perform the following actions on application signatures:

   - Add an application signature to the list of available signatures by clicking **Add** . The Software Identification Rule Editor Dialog Box opens. Assign properties to the application

signature, as described in "Software Identification Rule Editor Dialog Box" on page 170

- Edit an application signature that appears in the list by selecting it and clicking **Edit**  , or by double-clicking on the application signature in the list. The Software Identification Rule Editor Dialog Box opens with the properties of the selected application signature. You can change properties as described in "Software Identification Rule Editor Dialog Box" on page 170
- Remove an application signature from the list of available signatures by clicking on the signature in the list and clicking **Remove**  .
- Export an application signature to an XML file by selecting the signature in the list and clicking **Export Application Signature to XML**  .
- Import an application signature from an XML file to the list of available signatures by clicking **Import Application Signature from XML**  .
- Switch a listed application signature from being 'in use' to 'not in use' (or vis versa) by checking/unchecking it in the list.

5. Select **Ports** (if you want to add, edit, or remove a port).
   - To add a new port, click **Add Port**  . Clicking this button opens the Add New Port dialog box, where you assign a name and number to the new port.
   - To change a port number, select the port in the list and click **Edit Port**  . Clicking this button opens the Edit Port dialog box, where you can change the port number.
   - To remove a port from the list, select the port in the list and click **Remove Port**  .
6. Click **OK** in the Global Settings dialog box to save all changes.

Zone-Based Discovery User Interface

This section includes:

Discovery Troubleshooter Wizard

The Discovery Troubleshooter allows you to troubleshoot for running software CIs that do not show up when you run an activity on the Management Zone. This is useful for customers who are running activities for discovering running software, and they see that the running software is not found.

This wizard page allows you to initiate the Discovery Troubleshooter.

To access	Select a Management Zone in the Management Zones tree structure on the left and click the **Troubleshooting** button.
Important information	• The Discovery Troubleshooter wizard can be activated only within the context of a Management Zone. • The Discovery Troubleshooter wizard can be run on a Management Zone only after the Infrastructure and Basic Software Configuration Discovery activities have been run on that Management Zone. • If any discovery activities are still running when you start this wizard, the **Wait for Jobs** screen appears after clicking Next in the first screen of this wizard. If the **Wait for Jobs** screen appears, wait until the activities finish and then continue with the wizard.
Relevant tasks	"How to Run Zone-Based Discovery" on page 246
Wizard map	The Discovery Troubleshooter Wizard contains: Discovery Troubleshooter Wizard > "Activity Instances Mapping Page" below > "Target Host Page" on next page > "Additional Information Is Required Page" on next page > "Investigate Missing Node CI Page" on page 255 > "Retrieve Running Software CIs Page" on page 256
See also	• "Discovery Troubleshooter" on page 245 • "Universal Discovery Overview" on page 238 • "Zone-Based Discovery View" on page 266

Activity Instances Mapping Page

This wizard page allows you to select a Discovery Activity Instance associated with the Management Zone on which you are running the Troubleshooter.

Important information	This wizard page only appears if you have more than one Infrastructure or Basic Software Configuration Discovery activity associated with the Management Zone.
Wizard map	The Discovery Troubleshooter Wizard contains: "Discovery Troubleshooter Wizard" on previous page > Activity Instances Mapping Page > "Target Host Page" on next page > "Additional Information Is Required Page" on next page > "Investigate Missing Node CI Page" on page 255 > "Retrieve Running Software CIs Page" on page 256

User interface elements are described below:

UI Element (A-Z)	Description
Activity Type	Lists the types of Discovery Activities that are prerequisites for running the Troubleshooter. Currently, only Infrastructure and Basic Software Configuration Discovery activity types are listed here.
Activity Instance	Lists the instances of the Activity Type. If there is more than one instance, they are listed in a drop-down menu.
Troubleshooter Log	This log lists all actions performed by the Troubleshooter that occur in the background and do not appear in the user interface.

Target Host Page

This wizard page allows you to enter the name or IP address of the host that you want to discover.

Important information	• The name or IP address that you enter in this page should be within the range of at least one of the probes in the Management Zone. If it is not, an error message appears. • After clicking Next on this page, the **Validate Target Host IP Address** page appears. Wait briefly while the Discovery Troubleshooter validates the target host IP address. If the target host you entered is not within the range of the Management Zone, the **Validate Target Host IP Address** page offers you an option to choose a different target host, or close the wizard. If you choose a different target host, the **Target Host** page appears again. • Once an IP address is defined, the Discovery Troubleshooter checks if a CI exists for that IP. If no CI exists, the Discovery Troubleshooter automatically creates a CI for that IP address.
Wizard map	The Discovery Troubleshooter Wizard contains: "Discovery Troubleshooter Wizard" on page 252 > "Activity Instances Mapping Page" on previous page > Target Host Page > "Additional Information Is Required Page" below > "Investigate Missing Node CI Page" on next page > "Retrieve Running Software CIs Page" on page 256

User interface elements are described below:

UI Element (A-Z)	Description
Target host:	Enter here the name or IP address of the host that you want to discover.
Troubleshooter Log	This log lists all actions performed by the Troubleshooter that occur in the background and do not appear in the user interface.

Additional Information Is Required Page

This wizard page allows you to select a method for detecting the target host.

Important information	• After clicking **Next** in this page, the Discovery Troubleshooter attempts to activate a specific job. If this job is not active, a message appears stating that the job is about to be activated and that if you activate it, this may invoke the job on all potential trigger CIs that are relevant to this job. • After clicking Next in this page, the **Discovery Progress** screen appears and informs you that Discovery is currently running.
Wizard map	The Discovery Troubleshooter Wizard contains: "Discovery Troubleshooter Wizard" on page 252 > "Activity Instances Mapping Page" on page 253 > "Target Host Page" on previous page > Additional Information Is Required Page > "Investigate Missing Node CI Page" below > "Retrieve Running Software CIs Page" on next page

User interface elements are described below:

UI Element (A-Z)	Description
Select detection method for the requested host:	Discovery uses detection methods to communicate with the remote machine. Choose from one of the following detection methods: WMI, Shell, Power Shell, SNMP.
Troubleshooter Log	This log lists all actions performed by the Troubleshooter that occur in the background and do not appear in the user interface.

Investigate Missing Node CI Page

This wizard page lists errors found if the Troubleshooter does not succeed in connecting to the host, and offers options for trying to resolve those errors.

Important information	This page only appears if the Troubleshooter does not succeed in connecting to the host.
Wizard map	The Discovery Troubleshooter Wizard contains: "Discovery Troubleshooter Wizard" on page 252 > "Activity Instances Mapping Page" on page 253 > "Target Host Page" on previous page > "Additional Information Is Required Page" on previous page > Investigate Missing Node CI Page > "Retrieve Running Software CIs Page" on next page

User interface elements are described below:

UI Element	Description
<error messages>	Various error messages can occur when running the Troubleshooter. One of the more common types of error messages is **Permission Denied**. This error occurs if there is a problem with the user credentials. You can attempt to fix this error by clicking **Fix** by the error message. If you do this, the **Update Credentials** dialog box appears, and you can update the user credentials as explained in "Data Flow Probe Setup Window - Details Pane" on page 69, "[Protocol] Pane" on page 73. After updating user credentials, you should choose **Rerun relevant discovery job to find missing CI** in this wizard page and continue with the wizard.
Rerun relevant discovery job to find missing CI	Choose this option if you see an error in the list for which rerunning a job might help (for example, a timeout error). If you choose this option, the **Discovery Progress** screen appears.
Choose a different detection method to find missing CI	If you choose this option, the wizard returns to the "Additional Information Is Required Page" on page 254.
Close the Troubleshooter and save support log	Choosing this option exits the wizard and saves the log file to a location on the server machine (the exact location is indicated on the page that follows).
Troubleshooter Log	This log lists all actions performed by the Troubleshooter that occur in the background and do not appear in the user interface.

Retrieve Running Software CIs Page

This wizard page lists all running software that is currently listed as connected to the detected Node CI.

Wizard map	The Discovery Troubleshooter Wizard contains: "Discovery Troubleshooter Wizard" on page 252 > "Activity Instances Mapping Page" on page 253 > "Target Host Page" on page 254 > "Additional Information Is Required Page" on page 254 > "Investigate Missing Node CI Page" on previous page > Retrieve Running Software CIs Page

User interface elements are described below:

UI Element	Description
Yes, the CI was discovered	Check this option if the running software CI that you are looking for is in the list, or just close the Troubleshooter since you have successfully completed troubleshooting.

UI Element	Description
No, the CI is still missing	Check this option if the running software CI that you are looking for is not in the list. If you choose this option, the **Software Identification Rules Management** screen appears, and you can continue the search for the missing CI as follows: 1. In the **Software Identification Rules Management** screen, update the available application signatures as explained in "Software Identification Rule Editor Dialog Box" on page 170. 2. The Troubleshooter then attempts again to find the missing CI (by re-running its corresponding job) and this wizard page appears with a potentially more extensive list of all running software that is connected to the detected Node CI. 3. If the running software CI that you are looking for is still not in the list, select again **No, the CI is still missing** ,and the **Additional Information Is Required** page appears (see below).
Additional Information Is Required page	If after updating the available application signatures the Troubleshooter still does not find the missing CI, this page appears. You can choose either **Update software identification rules and rerun discovery** or **Close the Troubleshooter and save support log**. If you choose **Update software identification rules and rerun discovery**, the **Software Identification Rules Management** screen appears again and you can continue to update the software identification rules.
Troubleshooter Log	This log lists all actions performed by the Troubleshooter that occur in the background and do not appear in the user interface.

Find Management Zone Dialog Box

Enables you to locate Management Zones in the tree answering to specified search criteria.

To access	**Discovery Control Panel > Zone-Based Discovery > Management Zones pane >** Click the **Find Management Zone**  button

User interface elements are described below:

UI Element	Description
	Finds the next Management Zone in the tree meeting the search criteria.

UI Element	Description
Find Management Zone by	Enables you to enter search criteria: • **Name.** Enter the name of the Management Zone, or part of the name. • **IP Address.** Enter the IP address. **Note:** When looking for an IP address for a specific routing domain, also specify the domain. If no domain is provided, all domains will be searched.
Direction	Directs the search forwards or backwards through the Management Zone tree.

Global Settings Dialog Box

This dialog box enables you to set and view global settings for all Management Zones in your system.

To access	**Data Flow Management > Discovery Control Panel > Zone-Based Discovery tab** • In the section Management Zone Actions, click **View/Edit Global Settings**  .
Important information	The Global Settings dialog box can also be accessed from the Settings tab in the "New/Edit Management Zone Dialog Box", however the title of the dialog box remains "New/Edit Management Zone" and the following limitations exist: • The settings that you configure affect only the Management Zone that you are creating/editing and not all the Management Zones in the system. • You cannot configure the global setting **Maximum Probe Connections Per Second**, as this affects the entire probe and not only the management zone. • You cannot add, edit, or remove application signatures.
Relevant tasks	"How to Configure Global Settings for Management Zones" on page 251

User interface elements are described below:

UI Elements	Description
General Settings	Choose this option to view or change the following general settings: **Maximum Probe Connections Per Second, Shell Bandwidth Limit, Shell Default Command Timeout, SQL Query Timeout,** and **SSH Log Level**. **Note:** • When accessing this option from the "New/Edit Management Zone Dialog Box", you cannot configure the **Maximum Probe Connections Per Second** setting. • For details about each of the displayed settings, see the section describing the globalsettings.xml file in the *HP Universal CMDB Discovery and Integration Content Guide*. The General Settings options contains the following UI elements: • **Categories pane.** Contains a list of the global settings categories. If you select a category, only the settings in that category appear in the settings list on the right. If you select **<All>**, all of the global settings are listed. • **Properties**  **.** Opens the Properties window, and allows you to view the properties for a selected global setting and change it's value. **Note:** You can also open the Properties window by double-clicking on a global setting in the list. • **Undo**  **.** Restores the previous value of the selected setting (only relevant if you changed the value of that setting). • **Filter by column.** Filters the list of global settings by selecting a category from the drop-down list and entering filter criteria in the text box.

UI Elements	Description
Application Signatures	Choose this option to add or remove application signatures to or from the list of available signatures, or edit an application signature in the list of available signatures. You can also switch a listed application signature from being 'in use' to 'not in use' (or vis versa) by checking/unchecking it in the list. **Note:** If you accessed the Applications Signatures option from the Configurations tab of the "New/Edit Management Zone Dialog Box", the only UI element listed below that appears is **View Application Signature Parameters**, and the only changes you can make to application signatures are to switch listed application signatures from being 'in use' to 'not in use' (or vis versa) by checking/unchecking them in the list. The Applications Signatures option contains the following UI elements: • **Add**  **.** Adds an application signature to the list of available signatures. Clicking this button opens the "Software Identification Rule Editor Dialog Box" described on page 170. • **Edit**  **.** Edits an application signature. This button is active only if an application signature is selected. Clicking this button opens the "Software Identification Rule Editor Dialog Box" (described on page 170) with details for the selected application signature. • **Export Application Signature to XML**  **.** Exports an application signature to an xml file. This button is active only if an application signature is selected. • **Import Application Signature from XML**  **.** Imports an application signature from an xml file. • **Remove**  **.** Removes an application signature from the list of available signatures. This button is active only if an application signature is selected. • **View Application Signature Parameters**  **.** Enables viewing the parameters of a selected application signature. Clicking this button opens the "Software Identification Rule Editor Dialog Box" (described on page 170) in read-only mode, with details for the selected application signature. This button appears only in the Configurations tab of the "New/Edit Management Zone Dialog Box".

UI Elements	Description
Ports	Choose this option to add, edit, or remove a port. The Ports option contains the following UI elements: • **Add Port**  . Adds a new port. Clicking this button opens the Add New Port dialog box. • **Edit Port**  . Changes the port number of an existing port. This button is only active if a port is selected. The port name cannot be changed. • **Remove Port**  . Removes a port. This button is only active if a port is selected.

Management Zone Ranking Dialog Box

This dialog box enables you to set ranking levels for your Management Zones.

To access	**Data Flow Management > Discovery Control Panel > Zone-Based Discovery tab > Management Zones root >** Click the **View/Edit Management Zone Ranking**  button.
Important information	• Changing ranks of Management Zones may cause discovery activities to rerun. • As noted when defining ranges for your Management Zones, if you are aware of a discovery node having multiple IP addresses, we recommend that all of these IP addresses are included in the ranges of only one Management Zone. If IP addresses belonging to one discovery node span more than one Management Zone, and the Management Zones are ranked at different levels, unpredictable discovery results may occur. This is because the IP address that was selected to communicate with the discovery node is used to determine which Management Zone the Node belongs to, and that address may not always belong to the Management Zone with the highest rank.
Relevant tasks	• "How to Run Zone-Based Discovery" on page 246 • "How to Rank Management Zones" on page 249
See also	"Management Zone Ranking" on page 243

User interface elements are described below:

UI Elements	Description
	**Rank Higher/Lower.** Enables you to move the selected Management Zone to a higher or lower ranking level. **Note:** Management Zones with a ranking of level 1 are the highest ranking Management Zones.
	**Reset.** Enables you to undo changes that you made to the ranks.
	**Expand/Collapse All.** Expands/Collapses the **Ranks** tree, displaying the Management Zones under each rank.
<Ranks tree>	Displays all the Management Zones under its ranking level.
<Management Zone Ranking Details pane>	When you select a Management Zone in the Ranks tree, the right pane displays the following information: • **Management Zones Overlapping with <*Management Zone*>.** Displays all of the Management Zones that contain ranges that overlap with the range of the selected Management Zone. • **Ranges of <*Management Zone*>.** Displays the ranges defined for the Management Zone selected in the Ranks tree. For more details, see "New/Edit Range Dialog Box" on page 62.

New/Edit Management Zone Dialog Box

This dialog box enables you to create or edit a Management Zone.

To access	**Data Flow Management > Discovery Control Panel > Zone-Based Discovery tab >** • **To create a Management Zone:** Click **New**  . • **To edit an existing Management Zone:** Select the Management Zone and click **Edit**  .
Important information	You must have at least one Data Flow Probe set up to create a Management Zone.
Relevant tasks	"How to Run Zone-Based Discovery" on page 246
See also	• "Universal Discovery Overview" on page 238 • "Zone-Based Discovery View" on page 266 • "Discovery Troubleshooter" on page 245

Details Tab

User interface elements are described below:

UI Elements	Description
Name	The name of the Management Zone. **This field is mandatory**. **Note:** Naming conventions for Management Zones: • The name can contain the following characters: `a-z`, `A-Z`, `0-9`, hyphen (-), underscore (_), and space ( ) • The name is not case sensitive, for example, mz1/mZ1/Mz1 are all the same • The name must not start with a digit • The name must be limited to a length of 50 characters
Description	The description of the Management Zone. This field is optional. This description appears in the Details table in the right pane after creating the Management Zone. **Note:** The length of the description is limited to 600 characters.
Ranges	Enables you select a method for defining ranges for the Management Zone. • **Use full Data Flow Probe ranges.** Displays all the Data Flow Probes in the lower pane, enabling you to select Data Flow Probes with their full defined ranges for the Management Zone. To select Data Flow Probes for the Management Zone, see "Data Flow Probe Selection Area" below. **Note:** If you bind a Data Flow Probe to the Management Zone with **Use full probe ranges**, any future changes to the Data Flow Probe range will be applied to the Management Zone. • **Define partial ranges on Data Flow Probes**. Displays the Select Ranges area in the lower pane, enabling you to define ranges for the Management Zone that are subsets of the ranges defined for the existing Data Flow Probes. For details, see "<Select Ranges Area>" below. **Default**: **Use full Data Flow Probe ranges** is selected **Note:** In order to get predictable discovery results, we recommend that when defining the IP ranges for your Management Zones, they are configured in such a way so that all related IP addresses for a particular discovery node belong to the same Management Zone. If IP addresses belonging to one discovery node span more than one Management Zone, and the Management Zones are ranked at different levels, unpredictable discovery results may occur. This is because the IP address that was selected to communicate with the discovery node is used to determine which Management Zone the discovery node belongs to, and that address may not always belong to the Management Zone with the highest rank.

UI Elements	Description
Data Flow Probe Selection Area	Displayed when **Ranges > Use full Data Flow Probe ranges** is selected. It displays the all of the Data Flow Probes available in UCMDB, and enabled you to select Data Flow Probes for the Management Zone. Discovery in the Management Zone is run over the full ranges of the selected Data Flow Probes. • **Non-selected Probes column.** Lists the Data Flow Probes in UCMDB that can be added to the Management Zone. Select a Probe and click  to move it to the Selected Probes list. Click  to move all of the Probes to the Selected Probes list. • **Selected Probes column.** Lists the Data Flow Probes that have been selected for the Management Zone. Select a Probe and click  to remove it from the Selected Probes list. Click  to remove all of the Probes from the Selected Probes list.

UI Elements	Description
<Select Ranges Area>	Displayed when **Ranges > Define partial ranges on Data Flow Probes** is selected. • **Open Data Flow Probe Setup.** Opens the **Edit Probe Configuration** dialog box, enabling you to modify the range of the selected Data Flow Probe for the Management Zone. **Note:** Ranges can be displayed in the **Edit Probe Configuration** dialog box either according to IP range format or the CIDR format, as explained in "New/Edit Range Dialog Box" on page 62. For details on editing Probe ranges, see "Data Flow Probe Setup Window - Details Pane" on page 69 > "Details Pane (Probe)" on page 71 and "Ranges Pane" on page 75. • **Select Range.** Opens the Select Range dialog box, enabling you to select the sub-ranges you want to include or exclude from the full range of the selected Probe. In the Select Range dialog box, you can select multiple sub-ranges. If a sub-range has more than one excluded section, you cannot choose to exclude only one section. If you choose to exclude only one section, all sections will be excluded. **Note:** Ranges can be displayed here either according to the IP range format or the CIDR format, as explained in "New/Edit Range Dialog Box" on page 62. • **Delete Range.**Enables you to delete a sub-range from the Management Zone. This button appears only if you select **Define partial ranges on Data Flow Probes**, and is active only if you have previously added at least one sub-range of the Pobe to the Management Zone. Clicking this button deletes the sub-range from the Management Zone, but not from the Probe. • **<Probes pane>.** Displays the Data Flow Probes defined in UCMDB.

Settings Tab

This tab allows you to configure global settings for the selected Management Zone.

For information about configuring the Management Zone global settings, see "Global Settings Dialog Box" on page 258.

Note: If you configure global settings for an individual Management Zone, these settings override the global Management Zones configuration settings.

Zone-Based Discovery View

This view enables you to manage Management Zones, run discovery activities in the Management Zones, and troubleshoot why expected CIs are missing after discovery.

To access	**Data Flow Management > Discovery Control Panel > Zone-Based Discovery tab**

Important information	This view displays all of the Management Zones defined in Universal Discovery, and all of the discovery activities that have been defined in each Management Zone.
	
	The right pane of the Zone-Based Discovery view displays varying information, depending on what you select in the Management Zones tree.
	
	If you select:
	• The Management Zones tree root, the Zone-Based Discovery view displays:
	  ▪ "Management Zone Actions" on page 269
	  ▪ "Discovery Status Pane" on page 270
	• A Management Zone, the Zone-Based Discovery view displays:
	  ▪ "Management Zone Details Pane" on page 269
	  ▪ "Discovery Status Pane" on page 270
	• A discovery activity, the Zone-Based Discovery view displays:
	  ▪ "Activity Details Pane" on page 271
	  ▪ "Discovery Status Pane" on page 270

Relevant tasks	"How to Run Zone-Based Discovery" on page 246
See also	• "Universal Discovery Overview" on page 238 • "Management Zone Ranking" on page 243 • "New/Edit Management Zone Dialog Box" on page 262 • "Discovery Troubleshooter" on page 245 • "Discovery Troubleshooter Wizard" on page 252

Management Zones Pane

User interface elements are described below:

UI Element	Description
	**New.** Enables you to create a Management Zone. For more information on creating Management Zones, see "New/Edit Management Zone Dialog Box" on page 262. In addition, when you select a Management Zone you can create discovery activities in that Management Zone. For more information on defining discovery activities, see *HP Universal CMDB Discovery and Integration Content Guide*.
	**Edit.** • **Management Zone selected:** Opens the Edit Management Zone dialog box, enabling you to make changes to the definition of the selected Management Zone. • **Discovery activity selected:** Opens the relevant discovery activity wizard, enabling you to make changes to the selected discovery activity.
	**Delete.** Enables you to delete the selected Management Zone or discovery activity. **Note:** When you delete a Management Zone, all activities associated with it are also deleted.
	**Find Management Zone.** Opens the Find Management Zone dialog box, enabling you to locate a Management Zone in the tree by name or by IP address. For details, see "Find Management Zone Dialog Box" on page 257.
	**Reload Data.** Refreshes the list of Management Zones and discovery activities.
	**Activate.** Activates the selected Management Zone or discovery activity. **Note:** Activating a Management Zone activates all of its activities.
	**Deactivate.** Deactivates the selected Management Zone or discovery activity. **Note:** Deactivating a Management Zone deactivates all of its activities.
	**Pause.** • **Management Zone selected:** Pauses the selected Management Zone, including all of the activated and running discovery activities in the Management Zone. **Note:** Pausing a Management Zone does not have any effect on discovery activities that are not activated. • **Discovery activity selected:** Pauses the selected discovery activity.

UI Element	Description
	**Resume.** • **Management Zone selected:** Resumes the selected Management Zone (if paused), including all of the paused discovery activities in the Management Zone. **Note:** Resuming a Management Zone does not have any effect on discovery activities that are not activated. • **Discovery activity selected:** Resumes the selected discovery activity.
	**Rerun.** • **Management Zone root selected:** Runs discovery again in all of the Management Zones. • **Management Zone selected:** Runs discovery again in the selected Management Zone. • **Discovery activity selected:** Runs the selected discovery activity again.
	**Troubleshoot Missing CIs.** Opens the Discovery Troubleshooter wizard. If a CI is missing from the results of a Data Flow Probe and you expected to see it,the Discovery Troubleshooter wizard tries to find the missing CI. **Note:** This feature is enabled in a Management Zone only after the Infrastructure and Basic Software Configuration discovery activities have run. For more information on Discovery Troubleshooter, see "Discovery Troubleshooter" on page 245.
 / 	**Expand/Collapse All.** Expands/Collapses the Management Zone tree structure. When expanded, all discovery activities that have run in the Management Zones are listed.
Management Zones tree	Displays the defined Management Zones and their discovery activities. •  . Represents the Management Zone root directory. •  . Represents a Management Zone. ▪  . Indicates that all of the activated activities in the Management Zone are running. ▪  . Indicates that all of the activated activities in the Management Zone are paused. ▪  . Indicates that some of the activated activities in the Management Zone are running and some are paused. •  /  . Represents a running/paused activity in a Management Zone.

UI Element	Description
<right-click menu>	In addition to some of the functionality described above, right-clicking a discovery activity enables you to do the following: • **Clear Probe Results Cache.** Clears the selected activity's results cache on the Probes. **Note:** If an activity's results cache is cleared, all discovery results are sent again the next time the activity runs.

Management Zone Actions

Displayed when you select Management Zones root, this pane provides a portal to creating Management Zones, managing the ranking levels of the Management Zones, and configuring global Management Zone settings.

User interface elements are described below:

UI Element (A-Z)	Description
	Create Management Zone. Opens the New Management Zone dialog box, enabling you to create a new Management Zone. For details, see "New/Edit Management Zone Dialog Box" on page 262.
	View/Edit Management Zone Ranking. Opens the Management Zone Ranking dialog box, enabling you to manage the ranking levels of the Management Zones. For details, see "Management Zone Ranking Dialog Box" on page 261.
	View/Edit Global Configurations. Opens the Global Configurations dialog box where you can view and edit global Management Zone configurations. For details, see "Global Settings Dialog Box" on page 258. **Note:** An individual Management Zone's configuration settings override the settings defined in the global configuration settings. For details on configuring an individual Management Zone, see "New/Edit Management Zone Dialog Box" on page 262 (**Configurations** tab).

Management Zone Details Pane

Displayed when you select a Management Zone in the Management Zone tree.

Important information	To edit the details of the selected Management Zone, click the **Edit** button in the Management Zones pane.

User interface elements are described below:

UI Element (A-Z)	Description
Description	The description of the Management Zone, defined when the Management Zone was created.
Ranges Method	The method for defining ranges for the Management Zone, as defined when creating the Management Zone: • **Based on full Data Flow Probe ranges** • **Based on partial Data Flow Probe ranges** For more details, see "New/Edit Management Zone Dialog Box" on page 262.
Ranges	Displays the defined ranges for the selected Management Zone on the selected Data Flow Probe. **Note:** • You cannot edit ranges in this pane. To edit ranges, see "New/Edit Range Dialog Box" on page 62. • If the ranges method is **Based on partial Data Flow Probe ranges**, the range can be displayed here either according to the IP range format or CIDR format, as explained in "New/Edit Range Dialog Box" on page 62.

Discovery Status Pane

Displayed when you select the Management Zones root, a Management Zone, or a discovery activity in the Management Zone tree.

User interface elements are described below:

UI Element	Description
Progress Tab	• The discovery progress displayed varies depending on the area of focus. For user interface details, see "Discovery Progress Dialog Box" on page 318. ▪ **Management Zone root:** Displays the aggregated progress of all of the activities in all of the Management Zones. ▪ **Management Zone:** Displays the aggregated progress of all of the activities in the selected Management Zones. ▪ **Discovery Activity:** Displays the progress of the discovery activity. • The information in this pane is automatically refreshed every 30 seconds. • Use the information displayed in this pane to drill down to problematic trigger CIs, to uncover specific problems that Universal Discovery encountered during the run—for example, incorrect credentials. You can also add newly discovered CIs to the trigger CI list. • Use the SHIFT and CTRL keys to select adjacent and non-adjacent CIs in a list.

UI Element	Description
Results Tab	Displays the results from discovery activities that ran in the Management Zones. The results displayed depend on the area of focus. For details, see "Discovery Results Tab/Pane" on page 324.

Activity Details Pane

Displayed when you select a discovery activity in the Management Zones tree.

User interface elements are described below:

UI Element	Description
Overview Tab	Displays the type and status of the discovery activity, and a summary of the activity as it was defined when it was created. To edit an activity, select the activity in the Management Zones tree, and click the **Edit Activity**  button.

UI Element	Description
Activity Jobs Tab	Displays the activity jobs available for the discovery activity. • **Activity Jobs Toolbar** ▪  **Go to Adapter**. Redirects you to the adapter for the selected activity job. ▪  **View permission details.** Opens the Discovery Permissions dialog box, enabling you to view the permissions data for the selected activity job. ▪  **View Discovered CITs in Map.** Displays the selected adapter, together with its CIs and relationships, in the Discovered CITs Map window. Hold the cursor over a CIT to read a description in a tooltip. ▪  **View Parameters.** Opens the Activity Job Parameters dialog box, enabling you to view the parameters for the selected activity job. ▪  **Edit Script.** Displays a list of scripts related to the selected activity job. Select a script and edit it in the Script Editor. ▪  **Edit Trigger Query.** Displays the trigger query related to the selected activity job, enabling you to open and edit it in the Trigger Query Editor. ▪  **. Hide/Show Legend.** Hides/displays the legend at the bottom of the pane. • **Activity Jobs Grid**. Displays the information about jobs available for the discovery activity. ▪ **Activity Job Name.** The name of the activity job. ▪ **Discovered CITs.** The CITs discovered by the activity job. ▪ **Protocols.** The protocols used by the activity job. ▪ **Scheduling.** ○ **Activity Schedule** indicates that the activity job runs according to the activity's discovery schedule. ○ For an activity job that does not run according to the activity's discovery schedule, but rather according to its own discovery schedule, displays the job's schedule. • **Indicator Icons** The following icons indicate the status of the jobs: ▪  **. Enabled job.** The job is enabled with permissions. ▪  **. Enabled job has no permissions.** The job is enabled but it is missing permissions.

UI Element	Description
	▪  **. Job not enabled.** The job is not enabled.

Chapter 11

Module/Job-Based Discovery

This chapter includes:

Modules/Jobs-Based Discovery Overview

You can customize discovery by making changes to an out-of-the-box discovery job or building your own discovery jobs.

For details, see "How to Run Module/Job-Based Discovery" on next page.

For details about the jobs and how they are organized in modules, see the *HP Universal CMDB Discovery and Integration Content Guide*.

Viewing Permissions While Running Jobs

During a job run, you often need to know which credentials are being used to connect to a component in the system. You also often need to know the effect of a run on network performance, for example, whether the job should be run at night instead of during the day. View Permissions enables you to view the objects and parameters of a job's Jython script commands, as can be seen in the following image:

Permission	Operation	Usage Description	Objects and Parameters
shellprotocol	exec	Basic login	uname ver
shellprotocol	exec	CPU Info	AIX: lsattr | grep "proc" AIX: prtconf | grep "proc" FreeBSD: dmesg | grep "cpu|Multiprocessor" FreeBSD: dmesg | grep -A1 "CPU:" FreeBSD: sysctl hw.model hw.ncpu hw.clockrate HPUX: model Linux: cat /proc/cpuinfo SunOS: /usr/sbin/psrinfo -v SunOS: prtconf Windows: reg query HKEY_LOCAL_MACHINE\HARDWARE\DESCRIP...

Note: The information you define here is not dynamic, that is, if an adapter is changed, the information in this dialog box is not updated.

For details, see "Discovery Permissions Window" on page 303.

Example of Using the Discovery Permissions Window:

You are running the **Host Connection by Shell** job to discover a host running on a UNIX system. An error message in the Discovery Progress pane shows that 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.

How to Run Module/Job-Based Discovery

This task describes how to begin mapping your system and its components. You would use this workflow to customize the components of a module.

Note: For details about running Zone-based discovery, see "How to Run Zone-Based Discovery" on page 246.

This task includes the following steps:

1. **Prerequisites**

   a. Verify that the Data Flow Probe is installed on a Windows machine.

   Note: The Data Flow Probe installed on a Linux platform is intended only for integrations, and not for discovery

   b. Verify that the relevant packages are deployed.

If you need to deploy discovery packages, see "How to Deploy a Package" in the *HP Universal CMDB Administration Guide*.

2. **Determine the network range**

Define the range of the network to be discovered. For details, see "New/Edit Range Dialog Box" on page 62.

> **Note:** Adapters try to connect to every IP address in a range. Therefore, if a range is wide, network performance may be affected.

3. **Set the relevant credentials**

To enable the Data Flow Probes to connect to servers or applications using specific protocols, you must set the relevant credentials (for example, UD, NTCMD, SNMP, TTY, or WMI). For details on protocol parameters, see the *HP Universal CMDB Discovery and Integration Content Guide*.

> **Note:** The Data Flow Probe tries to connect to a node by using each credential in turn. Universal Discovery then saves the successful credential. The next time the Data Flow Probe connects to this node, it first tries to connect using the successful credential.

4. **Activate the relevant jobs**

Once you have defined the network range and set credentials, you can run discovery on specific jobs. For details on running specific jobs, see *HP Universal CMDB Discovery and Integration Content Guide*.

> **Tip:**
>
> - You can view a full description of a selected job in the **Properties tab > Description pane.**
> - You can search for all jobs that discover a particular connection type.
>
> For example, to search for all jobs that discover SNMP connections:
>
> In the **Discovery Control Panel > Discovery Modules/Jobs tab**, click the **Search for Discovery Job**  button. In the Find Jobs dialog box, enter **SNMP** in the **Name** box and click **Find All**. For details, see "Find Jobs Dialog Box" on page 307.

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 *HP Universal CMDB Developer Reference Guide*.

> **Caution:** Do not make changes to default adapters without consulting HP Software Support.

6. **Monitor the discovery process**

For details on monitoring the CIs that are discovered by the run, see "Discovery Progress Dialog Box" on page 318.

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 *HP Universal CMDB Modeling Guide*.

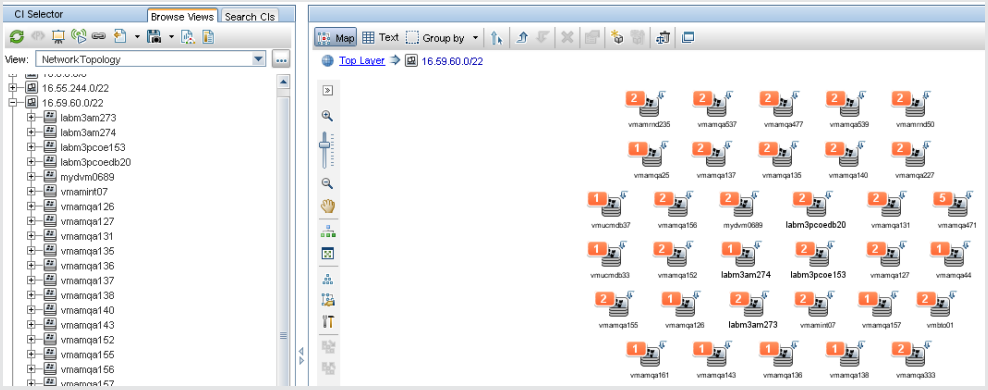
If necessary you can trigger queries to manually discover objects. For details, see "Trigger Queries Pane" on page 301.

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 *HP Universal CMDB Modeling Guide*.

Example – Creating a View to Display Discovered CI Instances:

To view the number of instances found by during discovery, select **Modeling > IT Universe Manager**, and display the view you created, as seen in the following illustration:



7. **View Discovery Results**

You can display overall results for a discovery job or you can filter the results by time range or by Data Flow Probe. Each time you log in to UCMDB and access the Discovery Control Panel, the results are updated so that the data displayed is the latest for the selected module or job.

For details viewing the discovery results, see "Discovery Results Tab/Pane" on page 324.

You can also view discovered CIs from the Data Flow Probe Status Window. For details, see "Data Flow Probe Status Window" on page 118.

8. **Troubleshoot the discovery progress**

You can check discovery progress to see which errors are being reported. For details, see the "Discovery Progress Dialog Box" on page 318.

How to Manually Activate Modules/Jobs/CIs

You can manually activate modules/jobs/CIs in the Discovery Modules/Jobs tab.

To manually activate a module/job:

- In the Discovery Modules pane, select the module/job, and click **Activate**  .

To manually activate a CI:

1. Select the job with the CI you want to activate manually.
2. Disable the Data Flow Probes for the job: In the job's **Properties** tab >**Trigger Queries** pane, select the query, and in the Probe Limit column, click the  button and ensure that no Probes are selected.
3. Manually activate CIs: In the **Details** tab, in the **Discovery Progress** pane, click the **Add CI**  button and manually add CIs.

   The job runs using only the redispatched CIs. For details, see "Discovery Modules/Jobs - Discovery Modules Pane" on page 295.

How to View Job Information on the 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:

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 "Discovery Job Operation Commands" on next page and "Job Operation Parameters" on page 285.

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).

Discovery Job Operation Commands

For details on viewing job information, see "How to View Job Information on the Data Flow Probe" on previous page.

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 285.

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 285.

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 285.

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 285.

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 *HP Universal CMDB Developer Reference Guide*. For details on the **appilog.common.system.typesClass ObjectStateHolder** method, see the **ObjectStateHolder** method in the online API documentation.

viewJobResults

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

For details on the job operation parameters, see "Job Operation Parameters" on page 285.

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	Click to filter the list to show results for one CIT only.
Total CIs	Click to go to the viewJobResultCiInstances page, to view a list of all CIs that have been discovered by a job.
Triggered CIs	Click to go to the viewJobTriggeredCIs page, to view a list of all Trigger CIs that have been discovered by a job.
Last Discover Time	The date and time that the job was invoked.

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

Column	Description
Job Name	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	Click to filter the list to show results for one CIT only.
Touched CIs	Click to go to the viewJobResultCiInstances page, to view a list of those CIs discovered by the job that are **Touched CIs**. For details, see "Job Operation Parameters" on page 285.
Non Touched CIs	Click to go to the viewJobResultCiInstances page, to view a list of those CIs discovered by the job that are not Touched CIs.
Triggered CIs for Touched CIs	Click to go to the viewJobTriggeredCIs page, to view a list of those Trigger CIs included in a job that are Touched CIs.
Triggered CIs for Non Touched CIs	Click to go to the viewJobTriggeredCIs page, to view a list of those Trigger CIs included in the job that are not Touched CIs.
Last Discover Time	The date and time that the job was invoked.

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

viewJobsStatuses

Click the **viewJobsStatuses** button to return status and scheduling information for all jobs. You can choose to filter the results. For details, see "Job Operation Parameters" on page 285.

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

The results page displays the following information:

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

Column	Description
Status	The severity of the job's status, as calculated by the Probe. • **Blocked.** Not in use. • **Removed.** The job is no longer active. • **Done/Total Triggers.** The number of trigger CIs that the Probe finished running on, against the total number of triggers for the job. For example, **(28/69)** indicates that there is a total of 69 triggers for the job, while the Probe has completed running on 28 of those triggers. • **Scheduled.** The job is scheduled to run. For details on scheduling jobs, see "Discovery Scheduler Dialog Box" on page 304. 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. Click to go 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. Click to go to the viewJobTriggeredCIs page.
Last Invocation	The date and time that the job was last run.
Next Invocation	The date and time that the job is next scheduled to run.
Last Total run duration (seconds)	The length of time, in seconds, taken to run the job in the previous invocation. This is calculated according to the start time of the first trigger until the end time of the last trigger, even if triggers were added later on.
Avg run duration (seconds)	The average duration (in seconds) per trigger of the time it took the Probe to run this job.
Recurrence	The number of times that the job was invoked. Click to go to the viewJobExecHistory page, to retrieve a history of job invocations.
Results	The number of CITs that have been discovered by the job. Click to go to the viewJobResults page to view the CITs.

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 285.

The results page displays the following information:

Column	Description
Threading info	The total number of worker threads created by the invocation, the free worker threads, and the stuck worker threads.
Total work time	The time that the Probe took to run this job.
Tasks waiting for execution	A list of jobs together with the number of Trigger CIs that are awaiting activation.
Max. Threads	The number of threads that are serving this job.
Progress	A summary of the current run, that is, since the specific run was activated. For example, `Progress: 2017 / 6851 destinations (29%)` means that out of 6851 CIs, 2017 CIs have already run.
Working Threads information	• **Thread Name.** The thread that is now running this job. Click to go to the **viewJobThreadDump** page. You use this page when a thread is running for a long time, and you must verify that this is because the thread is working hard, and not because there is a problem. • **Curr Dest. ID.** The name of the node on which the job is running. • **Curr Dest. IP.** The IP for which the job is discovering information. • **Work Time (Sec).** The length of time that this thread is running. • **Communication Log.** Click to go to the **viewCommunicationLog** page, to view an XML file that logs the connection between the Probe and a remote machine. For details, see the **Create communication logs** field in the "Execution Options Pane" on page 144.

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 282. • **Errors.** Click to go to viewJobErrorsSummary page, to view a list of error messages reported on this job. • **Triggered CIs.** Click to go 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 282. • **Avg run duration (seconds).** For details, see "Avg run duration (seconds)" on page 282. • **Recurrence.** The number of times that the job was invoked. Click to go to viewJobExecHistory page, to view a history of job invocations.
Results	The number of CITs that have been discovered by the job. Click to go to the viewJobResults page to view the CITs.

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 next page.

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. Click to go to the viewJobTriggeredCIs 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.

Column	Description
Total Exec. Duration (ms)	The time that it took for a job to run in the last invocation, including the periods when the job did not run.
Last Run Status	The status of the last run, that is, whether the run succeeded or failed. In case of failure, click to go to the viewJobProblems page, to view a list of Trigger CIs with problems.
Priority	The priority of the job. **Note:** The lower the value, the higher the priority.

viewJobTriggeredCIsWithErrorId

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

Job Operation Parameters

The following list includes job operation parameters.

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

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

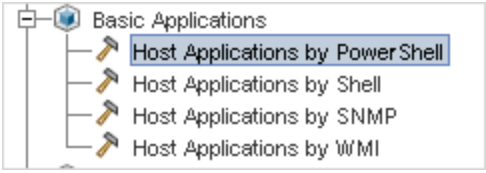
- **Error Id.** The error message hash string (error hash ID) that is displayed in the **Jobs_Problems** table.
- **HideRemovedJobs.True**: do not display jobs that have run previously and are not relevant to the current run.
- **Hide Touched CIs Info.** Touched CIs are CIs which were discovered in previous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

  True: the table displays the total number of CIs and the total number of Trigger CIs for each CIT. **False**: The table displays the total number of CIs and Trigger CIs divided between touched CIs and non-touched CIs.
- **includeNonTouched.** Enables filtering the table to view non-touched CIs. Choose between

viewing non-touched CIs only, all CIs (touched and non-touched), or none:

	Non-touched CIs	All CIs	No CIs
(boolean)includeTouchedCis	○ 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 Applications by PowerShell**:



- **maxRows.** The maximum number of rows that should be displayed in the results table. The default is 100 or 1000.
- **maxTriggeredCIs.** See **maxRows**.
- **objectID.** The CMDB object ID.
- **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 CMDB object ID of the trigger for a job.
- **triggeredCiID.** See **triggerCI**.

Permissions Document

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 of supported protocols, see the *HP Universal CMDB Discovery and Integration Content Guide*.

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

Module/Job-Based Discovery User Interface

This section includes:

Discovery Modules/Jobs View

Enables you to view and manage modules and jobs, to activate jobs, and to follow job progress.

To access	**Data Flow Management > Discovery Control Panel > Discovery Modules/Jobs tab**

Important information	• This tab is suitable for advanced users of Universal Discovery only.
	• Each change you make in Discovery Control Panel is delivered to and stored in the CMDB. From there, the changes are sent to the Probe. You can verify that changes have been sent to the Probe by opening the **wrapperProbe.log** file located in **C:\hp\UCMDB\DataFlowProbe\runtime\logs** and searching for the following lines:
	`processing document domainScopeDocument.bin`
	`Processing document domainScopeDocument.bin is done.`

Relevant tasks	"How to Run Module/Job-Based Discovery" on page 275

User interface elements are described below:

UI Element (A–Z)	Description
Dependency Map tab	Displays a visual representation of the real-time progress of the process. For details, see "Discovery Module/Jobs - Dependency Map Tab" on page 294.
Details tab	Enables you to manage a module's CIs and view CI statistics. For details, see "Discovery Module/Jobs - Details Tab" on page 292.
Discovery Modules pane	Each module includes jobs. You activate a module or job to discover a specific group of CIs. For details, see "Discovery Modules/Jobs - Discovery Modules Pane" on page 295.
Properties tab	Enables you to view and administer the properties of modules and jobs. For details, see "Discovery Modules/Jobs - Properties Tab" on page 299.

Create New Discovery Job Dialog Box

Enables you to create a job.

To access	Navigate to **Data Flow Management > Discovery Control Panel > Discovery Modules/Jobs**, right-click a module in the Discovery Modules pane, and select **New > Job**.

Discovery Job Details Pane

User interface elements are described below:

UI Element (A–Z)	Description
	Opens the Help document related to the selected job's adapter. To update or modify this document, see "Adapter Definition Tab" on page 137.
	Click to go to the adapter in the Resources pane.
	You can choose to view a map of the CIs and relationships that are discovered by the adapter, instead of a list. Click the button to open the **Discovered CITs Map** window. The selected adapter is shown together with its CIs and relationships. Hold the cursor over a CIT to read a description in a tooltip.
	Click to view permissions that are defined for specific adapters. For details, see "Discovery Permissions Window" on page 303. For details on editing these permissions, see "Permission Editor Dialog Box" on page 163.
Adapter	The adapter used by the job to discover the CIs.
Discovered CIs	The CIs that are discovered by this job.
Input CI Type	The CIT that triggers the CIs for this job.
Job Name	The name and description of the job and the package in which it is located. **Note:** Naming conventions for jobs: • Job names can contain the following characters: `a-z`, `A-Z`, `0-9`, hyphen (-), underscore (_), space ( ) • Job names must not start with a digit • Job names must be limited to a length of 50 characters
Required Protocols	The protocols needed by the activated job to access the system components.

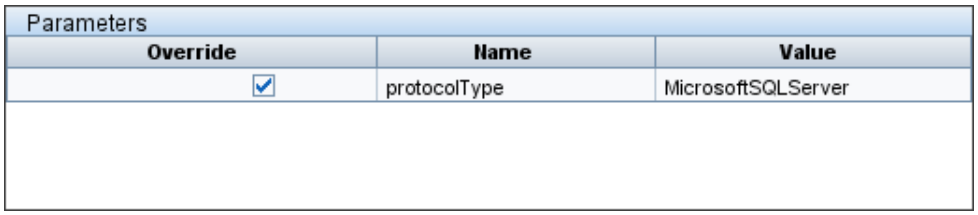
Parameters Pane

Enables you to override adapter behavior.

To view a description, hold the pointer over the parameter.

To access	Select a job in the **Discovery Modules** pane in the **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 Definition Tab" on page 137.
Value	The value defined in the adapter.

Trigger Queries Pane

Enables you to define one or more queries to be used as triggers to activate the selected job.

User interface elements are described below:

UI Element (A–Z)	Description
	**Add Query.** You can add one or more non-default TQL queries to be used as triggers to activate the selected job. Click to open the **Choose Discovery Query** dialog box which lists available queries for the job. Select a query to displayed it in the Query Preview pane. Hold the cursor over an TQL element to view details.
	**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.
	Click to add or remove Probes for a specific query. For details, see "Edit Probe Limitation for Query Output Dialog Box" on page 306.

UI Element (A–Z)	Description
	Click to open the **Trigger Query Editor**. For details, see "Trigger Query Editor Window" on page 308. **Available:** In the job's Properties tab only.
	Click to open the Modeling Studio. **Available:** In the job's Properties tab only.
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.

Global Configuration Files Pane

User interface elements are described below:

UI Element (A–Z)	Description
	**Edit.** Opens the selected configuration file in an appropriate editor. For example, the file msServerTypes.xml opens the Script Editor.

Discovery Scheduler Pane

Enables you to set up a schedule for this job.

User interface elements are described below:

UI Element (A–Z)	Description
	Click to add times to the **Allow Discovery to run at** list. The **Time Templates** dialog box opens. To add a time template to the list, in the **Time Templates** dialog box, click the **Add** button to open the **Edit Time Template** dialog box. For details, see "Edit Time Template Dialog Box" on page 306.
Allow Discovery to run at	Choose a template that includes the days and times when the job should run.
Edit scheduler	Click to open the **Discovery Scheduler**. For details, see "Discovery Scheduler Dialog Box" on page 304.

UI Element (A–Z)	Description
Invoke on new triggered CIs immediately	Enables the job to run as soon as the Trigger CI reaches the Probe. When this option is not selected, the job runs according to the schedule defined in the **Schedule Manager**. **Note:** If this option is not selected and a job is running, new triggered CIs are not run by the job. Although new triggered CIs are not run, they are counted into the status bar. This means the status bar does not reach 100% completed, even though the job successfully completed, and the user has to wait until the next run of the job for the status bar to reach 100% completed.

Discovery Module/Jobs - Details Tab

Enables you to view and administer modules and jobs, to follow the progress of the DFM process, and to manage errors during discovery.

To access	**Discovery Control Panel > Discovery Modules/Jobs tab >** Select a module/job in the left pane **> Details tab**.

Important Information	Depending which level you select in the **Discovery Modules** pane on the left, different information is displayed in the **Details** tab.
	If you select:
	• **The Discovery Module** root or a **module**, the following panes display information and statistics about all active jobs and errors discovered during a run:
	  ▪ "Progress Pane"
	  ▪ "Results Pane"
	• **A job**, the following is displayed:
	  ▪ "Discovery Job Details Pane"
	  ▪ "Progress Pane"
	  ▪ "Results Pane"
	• **Several jobs or modules**, the following is displayed:
	  ▪ "Selected Items Pane"

Relevant tasks	"Error Messages Overview" in the *HP Universal CMDB Developer Reference Guide*

Discovery Job Details Pane

Important information	Displayed when a job is selected in the Discovery Modules pane on the left.

User interface elements are described below:

UI Element (A–Z)	Description
	Opens the Help document related to the selected job's adapter. To update or modify this document, see "Adapter Definition Tab" on page 137.
	Click to go to the adapter in the Resources pane.
	You can choose to view a map of the CIs and relationships that are discovered by the adapter, instead of a list. Click the button to open the **Discovered CITs Map** window. The selected adapter is shown together with its CIs and relationships. Hold the cursor over a CIT to read a description in a tooltip.
	Click to view permissions that are defined for specific adapters. For details, see "Discovery Permissions Window" on page 303. For details on editing these permissions, see "Permission Editor Dialog Box" on page 163.
Adapter	The adapter used by the job to discover the CIs.
Discovered CIs	The CIs that are discovered by this job.
Input CI Type	The CIT that triggers the CIs for this job.
Job Name	The name and description of the job and the package in which it is located. **Note:** Naming conventions for jobs: • Job names can contain the following characters: `a-z`, `A-Z`, `0-9`, hyphen (-), underscore (_), space ( ) • Job names must not start with a digit • Job names must be limited to a length of 50 characters
Required Protocols	The protocols needed by the activated job to access the system components.

Results Pane

Displays the discovery results from discovery job runs.For details, see "Discovery Results Tab/Pane" on page 324.

Progress Pane

Displays the discovery progress. For details, see "Discovery Progress Dialog Box" on page 318.

Selected Items Pane

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

UI Element (A–Z)	Description
<right-click menu>	**Edit Scheduling**. Click to open the **Discovery Scheduler** to define a schedule for a specific job. For details, see "Discovery Scheduler Pane" on page 302.
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 301.

Discovery Module/Jobs - Dependency Map Tab

Displays a visual representation of the real-time progress of the discovery process. The map displays:

- CIs that were triggered by a job
- 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/Created/Last Updated CIs Dialog Box" on page 316

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

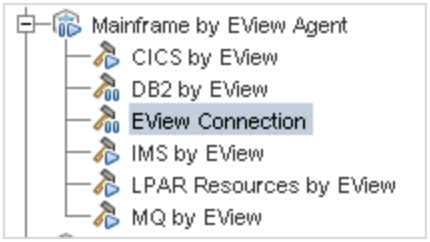
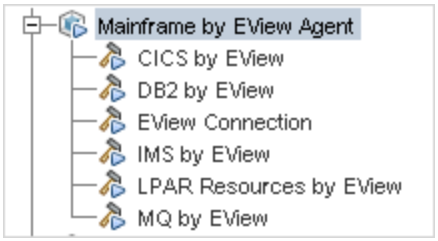
UI Element (A-Z)	Description
<right-click menu>	Use the right-click menu to view details for a job, CI, or link, for example, the number of CI instances (of a specific type) in the CMDB or the number of CI instances created by a specific job. Depending on which object is selected, the following menu options are displayed: • When a job is selected: **Show discovered CIs.** Click to view the CIs discovered by the job. To filter the query, select a CIT from the menu. **Show trigger CIs.** Click to view the CIs that triggered the job. • When a CI is selected: **Show all CIT instances.** Click to view all CIs of this CI type. • When a link from a CI to a job is selected: **Show trigger CIs for job.** Click to view CIs (of the selected type) that triggered the job. • When a link from a job to a CI is selected: **Show discovered instances.** Click to view CIs (of the selected type) that were discovered by the job.
<Toolbar>	For a description of the icons, see "Toolbar Options" in the *HP Universal CMDB 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 Modules/Jobs - Discovery Modules Pane

Enables you to view and manually manage modules and jobs. Each module includes the jobs necessary to discover specific CIs.

To access	**Data Flow Management > Discovery Control Panel > Discovery Modules/Jobs tab**.

User interface elements are described below:

UI Element (A–Z)	Description
	**Refresh All.** Updates the modules.
	**Search for Discovery Job.** Click to open the **Find Jobs** dialog box. For example, to search for all jobs that discover SNMP connections, in the **Find Jobs** dialog box, enter **SNMP** in the **Name** box and click **Find All**. For details, see "Find Jobs Dialog Box" on page 307.
	**Activate Selected Discovery Jobs.** You can run one job or several jobs in a module, and one or several modules. Select the jobs or modules and click **Activate**.
	**Deactivate Selected Discovery Jobs.** Select the jobs or modules to be stopped and click **Deactivate**.
	Represents the module root. To create a module, right-click to enter the name of the module you are creating. **Note:** A name is case sensitive. Names beginning with an upper case letter appear in the Discovery Modules list before names beginning with a lower case letter.
	Represents a module. •  . Indicates that some of a module's jobs are activated.  •  . Indicates that all of a module's jobs are activated. 

UI Element (A–Z)	Description
	Represents a job. •  . Indicates that the job is active. •  . Indicates that the job is paused. To view an adapter description, hold the pointer over the icon. Jobs contain configuration information derived from adapters and other resources and are the entities controlled by users, for example, when activating or deactivating a module. For details on the right-click menu, see "Right-Click Menu" below.
	An exclamation mark signifies that one or more of the jobs is experiencing a problem that could affect the discovery process, for example, a protocol connection failure. To view the reason for the problem, click the **(show errors)** link in the Discovery Progress pane. For details, see "Discovery Module/Jobs - Details Tab" on page 292. **Note:** If a problem is resolved by clicking the **Refresh All** button, the Problem Indicator disappears.

Right-Click Menu

UI Element (A–Z)	Description
 **Activate**	**Module:** Runs the jobs in the selected module. **Job:** Runs the selected jobs The Discovery Module discovers CITs and relationships of the types that are described in each job, and places them in the CMDB. For example, the Class C IPs by ICMP job discovers the **Dependency**, **IpAddress**, and **Membership** CITs and relationships.
 **Clear Probe Results Cache**	Clears the results cache on the Probes. **Note:** If the results cache is cleared, all discovery results are sent again the next time the jobs run.
 **Content Help**	Opens the Help document related to the selected job's adapter. To update or modify this document, see "Adapter Definition Tab" on page 137. To see the full *HP Universal CMDB Discovery and Integration Content Guide*, select **Help > Discovery and Integrations Content Help**.

UI Element (A–Z)	Description
Create New > Job	Opens the Create New Discovery Job dialog box, enabling you to create a job. For details, see "Create New Discovery Job Dialog Box" on page 288.
Create New > Module	Enables you to define a new name for the module root. **Note:** Naming conventions for modules: • Module names can contain the following characters: `a-z`, `A-Z`, `0-9`, hyphen (-), underscore (_), space ( ), and forward slash (/) • Module names must not start with a digit • Module names must be limited to a length of 50 characters
Deactivate	**Module:** Stops the running jobs in the selected module. **Job:** Stops the selected running jobs. **Note:** To stop all the running jobs simultaneously, right-click the **Discovery Modules** root folder and click **Deactivate all jobs**.
Delete	Enables you to delete the selected module. **Caution:** Only administrators with an expert knowledge of the Universal Discovery process should delete modules.
Delete job	Enables you to delete the selected job.
Edit Scheduling	Opens the **Discovery Scheduler** to define a schedule for the selected job.
Edit Script	Enables you to select and edit one of the selected job's scripts.
Go to adapter	Opens the details of the selected adapter in the Adapter Management module, enabling you to view and edit its definition.
Move to	Enables you to move the selected module folder or job to a different folder.

Pause	Click to pause an active job.
	To pause all active jobs simultaneously, right-click the **Discovery Modules** root folder and click **Pause jobs**.
	Note:
	• When you pause an active job:
	  ▪ triggers that are currently running continue to run until they are finished
	  ▪ all the execution information is retained, including errors
	• Jobs are paused based on their defined job execution policies. For details, see "Job Execution Policies" on page 28.

UI Element (A–Z)	Description
Rename	Enables you to enter a new display name for the selected module. **Available:** When you right click a module
Rename Job	Opens the **Rename Job** dialog box, enabling you to enter a new display name for the job. **Note:** You cannot rename active jobs. **Available:** When you right click a job
Rerun Discovery	Reruns the selected job using the selected Trigger CIs.
Resume	Enables you to resume a paused job. To resume all paused jobs simultaneously, right-click the **Discovery Modules** root folder and click **Resume jobs**.
Save as...	Enables you to clone the selected job.

Discovery Modules/Jobs - Properties Tab

Enables you to view and administer the properties of modules and jobs.

To access	**Discovery Control Panel > Discovery Modules/Jobs tab > Properties tab**
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 304. • **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" below. • **A job**, the **Parameters**, **Trigger Queries**, **Global Configuration Files**, and **Discovery Scheduler** panes are displayed. For details, see below.

Module Jobs Pane

Enables you to view the active jobs for the selected module.

User interface elements are described below:

UI Element (A–Z)	Description
	**Add Discovery Job to Module.** Opens the **Choose Discovery Jobs** dialog box where you can select jobs from more than one zip file. (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 discovered CITs as a map**. You can choose to view a map of the CIs and links that are discovered by the adapter, instead of a list. Click the button to open the **Discovered CITs Map** window. The selected adapter is shown together with its CIs and relationships. Hold the cursor over a CIT to read a description in a tooltip.
<Column 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 *HP Universal CMDB Modeling Guide*.
<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 304.
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**.

UI Element (A–Z)	Description
Trigger Queries	The name of the query that activated the job.

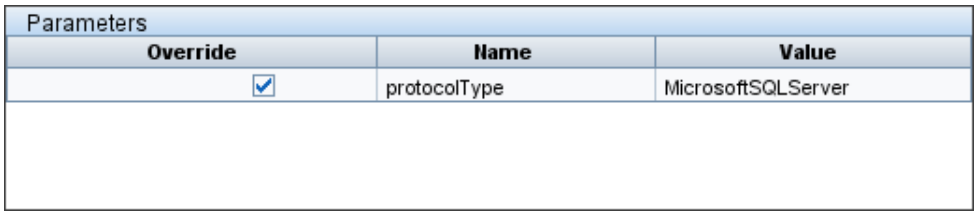
Parameters Pane

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:  Parameters Override | Name | Value protocolType | MicrosoftSQLServer For details on editing parameters in the Adapter Parameters pane, see "Adapter Definition Tab" on page 137.
Value	The value defined in the adapter.

Trigger Queries Pane

Enables you to define one or more queries to be used as triggers to activate the selected job.

User interface elements are described below:

UI Element (A–Z)	Description
	**Add Query.** You can add one or more non-default TQL queries to be used as triggers to activate the selected job. Click to open the **Choose Discovery Query** dialog box which lists available queries for the job. Select a query to displayed it in the Query Preview pane. Hold the cursor over an TQL element to view details.
	**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.
	Click to add or remove Probes for a specific query. For details, see "Edit Probe Limitation for Query Output Dialog Box" on page 306.
	Click to open the **Trigger Query Editor**. For details, see "Trigger Query Editor Window" on page 308. **Available:** In the job's Properties tab only.
	Click to open the Modeling Studio. **Available:** In the job's Properties tab only.
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.

Global Configuration Files Pane

Lists the global configuration files defined for the adapter used by the selected job.

User interface elements are described below:

UI Element (A–Z)	Description
	**Edit.** Opens the selected configuration file in an appropriate editor. For example, the file msServerTypes.xml opens the Script Editor.

Discovery Scheduler Pane

Enables you to view information about the schedule set up for the selected job.

User interface elements are described below:

UI Element (A–Z)	Description
	Click to add times to the **Allow Discovery to run at** list. The **Time Templates** dialog box opens. To add a time template to the list, in the **Time Templates** dialog box, click the **Add** button to open the **Edit Time Template** dialog box. For details, see "Edit Time Template Dialog Box" on page 306.
Allow Discovery to run at	Choose a template that includes the days and times when the job should run.
Edit scheduler	Click to open the **Discovery Scheduler**. For details, see "Discovery Scheduler Dialog Box" on next page.
Invoke on new triggered CIs immediately	Enables the job to run as soon as the Trigger CI reaches the Probe. When this option is not selected, the job runs according to the schedule defined in the **Schedule Manager**. **Note:** If this option is not selected and a job is running, new triggered CIs are not run by the job. Although new triggered CIs are not run, they are counted into the status bar. This means the status bar does not reach 100% completed, even though the job successfully completed, and the user has to wait until the next run of the job for the status bar to reach 100% completed.

Discovery Permissions Window

Enables you to view permissions data for jobs.

To access	**Data Flow Management > Discovery Control Panel > Discovery Module/Jobs tab**. 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 274 • "Adapter Definition Tab" on page 137 • "Permission Editor Dialog Box" on page 163

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*.

UI Element (A-Z)	Description
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 also can use this time template with the same schedule. • If you change a schedule for a job, DFM next runs the job according to the following calculation: The current date and time plus the selected interval. For example, if you choose **Once**, the Invocation Time is in one hour. For details on creating a time template, see "Edit Time Template Dialog Box" on page 306.

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

UI Element (A–Z)	Description
Validate Expression	Click to validate the Cron expression you entered.

UI Element (A–Z)	Description
<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. • **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.
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.

UI Element (A–Z)	Description
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, that is, 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/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 86.

To access	**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 304

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 CI type list. Locate the CI type that you are searching for. • **Output type.** CIs that are discovered as a result of the activated job.
Find Next	The next job meeting the search criteria is highlighted.

Time Templates Dialog Box

Enables you to define a daily or weekly schedule to run selected jobs.

To access	**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
	Click to add a time template. Opens the **Edit Time Template** dialog box.
	Select a time template and click to delete.
	Select a time template and click to edit it. 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	**Data Flow Management > Discovery Control Panel > Discovery Modules/Jobs** tab **> 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. That is, if an Input query queries for IPs running SNMP, a Trigger query queries for IPs running SNMP in the range 195.0.0.0-195.0.0.10.
See also	• "Trigger CIs and Trigger Queries" on page 24 • "Input Query Editor Window" on page 158

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

UI Element (A–Z)	Description
<Panes>	• "CI Type Selector Pane" below • "Editing Pane" on next page • "Information Pane" on next page
Query Name	The name of the Trigger query that activates the job.

CI Type Selector Pane

Displays a hierarchical tree structure of the CI Types found in the CMDB. For more details, see "CI Type Manager User Interface" in the *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

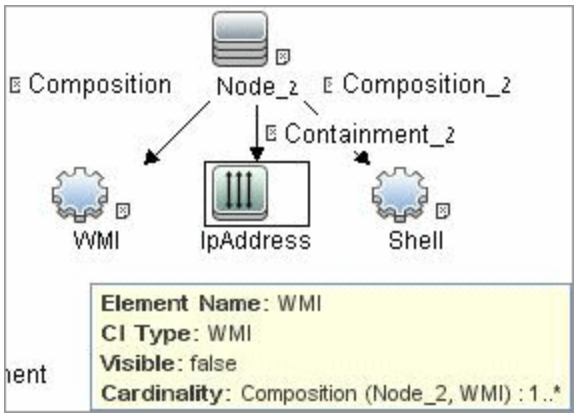
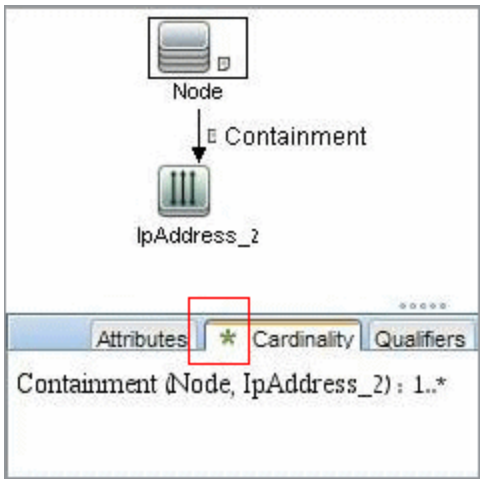
Enables you to edit the node selected in the **Trigger Queries** pane.

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

UI Element (A–Z)	Description
<node>	Click to display information about the node in the information pane.
<right-click menu>	To view a list of icons, see "Shortcut Menu Options" in the *HP Universal CMDB Modeling Guide*.
<Toolbar>	To view a list of icons, see "Toolbar Options" in the *HP Universal CMDB Modeling Guide*.

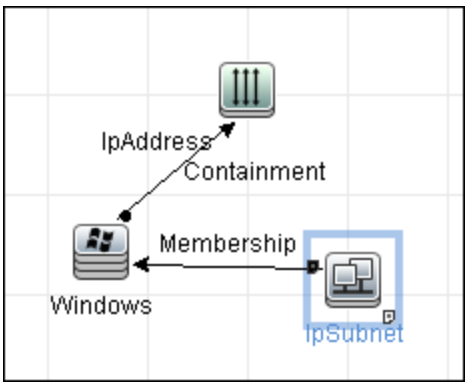
Information Pane

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*.

UI Element (A-Z)	Description
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*.
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*.

Chapter 12

Discovery Progress and Results

This chapter includes:

Managing Problems With Error Reporting

During discovery, many errors may be uncovered, for example, connection failures, hardware problems, exceptions, time-outs, and so on. You can drill down from the Trigger CI that caused the problem to view the error message itself.

DFM differentiates between errors that can be ignored (for example, an unreachable host) and errors that must be dealt with (for example, credential problems or missing configuration or DLL files). Moreover, DFM reports errors once, even if the same error occurs on successive runs, and reports an error even if it occurs once only.

For details on severity levels, see "Error Severity Levels" in the *HP Universal CMDB Developer Reference Guide*.

Error Table in Database

All DFM errors are saved to the **discovery_problems** table in the Probe Manager database schema. (The error information is saved to the database—and is not handled in the Probe's memory—to guarantee delivery to the server.) The Probe holds the latest list of problems for each Trigger CI. After each run, the Probe checks for changes and reports them in the Discovery Progress pane. For details, see "Discovery Progress Dialog Box" on page 318.

How to Find Discovery Errors

This task describes how to investigate problems that arise during discovery.

> **Note:** For details about severity levels and so on, see "Managing Problems With Error Reporting" above.

This task includes the following steps:

- "Prerequisites" on next page
- "Select the Module/Job" on next page

- "Locate the Problem CI" below

1. ### Prerequisites

   Set up DFM. For details, see "Data Flow Management Setup" on page 26.

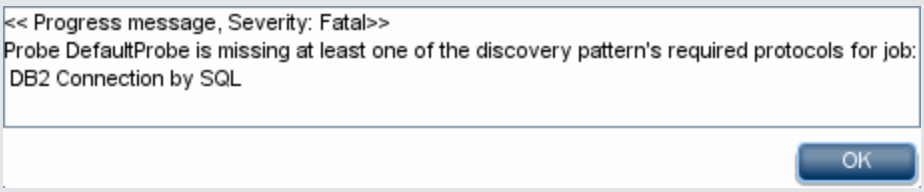
2. ### Select the Module/Job

   You can view error messages for one job, one module, or all modules. For details on running a job, see "How to Run Module/Job-Based Discovery" on page 275.

3. ### Locate the Problem CI

   Use the Discovery Progress user interface to drill down to the error messages. For details, see "Discovery Progress Dialog Box" on page 318.

   Example of an error message:

How to Manage Discovery Errors

This task describes how to investigate problems that arise during a discovery run.

Note: For details about severity levels and so on, see "Managing Problems With Error Reporting" on previous page.

This task includes the following steps:

- "Prerequisites" below
- "Run the discovery job" below
- "Locate the problem CI" below
- "Troubleshoot the problem" on next page

1. ### Prerequisites

   Set up DFM. For details, see "Data Flow Management Setup" on page 26

2. ### Run the discovery job

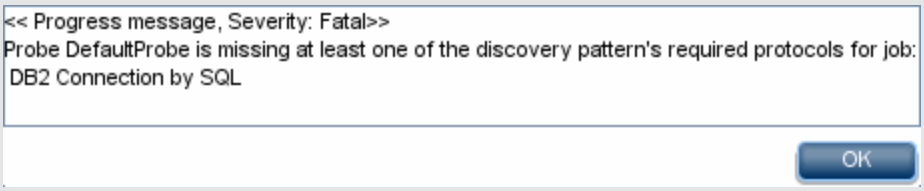
   You can view error messages for one job, one module, or all modules. For details on running a job, see "How to Run Module/Job-Based Discovery" on page 275.

3. ### Locate the problem CI

   Use the Discovery Progress pane to drill down to the error messages. For details, see "Discovery Progress Dialog Box" on page 318.

Example:

DFM displays the error message:



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 144.
   - For details on managing problems, see "Managing Problems With Error Reporting" on page 312.

Discovery Progress and Results User Interface

This section includes:

Choose CIs to Add Dialog Box

Enables you to choose CIs to run with selected jobs.

To access	**Discovery Progress** > Drill down to the CI instances, and click the **Add CI** button. For more details, see "Discovery Progress Dialog Box" on page 318.

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

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 *HP Universal CMDB 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.
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.** Click to display 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 was reported. **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 Probe Dialog Box

Enables you to filter the Probe list.

To access	Click a **Filter** button in the **Discovery Control Panel views** tab: For details, see "Discovery Progress Dialog Box" on page 318 and "Discovery Results Tab/Pane" on page 324

Discovered/Created/Last Updated CIs Dialog Box

The Discovered CIs dialog box enables you to view all CI instances found for a selected query node.

The Created/Last Updated CIs dialog boxes enable you to view all CI instances that were created or updated during the last discovery run.

The Created by <Job> dialog box displays the CI instances created when running a selected job.

To access	These dialog boxes are accessible from various places in the Discovery Control Panel, and all display information about discovered CI instances. • **A job's Dependency Map tab.** Right-click a CI, a job or a relationship. For more information, see "Discovery Module/Jobs - Dependency Map Tab" on page 294. • **Discovery progress**: Drill down to a CI and click **Show additional data**  • **Discovery Results**: Select a CI and click **View Created/Updated Instances**  .
Important Information	When viewing discovery results, the CI instances displayed are retrieved from the server when this dialog box opens. The number of CIs may differ from the number of CIs displayed in the **Results** pane because some created CIs may have been merged or deleted since they were created by the job.

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

UI Element (A-Z)	Description
Show CI instances of: Network	Specify the CIT you want displayed in the table. The table also includes the children of the selected CIT.
	**Delete from CMDB.** Deletes the selected CI from the database.
	**Properties.** Opens the Configuration Item Properties dialog box for the selected CI.
	**Refresh.** Refreshes the list of CI instances.

UI Element (A-Z)	Description
	**Set Filter.** Filters the CI instances you want to display for the selected discovery. Opens the Filter CI Instances dialog box.
	**Clear Filter.** Clears the filter definitions you created in the Filter CI Instances dialog box.
	**Select Columns.** Enables you to select the columns to be displayed. For details, see "Select Columns Dialog Box" in the *HP Universal CMDB Modeling Guide*.
	Enables you to set the sort order of the CI instances. For details, see "Sort Column Content Dialog Box" in the *HP Universal CMDB Modeling Guide*.
	**Find.** Displays the **Find** toolbar.
	**Send Mail.** Enables you to send the table data in an email.
	Choose the export format for the table data. The available options are: • **Excel**. The table data is formatted as an .xls (Excel) file that can be displayed in a spreadsheet. • **PDF**. The table data is exported in PDF format. **Note:** When exporting to PDF, select a reasonable number of columns to display to ensure that the report is legible. • **CSV**. The table data is formatted as a comma-separated values (CSV) text file that can be displayed in a spreadsheet. **Note:** For the CSV formatted table data to display correctly, the comma (,) must be defined as the list separator. In Windows, to verify or modify the list separator value, open Regional Options from the Control Panel, and on the Numbers tab ensure that the comma is defined as the List Separator value. In Linux, you can specify the list separator in the application that opens the CSV file. • **XML**. The table data is formatted as an XML file that can be opened in a text or XML editor. **Tip**: To extract HTML code from the report: ▪ Save the file as HTML ▪ Open the file in an HTML editor ▪ Copy the relevant table into the target file

UI Element (A-Z)	Description
30 Rows per page	Select the number of rows to be displayed on each page. You can also manually enter value for the number of rows per page.
3 of 16528	Click to navigate through the results page by page or to jump to the first or last page.
<CI Instances>	The CI instances created during the discovery. You can double-click an instance to open the Configuration Item Properties dialog box for that CI.
<CI instances shortcut menu>	For details, see "IT Universe Manager Shortcut Menu" in the *HP Universal CMDB Modeling Guide*.

Discovery Progress Dialog Box

This dialog box displays the progress of running discoveries, and enables you to drill down to discovered CI instances.

To access	• In the **CI Instances dialog box**, right-click a CI instance, click **Actions**, and select **Show Discovery Progress**. • **Discovery Control Panel** views: ▪ **Zone-Based Discovery > Discovery Status > Progress tab** ▪ **Discovery Modules/Jobs > Details tab > Discovery Progress pane**
Relevant tasks	"How to Check the Status of Application Discovery (Rediscover a View)" in the *HP Universal CMDB Modeling Guide*.
See also	"Error Messages Overview" in the *HP Universal CMDB Developer Reference Guide*

Triggered CIs View - Progress/Status Matrix

Displays the status of triggered CIs through the progress of discovery.

UI Element (A-Z)	Description
	**Refresh.** Refreshes the matrix.
	**Add CI.** Opens the Choose CIs to Add dialog box, enabling you to add a newly-discovered CI to the triggered CI list. For details, see "Choose CIs to Add Dialog Box" on page 314. **Available: Discovery Modules/Jobs** view only, when you select a module/job.

UI Element (A-Z)	Description
	**Rerun Discovery.** Enables you to rerun the selected discovery modules/jobs.
 / 	**Pause / Resume.** Enables you to pause or resume the selected discovery **Note:** • When you pause an active job: ▪ triggers that are currently running continue to run until they are finished ▪ all the execution information is retained, including errors • Jobs are paused based on their defined job execution policies. For details, see "Job Execution Policies" on page 28. **Available: Discovery Modules/Jobs** view only
Progress	Displays how far the discovery has progressed (%). **Note:** When you activate discovery, the trigger CIs list are prepapred During this time, discovery progress may not be reflected immediately. Thereafter, discovery progress is automatically refreshed every 30 seconds.

Understanding the Progress/Status Matrix

Progress Status	Total			
Pending Probe	Displays the total number of trigger CIs waiting for the Probe to pick them up for execution.	Displays the number of triggered CIs successfully waiting for the Probe to pick them up for execution.	--	--
Reached Probe	Displays the total number of triggered CIs that reached the Probe, and may have started running.	Displays the number of triggered CIs that successfully reached the Probe, and may have started running.	Displays the number of triggered CIs that successfully reached the Probe and have started running, but have warnings.	--

Progress Status	Total			
Completed	Displays the total number of triggered CIs that completed running (successfully or unsuccessfully).	Displays the number of triggered CIs that successfully completed running.	Displays the number of triggered CIs that successfully completed running, but have warnings.	Displays the number of triggered CIs that failed to complete running, did not reach the Probe, or were not picked up by the Probe for execution.
Total	Displays the total number of triggered CIs.	Displays the total number of successful triggered CIs.	Displays the total number of triggered CIs that were successful, but had warnings	Displays the total number of failed triggered CIs.

CI Count View

Clicking a link in the Triggered CIs view enables you to view the number of triggered CIs for each discovery job that have reached the selected stage of discovery and with the selected status.

Important Information	In the Discovery Modules/Jobs view, the CI Count job is displayed only when standing on a module which contains 2 or more jobs. If there is only one job in the module, clicking the triggered CI displays the CI Instances view.

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

UI Element (A-Z)	Description
	**Up one level.** Enables you to go back to the Triggered CIs view
	**Show triggered CIs.** Enables you to drill down to individual triggered CIs.
	**Refresh.** Refreshes the table.
	**Remove CI.** Deletes the selected CI. The CI is deleted from the specific job or activity job. **Available: Discovery Modules/Jobs** view only, when you select a module category and select a job.
	**Rerun Discovery.** Enables you to rerun the selected discovery jobs. The execution complies to the defined execution policy for the relevant discovery jobs.

UI Element (A-Z)	Description
	**Pause / Resume.** Enables you to pause/resume a selected job. **Note:** • When you pause an active job: ▪ triggers that are currently running continue to run until they are finished ▪ all the execution information is retained, including errors • Jobs are paused based on their defined job execution policies. For details, see "Job Execution Policies" on page 28. **Available: Discovery Modules/Jobs** view only
CI Count	Displays the number of triggered CI per job that have reached the selected stage of discovery and with the selected status.
Job Name	Displays the list of jobs that have reached the selected stage of discovery and with the selected status.

CI Instances View

Clicking a job in the **CI Count** view displays the triggered CIs for that discovery job.

UI Element (A-Z)	Description
	**Up one level.** Enables you to move up a level of information.
	**Refresh.** Refreshes the list of triggered CIs.
	**Add CI.** Opens the Choose CIs to Add dialog box, enabling you to add a newly-discovered CI to the triggered CI list. For details, see "Choose CIs to Add Dialog Box" on page 314. **Available: Discovery Modules/Jobs** view only
	**Remove CI.** Deletes the selected CI. The CI is deleted from the specific job or activity job. **Available: Discovery Modules/Jobs** view only

UI Element (A-Z)	Description
	**Filter CIs.** Enables you to filter the displayed CIs. • **By Status.** Available only when viewing the CIs of a particular discovery job in the Discovery Module/Jobs view. ▪ **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. Click to open 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.** Click to remove any filters.
	**Show Message.** When there are warnings/errors,opens a message box containing all the warning/error messages for the triggered CI.
	**Show additional data.** Opens the Discovered CIs dialog box, enabling you to view additional information about the CI. For details, see "Discovered/Created/Last Updated CIs Dialog Box" on page 316.

UI Element (A-Z)	Description
	**Show results for triggered CI.** An ad-hoc request is sent to the Data Flow Probe and retrieves the latest results of the job (CIT name and number of discovered CIs) that is running on a specific trigger CI. 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 327. If no communication log exists on the Probe, a message is displayed. You can choose to always create communication logs. For details, see "Adapter Configuration Tab" on page 144.
	**Rerun Discovery.** Enables you to rerun the discovery on the selected CI.
 / 	**Pause / Resume.** Enables you to pause/resume a selected discovery. **Note:** • When you pause an active job: ▪ triggers that are currently running continue to run until they are finished ▪ all the execution information is retained, including errors • Jobs are paused based on their defined job execution policies. For details, see "Job Execution Policies" on page 28. **Available: Discovery Modules/Jobs** view only
Look for 	To search for a specific Probe, related host, or related IP, enter part of its name in the box and click the  button.
<CI Instances table>	Displays all the CI instances discovered by selected job. You can drill down into any CI instance. If triggered CIs failed, or succeeded with warnings, you can drill down further to better understand the cause for the warning or failure.

UI Element (A-Z)	Description
<right-click menu>	In addition to some of the functionality described above, right-clicking a CI enables you to do the following: • **Debug.** Enables you to debug a CI. You can: ▪ View the Communication Log ▪ Go directly to the job's adapter ▪ Go directly to the job's details (Discovery Modules/Jobs view only) ▪ Select a script to edit • **Run from step.** Enables you to manually run the job on the selected CI from a particular step in the job's workflow. This is useful if you do not want to rerun the whole discovery job on the CI, but only a part of it. **Note:** ▪ The workflow steps are defined in the job's adapter file. You can view or edit the workflow in the Adapter Definition tab for the relevant adapter. For details, see "Adapter Definition Tab" on page 137 ▪ You cannot run the job from particular step if the status of the CI is **Waiting for probe** or **In Progress**. **Available:** In the Discovery Modules/Jobs view; For CIs that trigger workflow-based jobs • **Reprocess Scan File.** Reprocesses the scan files of the selected CI. **Available:** In the Discovery Modules/Jobs view; For CIs that trigger workflow-based jobs

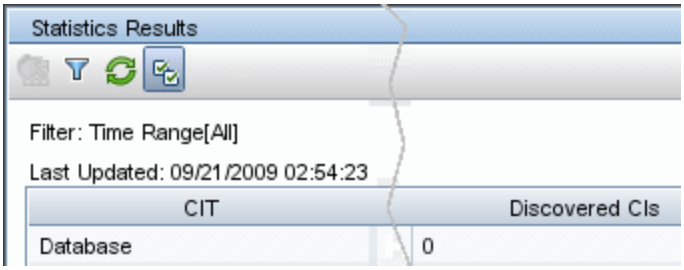
Discovery Results Tab/Pane

This tab/pane displays the discovery results from discovery job runs or from discovery activities that ran in Management Zones.

Important Information	UCMDB includes a purging mechanism for managing old discovery result statistics. This mechanism enables faster display of discovery result statuses. That is, the old result records are merged and 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 results (the interval for running the purging mechanism). • **appilog.collectors.DiscoveryStatisticsArchiveDays.name=Discovery results statistics archive period**. This property defines the number of days after which discovery results are archived (the number of days after which the statistics are considered old).

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

UI Element (A–Z)	Description
	**Refresh.** Retrieves the latest discovery results from the server (job results are not automatically updated in the **Results** pane).
	**View Instances.** Displays all new and updated CIs. Select a CIT and click: • **View Created Instances** to view CIs created during the discovery • **View Updated Instance** to view CIs updated during the discovery. **Note**: When you double-click a row, created CI instances are displayed. **Available:** When the discovery results include created or updated instances.
	Select the time range or Probe for which to display discovery results and statistics. • **By Time Range**: ▪ **All.** Displays results for all job runs. ▪ **From Now/Last Minute/Last Hour/Last Day/Last Week.** Choose a period of time for which to display results. ▪ **Custom Range.** Opens the **Change Timeframe** dialog box where you can enter the date or choose a **From** and **To** date and time from the calendar. Click **Now** to enter the current date and time. Click **Last Day** to enter the current date and time in the **To** box and yesterday's date and time in the **From** box. Click **OK** to save the changes. • **By Probe**: To view results by Probe, select to open the Choose Probe dialog box. Selecting All Data Flow Probes displays the results for all of the Data Flow Probes.

UI Element (A–Z)	Description
	**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: 
<Results grid>	Displays the discovery results and statistics. **Note:** Click a column heading to sort by that column. Right-click a column to select columns to display. • **CIT.** The name of the discovered CIT. You can configure discovery so that any object reported by the job and whose CIT is not defined in the adapter's **discovered CITs** list is marked in red. Objects include those added by the Probe result mechanism. **To set this parameter:** a. Select **Administration > Infrastructure Settings Manager**. b. Select the **General Settings** category. c. Locate the **Enable statistics results validation according to adapter** parameter. d. Change the value to **True**. • **Created.** The number of CIT instances created in the period selected or for the selected Probe. • **Deleted.** The number of CIT instances deleted in the period selected or for the selected Probe • **Discovered CIs.** The number of CIs that were discovered for each CI type. • **Total.** The total number of CIs in each column. • **Updated.** The number of CIT instances that were updated in the period selected.
Filter	The time range set with the **Set Time Range** button.
Last updated	The date and time that the Results grid was last updated.

Related CIs Window

Enables you to view, in map format, the CIs that are related to a selected CI.

To access	In the **Discovered CIs** dialog box, right-click a CIT and select **Get Related CIs**.
Important Information	Related CIs are CIs that are the parent, child, or sibling of an existing CI.

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 *HP Universal CMDB 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 Progress > Drill down to the CI Instances, right-click a CI, and choose **Show Results for Triggered CI**.

User interface elements are described below:

UI Element (A-Z)	Description
	Select a CIT and click to display additional information in the **Show Results for Triggered CI** dialog box.
	Click to open a topology map showing a result map for the Triggered CI. Right-click a CIT to view its properties.

Chapter 13

Inventory Discovery

This chapter includes:

Inventory Discovery Overview

Universal Discovery determines which devices are in your network and gathers basic information about each of them. This process allows you to get a good overview of the number and types of devices in your network, as well as a basic set of attributes for each. It also serves as the foundation for the other modules of discovery.

Discovery can be based on Management Zones. Universal Discovery can use a variety of methods to discover devices, and provides out-of-the-box discovery activity wizards that allow you to choose the appropriate settings for your different Management Zones. For example, UNIX servers in the Data Center may have different requirements for discovery than laptops in the Finance group.

After discovering a device, Universal Discovery runs a Scanner on the device to gather detailed hardware, configuration and software license information. This process is referred to as Inventory Discovery and makes it possible to drive standardization and compliance initiatives, manage risk, implement chargeback policies, and so on.

The Scanners can be launched automatically according to a configurable schedule, allowing complete control over network bandwidth usage and any impact on the end-user.

To automatically manage the Scanners, the Universal Discovery (UD) Agent needs to be in place. This is a small component deployed on the discovered device that enables secure communication with the Data Flow Probe. The UD Agent can be automatically deployed to Windows machines in your network, and must be manually deployed to UNIX machines. Once this is done, Universal Discovery can automatically upgrade the Scanners and agents when necessary.

Universal Discovery includes Agents and Scanners for most common desktop and server operating systems.

The Scanner can also be installed manually. This is known as agentless inventory discovery.

Universal Discovery can also gather information about what software is used on the machines on your network. This is referred to as Software Utilization and the information collected is necessary to optimize software license cost, for example by eliminating unused or under-utilized software installations.

For details on setting up the Inventory discovery and other activities, see the *HP Universal CMDB Discovery and Integration Content Guide*.

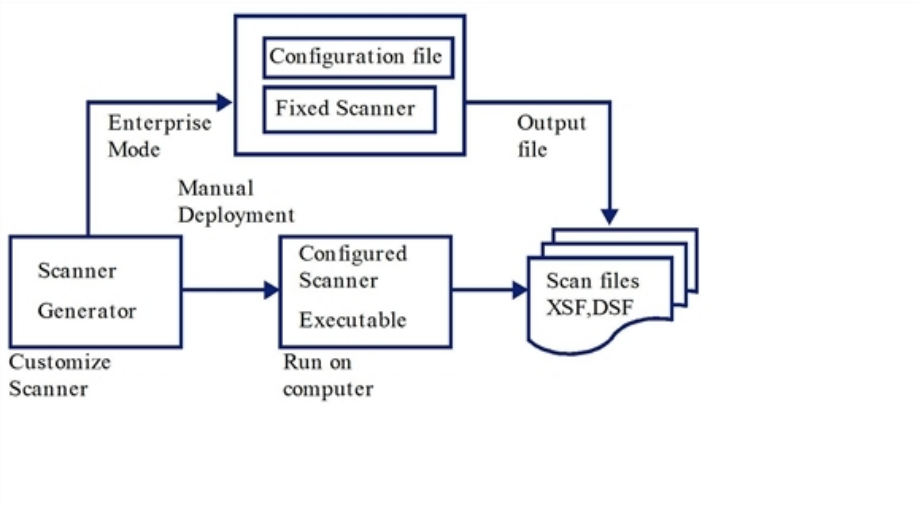
Scanner Generator

After defining requirements, the next step in an IT asset inventory is to collect data. This is accomplished by using the Scanner Generator to generate scanners and then by running the generated scanners.

The scanner is configured and generated in the Scanner Generator according to the specifications determined in the planning stage of the inventory. Then the scanner is run across the computer population to collect inventory data, either automatically using the scheduling mechanism (**Enterprise Mode**) or manually (**Manual Deployment Mode**).

- **Enterprise Mode.** This is the default option. Use this option to automatically collect an inventory using the scheduling and launching capabilities of Universal Discovery.
- **Manual Deployment Mode.** Use the **Manual Deployment Mode** option if Universal Discovery will not be used to schedule and launch scans. For example, choose this option if the scans will be launched from login scripts or on non-networked machines.

The Scanner Generator is used to both configure and define the level of information to be collected. One or more scanner executable programs with the desired configuration are then generated and subsequently run across a computer population.



Scanners can collect four different types of information and can be configured to collect any or all of them. See "Information Scanners Can Collect" on page 333. The details recorded for each computer within each main category depend on the options and settings selected when the scanner is generated and the configuration of the computer.

The Scanner Generator also provides a set of options for controlling the behavior of the scanner as it scans each computer, under both normal and exceptional conditions (such as when an error occurs).

Components of a Scanner

A scanner consists of the following files:

The scanner executable file	This file is an executable file. It contains the constant parts of the scanner: • strings • data files • the scanner executable code
The scanner configuration file	The configuration file is a compressed XML file containing the settings for the scanner you are currently configuring. When the scanners are used in Enterprise Mode, they read the configuration from a separate configuration file. This is a binary file with a **.cxz** extension. The typical size of the configuration file is about 3K. As the size of the configuration file is significantly smaller than the size of the complete scanner, a separate scanner configuration is useful for repetitive inventory collection when the configuration of the scanner has been altered. In this case, only a small configuration file is delivered to the user's computer to run with the original scanner instead of delivering the entire new scanner.

Note: When used in **Manual Deployment Mode**, the Scanner Generator generates self-contained scanner executables that consist of a combination of the scanner executable and configuration file.

Information Scanners Can Collect

Information Scanners can collect the following information:

Hardware and Configuration Information

Hardware information is detected automatically. The scanners collect and store from 100 to 900 hardware items for a computer, depending on the type and manageability options available on the computer.

The Scanner Generator allows a subset of the hardware collection to be disabled. Normally this is not required, but it may be desirable to decrease the scan file size or scan time.

The hardware details that can be defined and recorded by the scanner include the following:

- The processor type and BIOS details.
- The memory size and configuration details.
- The computer bus type and details of the attached cards.
- The hard disk drive specifications (including the total size and free space).
- The network type and ID (if applicable). This hardware item cannot be disabled in Enterprise Mode.
- Comprehensive detection of network settings, including detection of multiple network adapters, TCP/IP settings, gateways, DNS servers, subnet masks, DHCP status.
- The monitor and video display adapter details.
- The type of keyboard and mouse driver installed and details of the I/O ports.
- The Operating System version and other details.
- The expansion (or adapter) cards detected.
- The hardware data information from System Management BIOS (SMBIOS).

Note: For a comprehensive list of hardware data the scanner can collect, click the following link to access the file: DataCollectedByTheScanners.html.

Software Information

Software information is scanned automatically, and consists of detailed information about the files and directories on the drives scanned. The information collected about files can be defined (including the file types and the level of information collected). It is possible to define the drives that are to be scanned based on either the media or format of the drive, or to use the targeted scanning option to scan just a set of directories. Specific files can be collected (that is, stored in the scan file) for further analysis or for error recovery purposes. It is also possible to configure the level of file detail stored in the scan file and filters can be set up that specify directories or files to be included or excluded from being stored.

User or Asset Information

User or asset information consists of configurable fields that can be collected automatically. It usually includes the asset number which is used to uniquely identify each computer. Asset data

fields are automatically populated from the data extracted from text files, the Windows registry/WMI and environment variables.

Software Utilization

Universal Discovery can gather information about the software that is being used on the machines in your network. This is referred to as Software Utilization. The information collected can be used to optimize software license cost, for example by eliminating unused or under-utilized software installations.

From a software recognition perspective, any files that are Unknown and are shown to have a high Utilization should be marked for teaching.

Software utilization data shows the number of days that an application was used (as a percentage) over a period of time. This period of time is known as the **Utilization Period**.

As a guideline the Utilization Periods are as follows:

- Month (31 days)
- Quarter (90 days)
- Year (365 days)

Scanner Scheduler

The Scanner Scheduler enables you to determine when a scanner runs on a discovery node. Using this feature ensures uninterrupted scanning when connectivity or firewall issues prevent the Data Flow Probe from initiating scan jobs on discovery nodes.

Note: For optimal performance, also deploy the Store and Forward server. For more information on Store and Forward, see "Store and Forward" on page 342.

You can deploy the Scanner Scheduler manually using any remote access technology or third party distribution tool. The Scanner Scheduler runs as a service on Windows or as a detached process on UNIX.

You can centrally manage scanner schedules by using a configuration file that is stored on a remote server. The scanner, using a third party data transfer tool such as Curl, periodically downloads this remote file according to a download schedule that you configure. All updates that are contained in the remote file are applied to the local file.

To install the Scanner Scheduler, see "How to Install the Scanner Scheduler" on page 350.

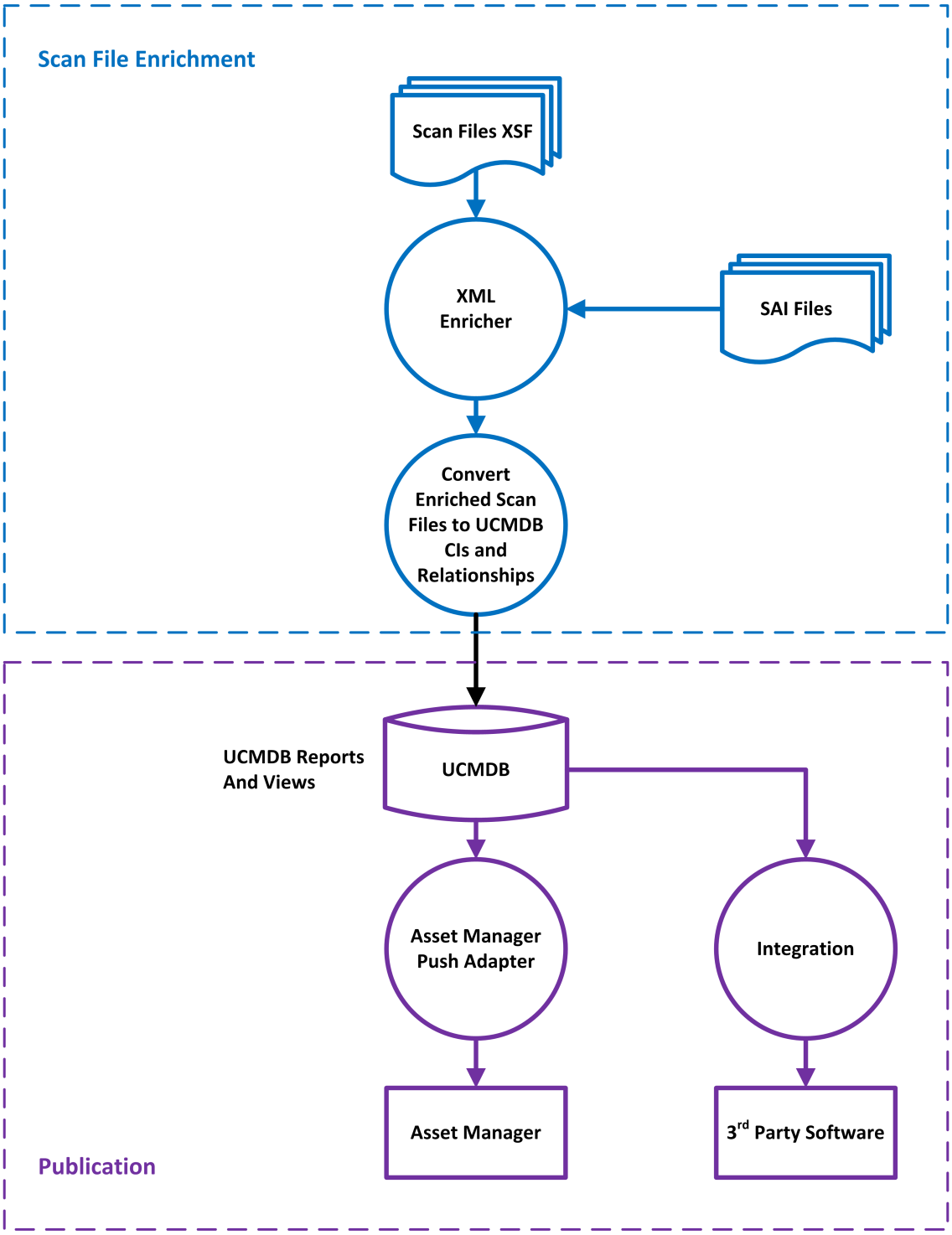
To see resources for the Scanner Scheduler, see "Scanner Scheduler Resources" on page 468.

XML Enricher

The XML Enricher is a process that runs in the background and automatically adds application data to scan files. This process is called **scan file enrichment**. It works as follows:

1. The XML Enricher looks for new scan files (xsf or dsf format) in the **Incoming** directory.
2. If a file is found, it processes the file using **SAI** (Software Application Index) application recognition.
3. Information about recognized applications is added to the file data and separate **<applicationdata>**, **<applicationusage>**, and **<users>** sections are added to the XML file.
4. Two types of enriched scan files are created:
   - In the **Processed** directory complete enriched files are stored. They contain the complete scan file information enriched with the application recognition and software utilization data. The Inventory tools (the Viewer, the Analysis Workbench, and the SAI Editor) can make use of the files in the Processed directory for analysis and application teaching. To prevent locking of the scan files in the Processed directory, and to reduce the load on the computer running the Data Flow Probe, it is recommended to copy these files to the Universal Discovery Administrator's desktop where Inventory Tools are installed.
   - In the **ProcessedCore** directory, the core enriched files are created. These files do not contain the information about stored files or file and directory data. Therefore, they are much smaller than the fully enriched files. The core enriched files are used internally by the InventoryDiscovery adapter to process the scan file information and convert it to the UCMDB CI and relationship data.

The XML Enricher can also be used to re-enrich scan files that were enriched previously. This can be useful after applying a significant update to the SAIs.



For information about setting up the Data Flow Probe to increase the processing power of the XML Enricher, see "How to Increase Scan File Processing Power" on page 353.

For information about setting up software recognition options, see "XML Enricher: Software Recognition Configuration Dialog Box" on page 447.

Processing Scan Files

Processing Normal Scan Files

At the end of the enrichment process, a new enriched scan file is created; the enriched core file is converted to UCMDB CI and relationship data, and reported to UCMDB. If delta scanning was enabled in the parameters for the Scanner used to produce the scan file, the incoming scan file is stored in the **Original** directory for future use by the delta scan processing. If delta scanning was disabled, the incoming scan file is deleted.

Tips

- If an error occurs, the original scan file is moved to a failure directory and is not deleted.
- If an enriched scan file for the same computer already exists, the old file is overwritten.

Reprocessing Normal Scan Files

Scan files can be reprocessed after they are enriched. For example, you may want to run this operation when you update the Software Application Index (SAI) file. Scan files for selected nodes are moved from the **Processed** folder to the **Incoming** folder. Then, the scan file is processed using the updated SAI file.

To reprocess normal scan files, see "How To Reprocess Scan Files" on page 357.

Processing Delta Scan Files

The delta scan file is used in conjunction with the previous version of the scan file located in the **Original** directory to reconstruct the new full version of the scan file. This full version is then moved into the **Incoming** directory, where it gets processed in the same way as other normal scan files.

At the end of the process, the reconstructed scan file is moved to the **Original** directory, ready for the next time a delta scan is found for this particular scan file instance.

For details handling delta scan files in Manual Deployment mode, see "How to Set up the Scanner to Handle Delta Scan Files in Manual Deployment Mode" on page 355.

Scan File Processing Power

Universal Discovery is configured, by default, to use one XML Enricher service to process and enrich incoming scan files.

When the scan files flow into the **incoming** directory of the XML Enricher faster than the XML Enricher is able to process them, a build-up of scan files occurs in the **incoming** directory. To allocate more processing power for enriching scan files, Universal Discovery can be configured to use two XML Enricher services.

Note: Running two XML Enricher services makes sense only if the computer on which Probe Manager is running has multiple physical CPUs or a single CPU with multiple cores. Although some benefit can be gained if a single processor system has hyper-threading supported and enabled, the real benefit can be seen on multi-core or multi-processor systems.

For details on how to configure the Data Flow Probe to use two XML Enricher services for scan file processing and enrichment, see "How to Increase Scan File Processing Power" on page 353.

Application Teaching

Application Teaching is a process to improve application recognition.

For more information, see the section that describes Application Teaching in the **Scan Data Analysis** document. You can view this document by clicking **Start** > **Programs** > **HP UCMDB** > **Inventory Tools**. Additionally, you can view more information about Application Teaching by clicking the **Help** menu option of the **SAI Editor** when it is installed on your Windows computer.

Note: This PDF document is available only if the Inventory Tools were installed on the computer. For more information on installing Inventory Tools, see the section that describes installing Data Flow Probes in the interactive *HP Universal CMDB Deployment Guide*.

Software Utilization

Universal Discovery can collect information about the software that is used on discovery nodes. The information that is collected can be used to optimize software license costs, for example, by eliminating unused or under-utilized software installations.

Software Utilization data shows the number of days that an application was used (as a percentage) over a period of time.

Universal Discovery includes a plug-in that collects Software Utilization data by monitoring the processes that are running on the discovery node. There is a separate file for each day, and there is a file that contains aggregated utilization information. When a discovery node is scanned, the Scanner collects a copy of the **discusg.cxu** file and stores its content in the scan file in a container called Software Utilization Data. Then, the **XML Enricher** extracts and processes the Software Utilization data.

Tip: From a software recognition perspective, any files that appear in the scan file that are unknown and have a high software utilization rate should be marked for teaching. For more information about Application Teaching, see "Application Teaching" above.

To see how to configure Software Utilization, see "How to Configure Software Utilization" on page 378.

To see platform-specific file location information for Software Utilization data files, see "Universal Discovery Agent File Locations" on page 110.

To see more information on how to view Software Utilization data by using Inventory Tools, see "Inventory Tools" on page 347.

To see more information on how Software Utilization data files are processed, see "Application Utilization Data" on page 342.

To see more information on how Software Utilization data is reported, see the section describing reports in the *HP Universal CMDB Modeling Guide*.

Hardware and Software Recognition

Recognition is the process of identifying certain properties and attributes of a hardware device or a software application by leveraging content that is supplied by Content Packs and by publisher data.

Hardware Recognition

- **Discovery Rules.** A database containing information on hardware that is available for sale by a wide range of manufacturers. The Discovery Rules Engine determines the device's operating system, application, device family, and model. Then, Discovery Rules assigns a device type to your device model.

This database is updated monthly and is included in Content Packs. For more information, see the Universal Discovery Community web site (https://hpln.hp.com/group/universal-discovery/).

To find more information about viewing Discovery Rules that are installed on your system, see "How to View Discovery Rules in JMX" on page 176.

Note: An HP Passport user name and password is required to log in to this site.

Software Recognition

- **Software Identification Tags.** Universal Discovery supports the ISO/IEC 19770-2 standard. A software identification tag is an XML file that contains identification information about a software product. The tag is installed on a discovery node together with the software product, and it uniquely identifies the software. When tags are captured by Scanners during discovery, the data can be leveraged for improved software asset management and compliance.

  The tag may be created as part of the installation process, or added later for software already installed without tags.

  Software identification tag files must have the **.swidtag** file extension in order to be recognized by Inventory Discovery tools. You can create installed package rules that can match the information found in the software ID tags.

  For more information, about viewing software identification tags, see "Inventory Tools" on page 347.

- **Software Application Index (SAI).** SAI files provided with the Content Pack contain information to identify applications on a discovery node. The library also contains license relationship information that allows Universal Discovery to identify how individual software products are related to a software product suite.

  SAI files can be exported from the **Administration** > **Package Manager**, then select **SAI**. For more information, see the section describing exporting resources using the Package Manager in the *HP Universal CMDB Administration Guide*.

  In addition to the standard libraries, Universal Discovery includes several tools that allow you to create your own library extensions in the form of one or more User SAI files that can be applied to the automatic Application Recognition process. For more information, see the section that describes the SAI Editor in "Inventory Tools" on page 347. For more information about teaching applications to improve the Application Recognition process, see "Application Teaching" on previous page.

The SAI contains information about applications in multiple languages for multiple platforms. SAI files are available as follows:

Windows	The following languages are available: ▪ English ▪ French ▪ German
UNIX	SAI files are available for the following variant systems: ▪ BaseUnix ▪ HP-UX ▪ AIX ▪ Solaris
Mac	Mac OS X

Hardware Mapping Configuration

This tool enables you to create custom mappings between captured data contained in scan files and an attribute of a CI in UCMDB.

By default, Universal Discovery maps a large subset of scan file data to UCMDB CIs and relationships, however, not all data is mapped. Moreover, if you create post-scan scripts to capture customized data, you need to create mappings for this data. For more information on post-scan scripts, see "Pre-Scan and Post-Scan Scripts" on page 136.

To create custom mappings, see "How to Map Scan File Attributes to UCMDB" on page 378.

Application Recognition in XML Enricher

The XML Enricher reads scan files and outputs enriched XML scan files containing all of the original data as well as data identified in the application recognition step.

Each file is stored as a <file> element. When a file is identified as belonging to an application, two attributes are added to the element:

- **versionid**
- **flag**

For example,

```
<file name="winword.exe" size="12345" versionid="1111" flag="M"/>
```

represents a file named **winword.exe** identified as belonging to the application with a version ID of 1111. The type of the file is "M", which means Main file. The possible values for the type field are:

flag	"type" tag in enriched XML file
Main	M

flag	"type" tag in enriched XML file
Associated	Y
3rd Party	3
Device Driver	A
Unknown	N

The **versionid** attribute refers to the unique ID associated with every version in the SAI library. In an enriched XML scan file, the **<applicationdata>** section contains a list of applications identified on the machine along with the version IDs.

For example:

```
<applicationdata>
<application version="6.0 sp1"
               release="6.0"
               name="Internet Explorer"
               desc="Microsoft Internet Explorer"
               publisher="Microsoft"
               language="English"
               os="Windows 98/NT/2K/ME/XP"
               type="Internet browser software"
               typeid="122252"
               maindir="C:\Program Files\Internet Explorer"
               lastUsed="2004-05-05 00:00:00"
               versionid="12790"
               releaseid="131"
               />

<application version="6.0 sp1"
               release="6.0" name="Outlook Express"
               publisher="Microsoft"
               language="English"
               os="Windows 98/NT/2K/ME/XP"
               type="Desktop communications software"
               typeid="105020"
               maindir="C:\Program Files\Outlook Express"
               lastUsed="2004-05-05 00:00:00"
               versionid="12792"
               releaseid="372"
               licencedby="12790"
               licencedbyrelease="131"
               />

</applicationdata>
```

The example above could be found for a machine with just two applications on it: Microsoft Internet Explorer and Microsoft Outlook Express. The **licencedby** attribute indicates that Microsoft Outlook

Express is licensed by Microsoft Internet Explorer. In other words, while both are licensable applications, this machine requires one license for Microsoft Internet Explorer; with this license, no separate Outlook Express license is required.

Application Utilization Data

Agent software utilization generates individual utilization files, one per day when it runs up to the maximum period for which utilization data is collected.

In addition, it also produces a summary file for the entire utilization period. This is an XML data file compressed using gzip, called **discusg.cxu**. (**CXU** means **Compressed XML Utilization**.) The XML is encoded using UTF-8 encoding. The inventory Scanner includes this file as a special stored file inside the scan file.

The XML Enricher does the following during its processing:

- Extracts and parses the XML data out of the stored file.
- Calculates the software utilization for each recognized application and adds this information to the enriched scan file.
- Adds a **Utilized** flag to the file attributes.

Store and Forward

Store and Forward is a system that enables you to design flexible,secure, and resilient communication paths to move scan files through firewalls or other networking obstacles. Store and Forward works together with Scanner Scheduler to maintain clear, uninterrupted paths between scanners and the Data Flow Probe. For more information on Scanner Scheduler, see "Scanner Scheduler" on page 334.

Each Store and Forward server uses a configuration file to determine its behavior. Depending on the parameter values contained in the configuration file, a Store and Forward server may forward or route scan files through logical "channels" that map to directories on one or more "upsteam provider" Store and Forward servers. The last Store and Forward server in the system is the Data Flow Probe. A web server that is installed together with the Store and Forward server continuously listens on a TCP port for incoming scan files. Store and Forward servers support resumed file transfer.Monitoring statistics for each Store and Forward server are available by accessing a web page that is hosted on each server.

To install the Store and Forward server, see "How to Install the Store and Forward Server" on page 357.

Software License Compliancy

Tracking and maintaining software licenses ensures that only the allowed number of licenses are in use, and that there are enough licenses for everyone using it. This is often used when limited license counts are available to avoid violating strict license controls.

To use this feature, select certain options in the **Scanner Generator**. For more information, see "Hardware Data Page" on page 388.

You can calculate your license compliancy position for the IBM and Oracle software packages.

This section includes:

IBM: Processor Value Unit

The processor value unit is a unit of measure used to differentiate licensing of IBM software on distributed processor technologies. The number of required licenses per processor is determined by multiplying the number of processor chips where IBM software is installed by the number of cores per chip. Then, the resulting value is multiplied by a processor value unit multiplier that IBM provides.

You can also see reports on PVU values if you configure adapters to push certain data to **Asset Manager**. For more information, see the section describing integrations in the *HP Universal CMDB Discovery and Integration Content Guide*.

Note: Only full capacity (non-virtualized) environments are supported.

Calculate the Processor Value Unit:

1. Locate the scan file data that you want to use for the calculation

   Open a scan file using **Viewer**. For more information, see "Inventory Tools" on page 347. Then, locate certain data in scan files to determine the vendor and processor technology.To do this, refer to the following table:

   Processor Attributes Mapping

Generic Name	Universal Discovery Field Name	UCMDB CI/Attribute Name
Processor Vendor	hwCPUVendor	CPU/CPU_Vendor
Processor Name	hwCPU_Type	CPU/CPU_Specifier
Server Model Number (required for IBM only)	hwBIOSMachineModel	Node/Discovered_Model
Maximum Number of Sockets per Server	hwPhysicalCPUCount	Calculate Raw Count of CPU CI Instances for Each Node.
Processor Model Number	hwCPUDescription	CPU/CPUType
Processor Type (Cores per Socket)	hwCPUCoreCount	CPU/Core_Number
	hwPhysicalCPUCount	Calculate Raw Count of CPU CI Instances for Each Node.

   Note:
   The values of the fields in the **Universal Discovery Field Name** column can be viewed by opening a scan file in the **Viewer**. The data is contained at **Hardware and Configuration** > **Hardware Data** > **CPU Data** > **CPUs** or **BIOS**.

The values of the fields in the **UCMDB CI/Attribute Name** column can be viewed at **UCMDB** > **Modeling** > **CI Type Manager**. For more information, see "CI Type Manager" on page 1 in the *HP Universal CMDB Modeling Guide*.

Use a search engine to map **Server Model Number** values in the **Universal Discovery** column or the **UCMDB CI/Attribute Name** column to the **Server Model Number** column in the IBM Processor Value Unit table. Enter the value into the search engine and perform basic analysis to derive the correct value.

The **Processor Model Number** value is contained in a long string. For example, the Processor Model Number value is "M540" in the string "Intel(R) Core (TM) i5 CPU M540 @ 2.53GHz". To find **Processor Model Numbers** locally on a discovery node, see more information at IBM Processor Model Number Discovery Guide.

To calculate **Processor Type (Cores per Socket)** using the corresponding field in the **Universal Discovery Field Name** column, use the following calculation:

[hwCPUCoreCount/hwPhysicalCPUCount]

If the value is equal to 1, the processor is a single (one) core processor type.

To calculate Processor Type (Cores per Socket) using the corresponding field in the **UCMDB CI/Attribute Name** column, use the following calculation:

[CPU/Core_Number]/Calculate Raw Count of CPU CI Instances for Each Node]

2. Find the processor value unit

   Go to the IBM PVU Licensing table to find the processor technology for which you want to calculate the processor value unit.Then, find the multiplier in the **PVUs Per Core** column.

   Note: Not all processor names are listed in the IBM PVU Licensing table.

Oracle: Processor Core Factor

The Processor Core Factor is a unit of measure used to differentiate licensing of Oracle software on distributed processor technologies. The number of required licenses per processor is determined by multiplying the number of processor chips where Oracle software is installed by the number of cores per chip. Then, the resulting value is multiplied by a core processing license factor that Oracle provides.

Note: Only full capacity, or non-virtualized environments are supported.

Calculate the Processor Core Factor as follows:

1. Locate the scan file data that you want to use for the calculation
   Open a scan file using **Viewer**. For more information, see "Inventory Tools" on page 347. Then, locate certain data in scan files to determine the processor and vendor. To do this, refer to the following table:

Processor Attributes Mapping

Generic Name	Universal Discovery Field Name	UCMDB CI/Attribute Name
Processor Name	hwCPUType	CPU/CPU_Specifier
CPU Speed	hwCPUSpeed	CPU/CPU_Clock_Speed
Core Count	hwCPUCoreCount	CPU/Core_Number
CPU Count	hwPhysicalCPUCount	CPU/Core_Number
Series Number	hwCPUFamily hwCPUModel	Not Mapped
Vendor	hwCPUVendor	CPU/CPU_Vendor
The DDMI fields are at the following location: **Viewer**>**Hardware and Configuration**>**Hardware Data**>**CPU Data**>**CPUs**.		
For details, see the section that describes UCMDB CIs and attributes in "CI Type Manager" on page 1 in the *HP Universal CMDB Modeling Guide*.		

2. Determine your processor type

   - The processor is a single core chip processor if the following calculation is true:

   [Core Count/CPU Count = 1]

   If your processor is a single core chip processor, skip to step 4.

   - The processor is a multi core chip processor if the following calculation is true:

   [Core Count/CPU Count > 1]

   If your processor is a multi core chip processor, than continue to step 3.

3. Find the multi core processor name and vendor name

   Find the row in the Formula column that contains attribute values that match the data that you found in step 1.

Formula	Multi Core Processor Name and Vendor Names
[hwCPUType = UltraSPARC-T1] and [hwCPUSpeed = (1000 or 1200)]	Sun and Fujitsu UltraSPARC T1 processor (1.0 or 1.2 GHz) Only named servers including: Sun Fire T1000 Server, SPARC Enterprise T1000 Server, with 6 or 8-core 1.0 GHz UltraSPARC T1 processor Sun Fire T2000 Server, SPARC Enterprise T2000 Server, with 4, 6, or 8-core 1.0 GHz, or 8 core 1.2 GHz UltraSPARC T1 processor **Note:** SPARC Enterprise T1000 and SPARC Enterprise T2000 Servers may be sold and branded by Oracle, Sun Microsystems, Fujitsu or Fujitsu Siemens.
[hwCPUType = UltraSPARC-T1] and [hwCPUSpeed = (1000 or 1200)]	Sun Netra T2000, 1.0 or 1.2 GHz UltraSPARC T1 processor
[hwCPUType = UltraSPARC-T3]	SPARC T3 processor
[hwCPUType = UltraSPARC-T1] and [hwCPUs.hwCPUSpeed = 1400]	Sun and Fujitsu UltraSPARC T1 1.4 GHz Only named servers including: Sun Fire T2000 Server and SPARC Enterprise T2000 Server, with 8-core,1.4 GHz UltraSPARC T1 processor
[hwCPUType = UltraSPARC-T1] and [hwCPUs.hwCPUSpeed = 1400]	Sun T6300, 1.4 GHz UltraSPARC T1 processor
[hwCPUType = UltraSPARC-T2+]	Sun UltraSPARC T2+
[hwCPUType = Fujitsu SPARC64 VI | Fujitsu SPARC64 VII]	Sun and Fujitsu SPARC64 VI, VII
[hwCPUType = UltraSPARC-IV+ | UltraSPARC-IV | UltraSPARC-IIIi | UltraSPARC-III+ | UltraSPARC-IIe | UltraSPARC-III | UltraSPARC-IIi | UltraSPARC-II | UltraSPARC]	Sun UltraSPARC IV, IV+, or earlier Multicore chips
[hwCPUType = UltraSPARC-T2]	Sun UltraSPARC T2
[hwCPUFamily<16] or [hwCPUFamily=16] and [hwCPUModel<=9]	AMD Opteron Models 13XX, 23XX, 24XX, 41XX, 61XX, 83XX, 84XX or earlier Multicore chips

Formula	Multi Core Processor Name and Vendor Names
[hwCPUVendor = (GenuineIntel | AuthenticAMD)] and [hwCPUType= (Xeon | Opteron)]	Intel or AMD Desktop, Laptop/Notebook, or Netbook Multicore chips
[hwCPUFamily=15] or [hwCPUFamily=6]and [hwCPUModel<=47)]	Intel Xeon Series 56XX, Series 65XX, Series 75XX, Series E7-28XX, Series E7-48XX, Series E7-88XX or earlier Multicore chips
[hwCPUType = Itanium 9300 Series]	Intel Itanium Series 93XX or earlier Multicore chips (For servers purchased prior to Dec 1st, 2010)
[hwCPUType = Itanium 9300 Series]	Intel Itanium Series 93XX_ (For servers purchased on or after Dec 1st, 2010)
[hwCPUType = HP PA-Unknown | HP PA-RISC 2.0 | HP PA-RISC 1.2 | HP PA-RISC 1.1 | HP PA-RISC 1.0]	HP PA-RISC
[hwCPUType = Power5]	IBM POWER5+ or earlier Multicore chips
[hwCPUType = Power6]	IBM POWER6
[hwCPUType = Power7]	IBM POWER7
Not Supported	IBM System z (z10 and earlier)

4. Find the Processor Core Factor

   When you have determined the correct processor for which you want to calculate the core processing license factor, go to Oracle Processor Core Factor to find the current factor multiplier for that processor.

Inventory Tools

The Inventory Tools enable you to view and analyze scan file data.

Note: These tools are installed using the Data Flow Probe Installer program. They are installed together with the Data Flow Probe. However, it is recommended to install them on a separate computer to prevent performance degradation on the Data Flow Probe, and also to prevent data corruption of the SAI files.

To install them separately, run the Data Flow Probe Installer program and select the **Inventory Tools** type installation. For details about supported platforms, see the *HP Universal CMDB Support Matrix* document.

To start the tools (on Windows), click **Start** > **Programs** > **HP UCMDB** > **Inventory Tools**.

When the Inventory Tools are installed on your Windows computer,you can view the help documentation for the tools by clicking the **Help** menu option of the Inventory Tool. Users of all platforms that have Adobe Reader installed on the computer can also view the help documentation by clicking **Start** > **Programs** > **HP UCMDB** > **Inventory Tools**.

Software Application Index (SAI) Editor

View Software Application Index (SAI) file data, and perform additional tasks as follows:

- View and edit a collection of SAI files
- Create new User SAIs
- Move and copy items between SAIs (you can only edit User SAIs), and delete items
- Export the contents of an SAI to XML format
- Display license relationships
- Add and edit existing license relationships

Viewer

Displays software, hardware and asset information that is collected for an individual computer as follows:

- Details of all software scanned, presented in an explorer style view
- User entered asset information
- Detailed and summarized hardware and configuration information
- The contents of key files collected during Inventory Discovery, such as system configuration files
- Details of all logical drives
- Details of all recognized applications and their utilization statistics
- Detailed comparison of two scan files

Analysis Workbench

Perform analysis tasks using three types of information as follows:

- Software files that are recognized as belonging to a particular application
- Unidentified software and files that may belong to unrecognized applications
- Hardware and asset data

  Analysis Workbench uses the Software Application Index (SAI) that contains application and version descriptions to identify the files found during Inventory Discovery. Scan results are checked against the SAI to identify and recognize software. Any unrecognized files can be marked for further investigation, and when identified, their details can be added to the SAI file so they will be correctly identified in the future. For more information on Application Teaching, see "Application Teaching" on page 338.

How to Install the Scanner Manually

This task describes how to configure and deploy scanners manually for inventory discovery.

This task includes the following steps:

1. Prerequisites
   - A Data Flow Probe is installed.
   - A Management Zone is defined.
2. Configure the scanners

   Prepare resources to distribute to discovery nodes.

   a. Generate a scanner using the **Scanner Generator**. For more information, see "Scanner Generator Wizard" on page 384.

   b. In the **Scanner Generator**, select **manual** mode.

   Note: During installation if you plan to override certain configurations that you set in the **Scanner Generator**, ensure that you select the "**Allow Scanner Command Line to Override**" check box in the "Software Data Page" on page 394.

   If you do not select the **Offsite Scan File** check box, you can manually copy the scan files to the Data Flow Probe at the following location:

   `C:\hp\UCMDB\DataFlowProbe\runtime\xmlenricher\Scans\incoming`
3. Distribute the scanners

   Connect to discovery nodes using any remote access technology to copy the scanner executable file to the discovery nodes
4. Run the scanners

   There are two methods to run scanners as follows:

   - **Attended**

     Click the executable file. To see a list of default file names, see "Scanners Tab" on page 441.
   - **Unattended**

     Connect to the discovery nodes using any remote access technology, third party solution, or scripting solution and then run the scanner executable file. To see a list of default file names, see "Scanners Tab" on page 441. You can pass command line parameters to the discovery node shell to override any configurations that were used in the Scanner Generator. For more information about scanner command line options, see "Scanner Command Line Parameters and Switches" on page 453.
5. Save the scan files to the Data Flow Probe

There are two methods to save the scan file to the Data Flow Probe as follows:

- Run the **Inventory Discovery** activity. For more information, see the *HP Universal CMDB Discovery and Integration Content Guide*.

or

- Run the **Inventory Discovery by Manual Scanner Deployment** job. For more information, see "How to Manually Activate Modules/Jobs/CIs" on page 277.

6. Results

   The results depend on the method that you chose in step 5.

   - **Inventory Discovery** activity

     To verify that the activity ran successfully, click the activity and view the results summary in the **Discovery Status > Progress** tab. For more information, see "Discovery Progress Dialog Box" on page 318.

   - **Inventory Discovery by Manual Scanner Deployment** job
     - The scanner is saved to the location specified in the Scanner Generator. The scan files are saved according to the configurations specified in the Scanner Generator.
     - You can verify that the scan files are processed at the following location:

       C:\hp\UCMDB\DataFlowProbe\runtime\xmlenricher\Scans\processed

How to Install the Scanner Scheduler

This task describes a recommended workflow for installing the Scanner Scheduler.

This task includes the following steps:

1. Prerequisites

   UCMDB is installed.

2. Copy the installer package for the Scanner Scheduler or resources to the discovery node

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

   Windows:

a. From the UCMDB installation media, copy the MSI installer package to your local computer.

b. Copy the MSI file to the discovery node using any manual method or remote access technology.

UNIX:

From the UCMDB installation media, copy the file that is appropriate to your discovery node platform to your local computer. Additionally, copy the **scannerschedulerinstall** installation script file.

> **Tip:** The file name of the resources file indicates the platform.

3. Install the Scanner Scheduler

Windows:

a. For attended installations, double-click or execute the MSI file. For unattended, or silent installations, run the following command: **msiexec /quiet /I <MSIFilename>**

> **Note:**
> To debug the installation, use the following command: /L*v <FullPathToLogFile>. Log files are stored in the same location as scan files. For more information on scan file locations, see "Saving Tab" on page 420.

UNIX:

Run the following command with root privileges: **scannerschedulerinstall hp-ud-scanner-scheduler-<platform>-10.01.000<buildnumber>.<packageformat>**

4. Customize the running schedules and download schedules

a. Customize the **config.ini** file to create your configuration file download schedule and your Scanner Scheduler running schedule. For more information, see "Scanner Scheduler Resources" on page 468.

b. If you want to update config.ini files using a remote server, configure the Curl program to download the **config.ini** file from a remote server. For more information on Curl, see "Scanner Scheduler Resources" on page 468.

5. Results

- The Scanner Scheduler starts automatically when the discovery node is started.
  - For Windows, the name of the service is **ovedScannerScheduler**.
  - For UNIX, the name of the service is **discscannerscheduler**.
- The scanner runs according to the parameter values that are used in the **config.ini** file.

Additionally, the following operations are available:

- To uninstall the Scanner Scheduler, use the **uninstall** parameter. For example, **scannerschedulerinstall --uninstall**

- To upgrade the Scanner Scheduler, use the **upgrade** parameter and specify the file name. For example,**scannerschedulerinstall --upgrade hp-ud-scanner-scheduler-<platform>-10.01.000<buildnumber>.<packageformat>**

For more information on Scanner Scheduler concepts, see "Scanner Scheduler" on page 334.

For more information on Scanner Scheduler operations and resources, see "Scanner Scheduler Resources" on page 468.

How to Edit Pre- and Post-Scan Scripts

This task describes how to edit pre and post scan scripts in your Management Zones.

This task includes the following steps:

- "Prerequisites" below
- "Navigate to the script editor" below
- "Edit the script" below
- "Deploy the scripts" on next page
- "Results" on next page

1. Prerequisites
   - A Data Flow Probe is installed.
   - A Management Zone is defined.
2. Navigate to the script editor

   You can access the Pre/Post Scan Script Editor using the following ways:
   - In the Management Zone:
     i. Set up and activate the **Inventory Discovery Activity**.
     ii. On the Preferences Page, click to select **Scanner based Inventory Discovery** and then click **Edit script**. The Pre/Post Scan Script Editor opens.
   - From the Adapter Management module:

     Inventory Discovery > **Adapters**, click **Inventory Discovery by Scanner**, expand the Global Configuration Files pane, click the **PrePostScanScriptingConfiguration** file, and then click **Edit**  .
3. Edit the script
   a. Click the platform for which you want to edit a script. Depending on the platform, you might also need to select a version.

      Tip: Click **All UNIX** to create a script that is used as a backup script in the case that a script for any of the other UNIX variant scripts fails to run.

   b. Click **pre scan script** or **post scan script**. The script editing window opens.

c. Write your script using shell commands that are appropriate for the platform or shell that is running on the discovery node.

4. Deploy the scripts

   To deploy and run the scripts, click to select **Run Pre/Post Scripts** on the Preferences Page of the **Inventory Discovery Activity**.

5. Results

   To verify the script is deployed successfully, verify the script file is stored in the same directory as the scanner executable. For more information on the location of the scanner executable, see the section describing scanner file locations in the *HP Universal CMDB Discovery and Integration Content Guide*.

How to Increase Scan File Processing Power

This task describes how to configure the Data Flow Probe to use two XML Enricher services so as to increase the power for processing and enriching scan files in the **incoming** directory of the XML Enricher.

To learn more about the processing power of the XML Enricher, see "Scan File Processing Power" on page 337.

The following methods can be used to increase scan file processing power:

To configure the Data Flow Probe to use two XML Enricher services using the JMX Console: (Recommended)

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

   Enter a user name and password if prompted.

   > **Note:** If you have not created a user account, log in using the default user name **sysadmin** and the password **sysadmin**.

2. Click the **XmlEnricherMonitor** Mbean link.
3. Locate the **activateSecondaryXmlEnricher** parameter and ensure that **activated = true**.
4. Under the **Start** process, click **Invoke** to start the secondary XML Enricher service.

   > **Note:** By default, **activated = true** whether or not the **Start** process was invoked.

5. (Optional) To verify that the secondary XML Enricher service is running, under the**ViewXMLEnricherStatuses** process, click **Invoke**.

To configure the Data Flow Probe to use two XML Enricher services from the DataFlowProbe.properties file: (Requires restarting the Data Flow Probe)

1. Under the **Probe Manager Configurations > Xml Enricher** parameters, locate the following parameter:

com.hp.ucmdb.discovery.probe.agents.probemgr.xmlenricher.activateSecondaryXmlEnricher

Then enter one of the following values:

false	Enables one XML Enricher service
true	Enables two XML Enricher services

2. Restart the Data Flow Probe.

How to Set up the Scanner to Handle Delta Scan Files in Manual Deployment Mode

When conducting an inventory in Manual Deployment mode, for the delta scan file processing in the XML Enricher to work correctly, ensure you do the following:

1. **Configure the Scanner to save results to the XML Enricher Incoming directory.**

   This is done using the **Save result to network (off-site)** option on the **Scanner Generator > Scanner Options>Saving** tab page.

   - By default, the Data Flow Probe shares the Incoming and Original directories via HTTP.
   - The Data Flow Probe can be configured to share these directories via HTTPS instead. The following entries in the **DataFlowProbe.properties** file control the HTTPS behaviour:
     - **jettyHttpsEnabled** = false
     - **jettyHttpsPort** = 8453

     By default this property file is located in the following location:

     - **C:\hp\UCMDB\DataFlowProbe\conf\DataFlowProbe.properties** and HTTPS support is disabled. In order to enable it, the file needs to be modified to set

       jettyHttpsEnabled = true

       The default HTTPS port is 8453. It can be changed by modifying the **jettyHttpsPort** setting.
   - Depending on whether HTTP or HTTPS is used for off-site scan file saving, the off-site scan path that is configured in the Scanner Generator should be as follows:
     - HTTP: **http://DataFlowProbeHost:1977/incoming**
     - HTTPS: **https://DataFlowProbeHost:8453/incoming**

       where:

       - **1977** is the default Probe Manager JMX port. If the Probe Manager JMX was configured to use a different port, 1977 in the URL above needs to be replace with the corresponding probe manager port.
       - **8453** is the default HTTPS port. If a different port is used (as described earlier), 8453 in the URL above needs to be replaced with the corresponding HTTPS port.
       - **DataFlowProbeHost** is the host name or the IP address of the Data Flow Probe computer.
   - When the Data Flow Probe is installed, user credentials are provided for uploading scan files to the Data Flow Probe. These credentials are stored in the **DataFlowProbe.properties** file on the Data Flow Probe. (**C:\hp\UCMDB\DataFlowProbe\conf\DataFlowProbe.properties**)

     To change the user name:

In the **DataFlowProbe.properties** file locate **com.hp.ucmdb.discovery.Probe.JMX.UploadAuth.User** and replace the value with the new user name.

To change the password:

i. 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 Web browser 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 sysadmin and the password sysadmin to log in.

ii. Search for **type=mainProbe**, and click the link.

iii. Click **getEncryptedKeyPassword**, enter a new password, and click **Invoke**.

iv. Copy the generated value to the Clipboard.

v. In the **DataFlowProbe.properties** file locate **com.hp.ucmdb.discovery.Probe.JMX.UploadAuth.Pwd** and paste the new encrypted password over the old value.

> **Note:** You can also use the command line option -p:<path> with the Scanner to override the selection made in the Scanner Generator.

2. **Set the separate refilling path to the Original directory.**

Depending on whether HTTP or HTTPS is used for off-site scan file saving, the path should be as follows:

- HTTP: **http://DataFlowProbeHost:1977/original**
- HTTPS: **https://DataFlowProbeHost:8453/original**

The special user **UploadScanFile** with the corresponding password should be configured for the original directory.

For details, see **Enable Delta Scanning** in the Scanner Generator documentation.

> **Note:**
>
> - You can also use the Scanner `-r:<path>` command line option to specify the location of this directory.
> - In addition to the default HTTP/HTTPS options, it is possible to configure manual deployment Scanners to store the off-site scan files using the following:
>   - **File Share**
>   This is usually only suitable for Windows platforms. The Incoming and Original directories of the XML Enricher can be shared via Windows shares. For example: **Incoming$** and **Original$**, then the off-site scan file path and the original scan path in the Scanner Generator can be configured as the following UNC paths:

\\DataFlowProbeHost\Incoming$** and **\\DataFlowProbeHost\Original$. Make sure that these shares/NTFS permissions on these directories allow appropriate access to all users, under the user's account through which the manual deployment Scanners are to be executed.

- **FTP/FTPS**
  The Incoming and Original directories of the XML Enricher can be shared via FTP/FTPS protocols. The Data Flow Probe does not include an FTP/FTPS server, but either a standard Windows FTP server supplied with IIS can be installed or enabled, or a suitable 3rd party server can be installed for this purpose.

  The FTP/FTPS URLs must be configured for off-site scan saving. For example: **ftp://DataFlowProbeHost/incoming** and **ftp://DataFlowProbeHost/original**.

How To Reprocess Scan Files

This task describes how to reprocess scan files.

1. Right-click a **Node CI** or any of its subtypes.
2. Select **Actions** > **Reprocess Scan File**. The scan file is moved from the **Processed** folder to the **Incoming** folder and then reprocessed.

For more information about reprocessing scan files, see "Processing Scan Files" on page 337.

How to Install the Store and Forward Server

This task describes how to install the Store and Forward server. Perform this task for each computer that you want to use as a Store and Forward server.

This task includes the following steps:

1. Prerequisites
   - Scanners are deployed in Manual Deployment mode.
   - Scanners are configured to save scan files offsite. For more information, see "Saving Tab" on page 420.
2. Copy the installation package

> **Note:** Ensure that you copy installation files that are appropriate to the platform of the computer that you want to install the Store and Forward server.

Windows:

From the UCMDB installation DVD, copy the **HP Universal Discovery Store and Forward Server (x86) 10.01.xxx.msi** installation file to the computer that you want to install the Store and Forward server.

Linux:

From the UCMDB installation DVD, copy the **hp-ud-store-and-forward-linux-x86-10.01.000.xxx.tar** installation file to the computer where you want to install the Store and Forward server.

3. Install the Store and Forward server

   Windows:

   a. Double-click the MSI file. The main page of the installation wizard displays.

   b. Navigate through the wizard. For more information about the wizard, see "Store and Forward Installation Wizard " on page 451.

   Linux:

   a. Run the following command to decompress the archive file: **tar -xzf <FileName>.tar.gz**

   b. Run the following command to switch to root user if not logged in as root already: **su root**

   c. Run the following commands with root privileges to configure parameter values: **./configure**

   > **Note:**
   > The installation directory must be the current directory when you run this command.

   d. Enter the following information when prompted:
      i. The TCP port that you want to use for the Store and Forward server service. The default is **5005**.
      ii. The username that you want to use to authenticate to the web server that is hosting the Store and Forward status page. The default is **hpud**.
      iii. The password that you want to use together with the username to authenticate to the web server that is hosting the Store and Forward status page. This field is mandatory.
      iv. The communication protocol that you want to use between Store and Forward servers. Enter **1** for HTTP (plain) or **2** for HTTPS (secure).

   e. Start the service by running the following command with root privileges: **/etc/init.d/hpudsaf start**

4. Copy certificate files from upstream servers

> **Note:** This step is only applicable if the HTTPS (secure) communication protocol is used.

a. Copy the **server.crt** files of each upstream server to the computer that you are installing the Store and Forward server. An upstream server is a server that you are forwarding scan files to. This file is stored in the **<DataDir>\Cert** directory. For Windows, **<DataDir>** is configured in"Install the Store and Forward server" on previous page. For Linux, **<DataDir>** is the **data** folder in the directory where you installed the Store and Forward server in "Install the Store and Forward server" on previous page.

b. Rename each upstream server certificate file so that all files have unique names. For example, **server1.crt**, **server2.crt**.

c. Concatenate all the certificate files from upstream servers into one file. Separate each upstream server file with plus (+) signs. To do this, run the following command with root privileges: **copy /b <server1.crt> + <server2.crt> + <server3.crt> trustedcerts.crt**. A file named **trustedcerts.crt** is created.

d. Copy the **trustedcerts.crt** file to the **<DataDir>\Cert** directory of the computer that you are installing the Store and Forward server.

> **Note:**
> If the host name of any upstream server changes, perform this step again.

5. Configure the system behavior

   Update the **config.ini** file to control the behavior of the Store and Forward server.

   - The **config.ini** file is contained in the following location:
     - **Windows:** The **conf** folder that is contained in the directory where you installed the Store and Forward server.
     - **Linux:** The **conf** folder that is contained in the directory where you installed the Store and Forward server.

   To see parameters that are available to update, see "Store and Forward Resources" on page 471.

   > **Note:** If you make changes to the configuration file, restart the Store and Forward server. For more information, see "Results" below.

6. Results

   - The Store and Forward server service and the Apache web server service start automatically when the computer is started. For more information on names of services, see "Store and Forward Resources" on page 471.
   - To verify the system is operating as expected, go to the following web page on each Store and Forward server to view operating statistics:
     http://<StoreAndForwardServer>:<port>/server_status.xml

     > **Note:** If the HTTPS communication protocol is used, type **HTTPS** instead of **HTTP**.

The following operation is also available:

- To throttle the upload bandwidth, perform the following:
  i. Locate the **http.conf** file in the installation folder where you installed the program files.
  ii. Locate the following line: **safbwInputLimit 0**
  iii. Change **0** to any non-zero integer to specify the maximum bandwidth (in kilobytes).

For more information on Store and Forward concepts, see "Store and Forward" on page 342.

For more information on Store and Forward operations and resources, see "Store and Forward Resources" on page 471.

For more information on Store and Forward commands, see "Store and Forward Commands" on page 470.

How to Set Up an Asset Field

The Scanner Generator provides several predefined standard field types that indicate to which hardware field the asset field is mapped.

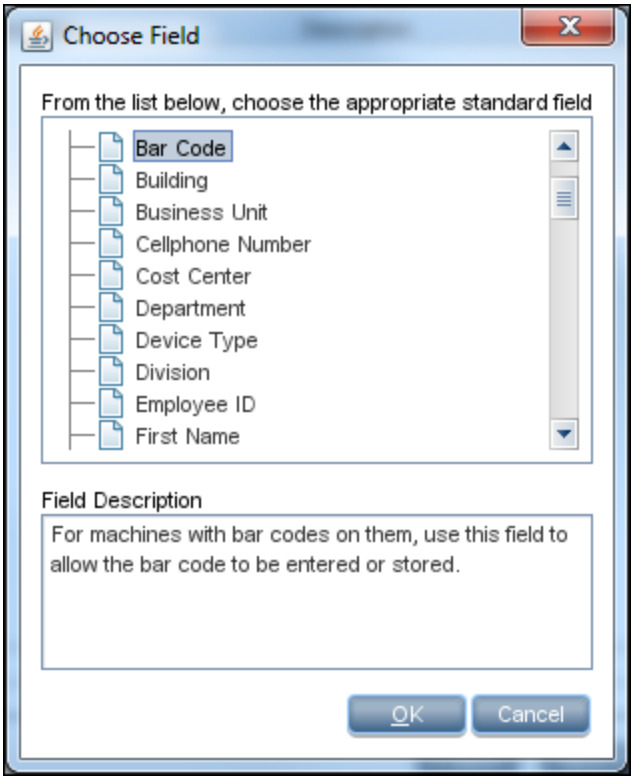
There are two special standard fields that you need to understand before proceeding with this task.

Description Field	The **Description** field is represented by the icon and can be configured to contain a brief description of the computer. This field by default is configured to be of type Combination. It combines information from several hardware and asset fields. When loading data from scans into the analysis tools (Analysis Workbench and Viewer), the contents of the description field are displayed for each scan file to help identify them.
Asset Tag Field	The **Asset Tag** field is represented by the icon. It contains a unique identifier for the machine. It is normally populated from a sequence of hardware fields such as MAC Address, Serial Number or Asset tag. The asset number entered in this field is used to name the off-site scan file. If you have not configured an asset tag field and the **Asset Number Source** is set to **Asset Field**, you will not be allowed to proceed to the next page and a warning will appear.

Note: It is strongly recommended that **Description** and **Asset Tag** fields are included in your list of asset fields.

How to Set Up a New Asset Field

1. In the **Asset Data** tab, click the button. The **Choose Field** dialog box is displayed, showing all standard fields not currently in use.



2. Choose a new standard field from the list.

   A number of standard fields are available as shown in the following table:

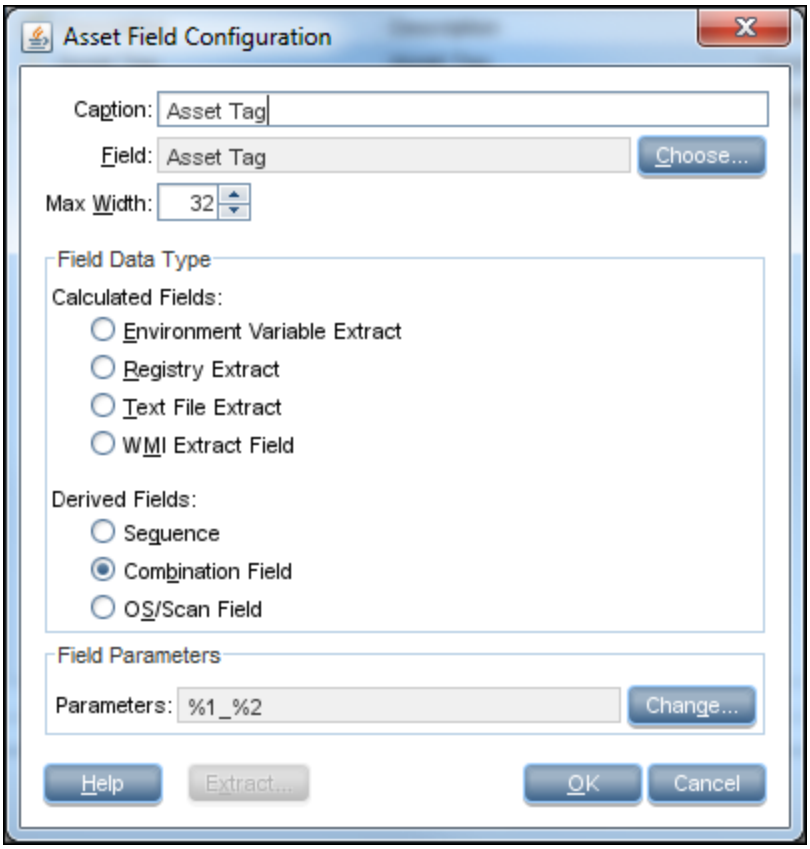
Field	Description	Hardware Field in Scan File
Asset Tag	The Asset Tag field contains a unique identifier for the machine.	hwAssetTag
Automatic Asset Fields	These asset data fields can be automatically populated from data extracted from text files, the Windows registry/WMI or environment variables. You can configure up to 56 automatic fields, which can then be used in the calculation of derived or calculated fields.	hwAssetAutomatic1..56
Bar Code	For machines with bar codes on them, use this field to allow the bar code to be entered or stored	hwAssetBarCode
Building	Identified the building containing the machine	hwAssetBuilding

Field	Description	Hardware Field in Scan File
Business Unit	Name of business unit	hwAssetBusinessUnit
Cellphone Number	Cell/Mobile phone number of user.	hwAssetCellphoneNumber
Cost Center	Cost center description or code	hwAssetCostCenter
Department	Department description or code	hwAssetDepartment
Device Type	Device type of the machine (Server, Notebook, Tower and so on)	hwAssetDeviceType
Division	Division description or code	hwAssetDivision
Employee ID	Employee ID as used in the organization.	hwAssetEmployeeID
First Name	First name of user	hwAssetUserFirstName
Floor	The floor on which the machine is located	hwAssetFloor
Full Name	Full name of user	hwAssetFullName
Job Title	Job title of user	hwAssetUserJobTitle
Last Name	Last name of user	hwAssetUserLastName
Machine Make	Make or Manufacturer of the machine	hwAssetMachineMake
Machine Model	Model of the machine. This data can be populated from SMBIOS using a Sequence Field on machines supporting SMBIOS.	hwAssetMachineModel
Office Location	Location of the office - normally a combination of country and city	hwAssetOfficeLocation
Printer Asset Tag	Asset tag of a local printer attached to the machine, if any	hwAssetPrinterAssetTag
Printer Description	Contains a description of a local printer attached to the machine, if any	hwAssetPrinterDescription
Room	Description, name or number of the room containing the machine	hwAssetRoom
Section	Section description or code	hwAssetSection

Field	Description	Hardware Field in Scan File
Telephone Extension	Internal telephone extension	hwAssetTelephoneExtension
Telephone Number	Full direct telephone number of user	hwAssetTelephoneNumber
User Field	These are user-defined fields. You can configure up to 30 User fields.	hwAssetUserField1..30

3. Select a field and click **OK**. The field is displayed in the **Asset Data** form.

4. Ensure the field is selected and click the button. The **Asset Field Configuration** dialog box is displayed.



5. Complete the following Asset Field configuration steps:

   a. "Caption"

   b. "Maximum Number of Characters for Field"

   c. "Field Data Type"

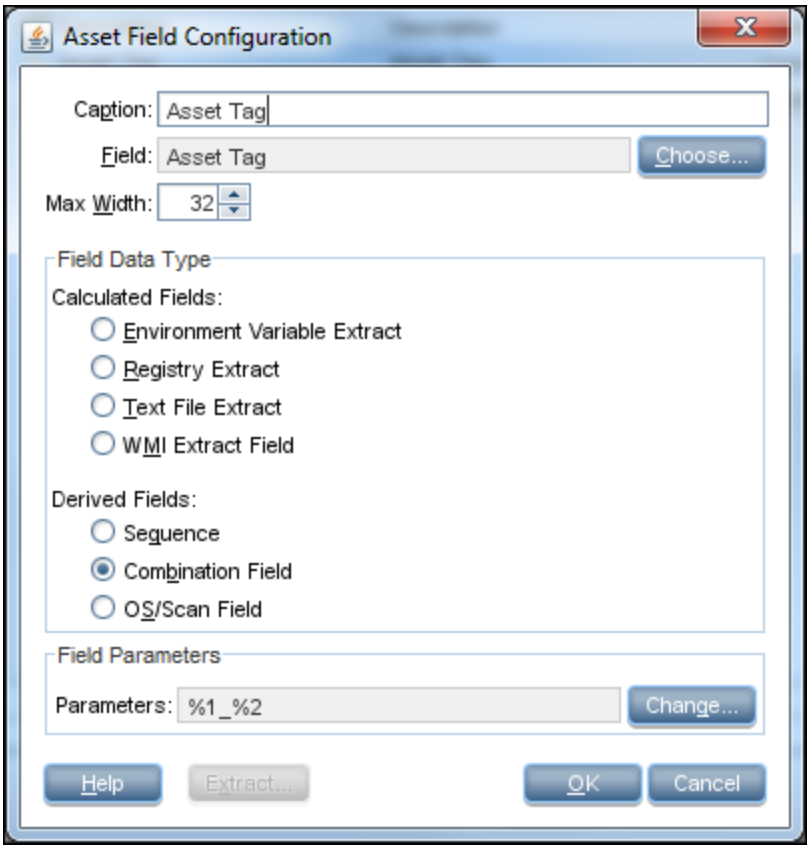
   d. "Setting Field Parameters"

e. "Setting Extract Options"

f. "Order of the Fields in the Form"

How to Edit an Existing Asset Field

1. In the **Asset Data** tab, ensure the field is selected and click the button. The **Asset Field Configuration** dialog box is displayed.



2. Edit the required Asset Field configuration items:

a. "Caption"

b. "Maximum Number of Characters for Field"

c. "Field Data Type"

d. "Setting Field Parameters"

e. "Setting Extract Options"

f. "Order of the Fields in the Form"

Caption

This text caption is used to identify each data input item.

To change the caption, change the entry in the **Caption** field.

The text entered here is displayed in Inventory Tools.

Maximum Number of Characters for Field

To specify the maximum number of characters for the field, enter a numeric value in the **Max. width** field.

Field Data Type

The asset data fields are automatically populated. The data is either **calculated** or **derived**. The data can be extracted from text files, the Windows registry, environment variables and WMI fields. All data entry fields can be given a default value.

To chose the field data type:

In the **Asset Field Configuration** dialog box, choose a standard field type from the **Field data type** list: **Calculated** or **Derived**.

Calculated Fields

The following table describes calculated fields. These asset data fields can be automatically populated from data extracted from text files, the Windows registry, environment variables and so on.

Field	Description
Environment Variable Extract	Accepts data from a specified environment variable set in the operating system.
Registry Extract	This field type extracts its value from the Windows registry. The Data field must contain a valid registry key name to extract from, for example: HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control \TimeZoneInformation\StandardName
Text File Extract	Extracts information from a single line in a named text file. This field type is normally used for the Asset Number field. This is used to extract the asset number from the file Asset.bat on the line containing the text: SET ASSETNO= Other useful file extracts include the predefined SMS, which extracts the SMS Unique Machine ID.
WMI Extract	This field type allows you to extract and store pieces of data on Windows available through the WMI interface. The Windows scanner will populate this field (if set up) on systems where WMI is enabled.

Derived Fields

The following table describes derived fields.Derived fields are those that have dependencies on the data of other types of fields. In other words, the data they contain is derived from other fields.

Field	Description
Sequence	The Sequence field allows you to define a sequence of up to ten asset or hardware fields. Each of these fields returns a value depending on the machine or environment running. The value returned as the result of the sequence field will be the first of these fields which contains a non-blank value.
Combination	The Combination field uses a substitution string to replace occurrences of %1, %2 and so on. placeholders with the actual values of hardware or asset fields. An example of a Combination field can be found in the Description field of the default Asset Data tab. Up to five fields can be combined into one.
OS/Scan	Allows a single field to collect different information for different operating systems. For example, you may want to extract information from a registry on Windows and from a file on UNIX. For each scanner platform a separate asset field could be defined.

Setting Field Parameters

Field parameters need to be set for the following types of fields:

- **Sequence Fields**

  The Sequence field enables you to define a sequence of up to ten asset or hardware fields. Each of these fields returns a value depending on the machine or environment running. The value returned as the result of the sequence field is the first of these fields containing a non-blank value.

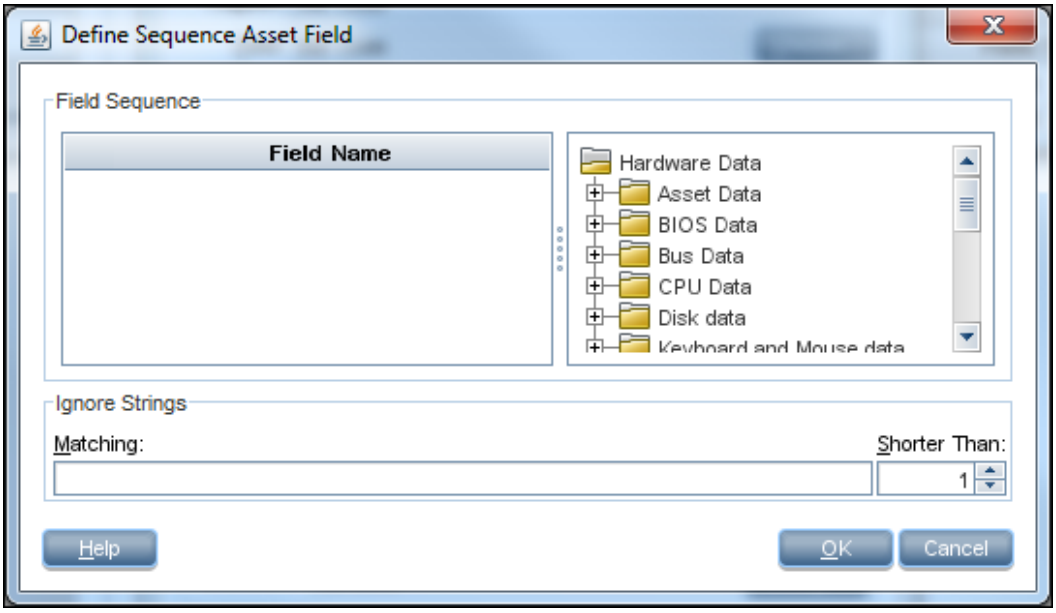
  Ignore Strings. Ignore strings are used to specify a set of values that are known to be incorrect, fake, or unwanted. These values should be ignored. For example, when specifying a MAC address as one of the hardware fields in a sequence, you can designate the known fake MAC addresses in the **Ignore Strings** so that they can be filtered out.

  A blank field can be defined based on either of the following two criteria:

  - The string matches an ignore string.
  - The length of the field is shorter than the number specified in the **Shorter Than** field.

  To set up a sequence field, perform the following steps:

  1. Select **Sequence** from the **Field Data Type**.
  2. Click **Change**. The **Define Sequence Asset Field** dialog box is displayed.



3. Select the desired field by expanding the tree on the right side and double-clicking it. The selected field is displayed in the **Field Name** list on the left side.

   You can also select the field with the drag-and-drop operation.

4. Use one or both of the following methods to specify the ignore strings:

   a. In the **Matching** box, type a string or a set of strings.

   > **Note:** The string is case-sensitive and the strings are separated by semicolons (;). For example, you can define a set of ignore strings as **Unknown;unknown;Not Tested.**

   If the content of the sequence field matches (is equal to) any of the strings specified here, the field is considered to be blank. For example, if the string Not Found is defined here, then a field that has the value 'Not Found' is considered to be blank.

   You can type a string in the form: *STRING*. Here the asterisks (*) are ignored and any string that contains the texts between the two asterisks will also be ignored.

   b. In the **Shorter** box, use the arrows or type a number to specify the minimum length of the string to be considered as non-blank.

   The default value is 1 and the maximum value is 255. If a field value's length is shorter than the specified number, then the field is ignored and considered blank.

   > **Note:** As an empty value's length is 0, an empty field is always ignored.

5. Click **OK**.

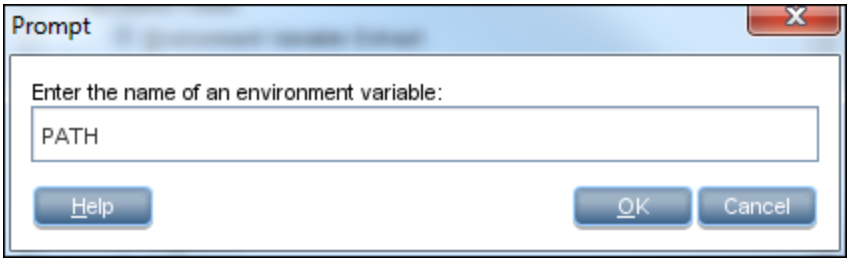
- **Environment Variable Extract Fields**

  This field is set up to read the value contained in an operating system's environment string. For example, you may have the Host Name or SMS ID stored in an environment variable and want

this to be automatically picked up by the scanner.

To set up environment field parameters:

1. After you have selected **Environment Variable Extract** as the date field type, click **Change**. The **Prompt** dialog box is displayed.



2. Enter the name of the environment variable in the **Prompt** dialog box. Examples of environment variables are TEMP and PATH.
3. Click **OK** to return to the **Asset Field Configuration** dialog box.

- **Text File Extract Fields**

  If you are using environment variables in the file path, they must be in uppercase. For example:

  ```
  %WINDIR%\SMSCFG.INI
  ```

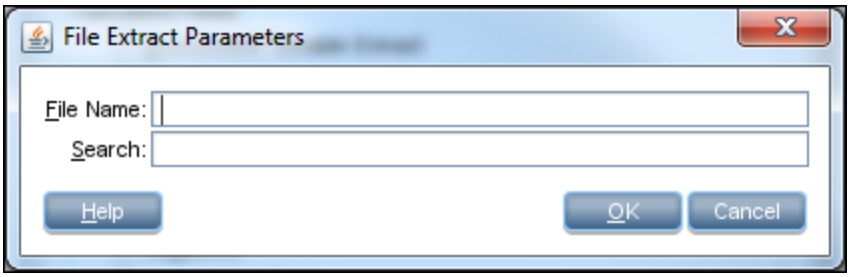
  This field searches a named text file for a defined character string and makes an automatic entry of the characters between the search string and the end of the line.

  This field type is normally used for the **Asset Number** field. This is used to extract the asset number from the file **Asset.bat** on the line containing the text:

  ```
  SET ASSETNO=
  ```

  To set up the Text File Extract field parameters:

  1. After you have selected **Text File Extract** as the data field type, click **Change**. The **File Extract Parameters** dialog box is displayed.



  2. In the **File Name** field enter the name of the file that the information is to be extracted from. Type the name and path to the file in the box.

     Note: Entries in this field are case-sensitive. This is applicable to UNIX and Mac OS X only.

     Using Environment Variables to Specify the File Name

You can use an environment variable to specify the file name. The environment variable name must be in upper case for this to happen. If it is not, the string is interpreted as a literal.

For example, if the path is

```
%WINDIR%\SMS.INI
```

Then the final path (assuming WinDir=C:\WINNT) will be

```
C:\WINNT\SMS.INI
```

But if the path is

```
%WinDir%\SMS.INI
```

Then no substitution will take place and the file extract will fail. This is done to ensure that it is possible to extract files from a directory or a file that has one or more % signs in the name.

Another example of using an environment variable is as follows:

You can type:

```
%HOME%/.bashrc
```

or

```
%SYSTEMDIR%\win.ini
```

Then the %HOME% will be replaced with the value of the HOME environment variable.

> **Note:** This is applicable to all platforms, and UNIX notation of the form $NAME is not supported.

3. Enter the **Search String**. This determines what information is to be extracted. A search string expression can be created in two ways depending on the file contents:
   - If you type * (an asterisk) for the search string, the scanner takes the complete first line of the file.
   - The scanner can find a line beginning with a particular anchor in a text file, and extract the rest of the line following the anchor. For example, if the line of the file has the following structure **VariableName=Value**, and **Value** needs to be extracted, set the search string to be **VariableName=**

   > **Note:**
   > - The search string is case *insensitive*.
   > - In the file being extracted from, if a comment is on the same line as the search string, then the comment is also returned. To prevent this happening, ensure that any comments in the file are placed on separate lines from the search string. This is particularly relevant to UNIX users.

4. Click **OK** to return to the **Asset Field Configuration** dialog box.

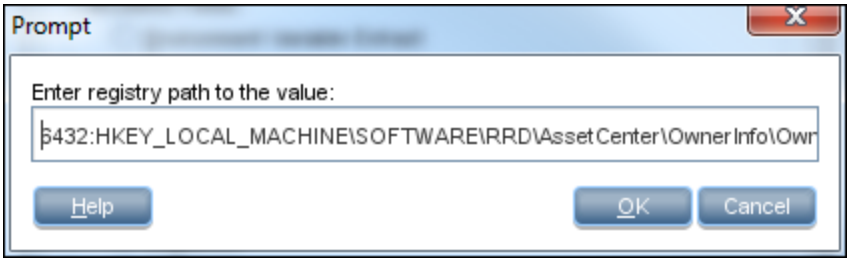
- **Registry Extract Fields**

  This type of field searches the Windows registry for the defined key and makes an automatic

entry of the key value. This extract field is applicable to Windows only.

To set up registry extract field parameters:

1. After you have selected a **Registry Extract** field as the data field type, click **Change**. The **Prompt** dialog box is displayed.



2. Type the full path to the registry value you want to have in this field in the form RegistryKey\Value.

   For example, to find out whether the Screen Saver is active on the system, you can use the following registry extract field:

   ```
   HKEY_CURRENT_USER\Control Panel\Desktop\ScreenSaveActive
   ```

   Note: The registry does not allow the backslash ("\") character in the RegistryKey. However, it can be used in Value. If the backslash character is contained in the Value name, it must be escaped. For example, if Value is "a\b", it must be specified as follows:

   ```
   HKEY_LOCAL_
   MACHINE\SY-
   STEM\CurrentControlSet\services\VSS\VssAccessControl\\NT
   Authority\NetworkService
   ```

   In Windows, the paths to various registry values can be found by viewing the content in the Registry Editor. For more information about the Registry Editor refer to the documentation supplied with Windows.

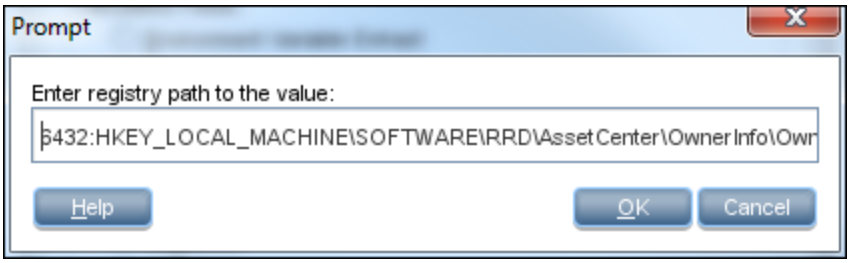
   In 64-bit versions of Windows, portions of the registry entries are stored separately for 32-bit applications and 64-bit applications and mapped into separate logical registry views using the registry redirector and registry reflection. This is because the 64-bit version of an application may use different registry keys and values than the 32-bit version. There are also shared registry keys that are not redirected or reflected.

   As the Universal Discovery Windows scanner is a 32-bit application, by default, the scanner only reads the 32-bit portion of the registry. In order to access the 64-bit registry portion in 64-bit versions of Windows, the scanner supports the following prefixes:

   - “32:” - forces only the 32-bit registry value to be read.
   - “64:” - forces only the 64-bit registry value to be read. In 32-bit versions of Windows, the registry extract field with this prefix will always be empty.
   - “3264:” - reads the 32-bit registry value, and, if it is empty, reads the 64-bit registry value.
   - “6432:” - reads the 64-bit registry value, and, if it is empty, reads the 32-bit registry value.

If no prefix is given, the scanner will only read the 32-bit registry value.

The actual registry value path should follow the prefix, as shown in the following example:



3. Click **OK** to return to the **Asset Field configuration** dialog box.

> **Caution:** Do not change any of the settings in the Registry Editor. Doing this could result in lost registry settings and may cause some of your applications to fail.

- **OS/Scan Fields**

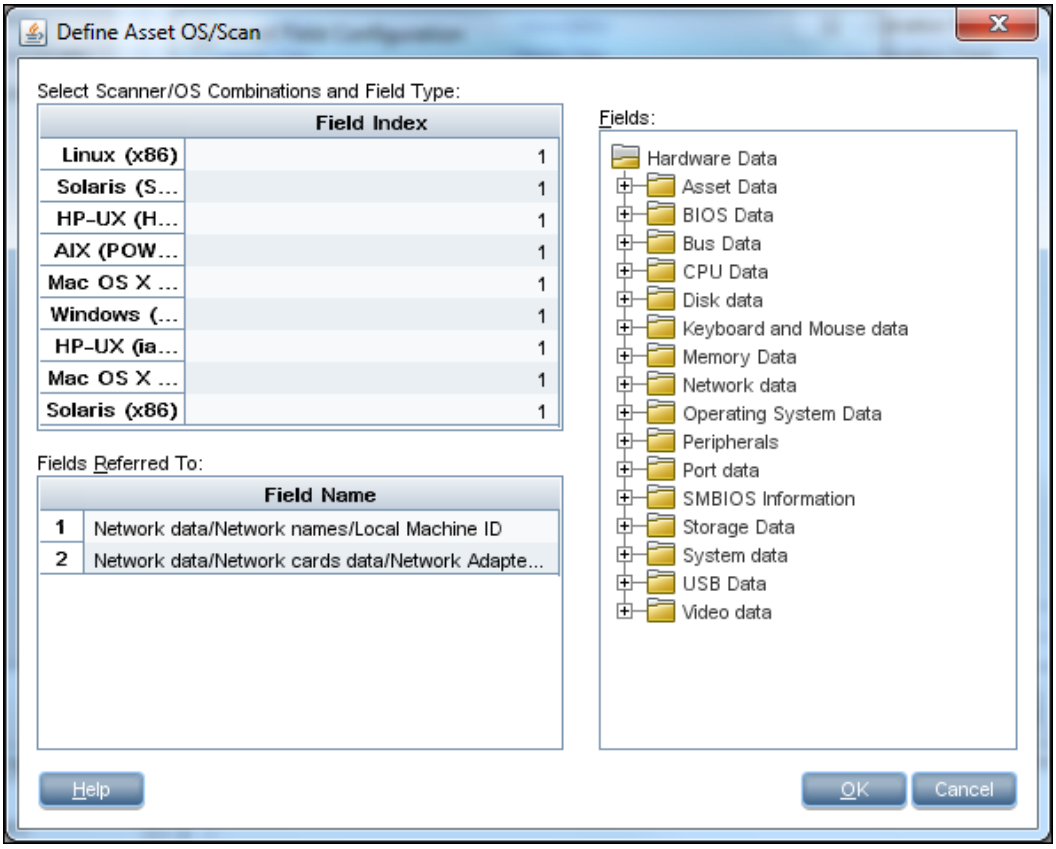
  The **OS/Scan** fields allow the definition of multiple types of data sources to provide an automatic entry depending on the scanner used and the operating system being scanned.

  This type of asset field is very useful in situations when you want to scan multiple operating systems but want to collect the same piece of information for each from different sources.

  For example, the data can be extracted from the registry on Windows or from a file on UNIX and Mac OS X.

  To set up OS/Scan fields:

  1. After you have selected **OS/Scan Field** as the data field type, click **Change**. The **Define Asset OS/Scan** dialog box appears.



2. In the **Field Index** list select the operating system that will be affected by this definition.
3. Select the field that is to be included in this definition from the **Fields** tree. This can be any existing asset field or any hardware/configuration field (except hardware fields where multiple values may be collected, such as CPU type or IP address).
4. Double-click the selected item in the **Fields** tree. The new definition is included in the **Fields referred to** list.
5. Click **OK** to return to the **Asset Field configuration** dialog box.

The **Field Index** column has a drop-down list which refers to the line numbers in the **Fields referred to** list.

- **Combination Fields**

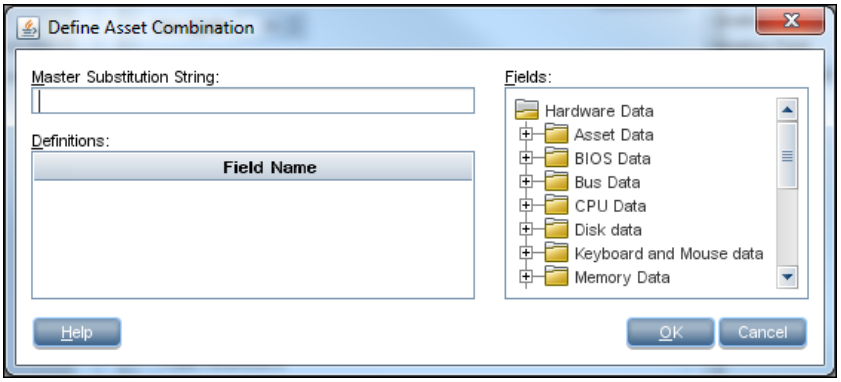
  Combination fields can combine up to five asset or hardware fields into a single field. This is particularly useful for the description field.

  The combination field is made up by string substitution.

  To set up a combination field:

  1. After you have selected **Combination Field** as the data field type, click **Change**.

     The **Define Asset Combination** dialog box is displayed.



2. Assign a **Master substitution string** by typing the template string in the box. The convention is to use percentage signs followed by a number. For example, '%1 (%2)'
3. The **Definitions** box lists the fields that have been defined for use in the substitution string.
4. To add a field to the **Combination** field, select either the **Asset** or **Hardware** field option and the available fields will be listed in the **Definitions** box.
5. To clear an entry select the **Delete** command from the right-click menu or press the **Delete** key.
6. In the **Definitions of %1 to %5** grid, build up a list of up to five index entries (represented as %1, %2, %3, %4 and %5).
7. Click in a row in the grid and from the Fields tree select the asset or hardware item that is to be associated with the index. The asset or hardware field will now appear in the **Field/Description** column.
8. Continue this for up to five index entries.
9. Define a master substitution string which replaces the percent values (for example, %1) with the appropriate hardware or asset item. An example of a master substitution string is shown in the next section.
10. You can also specify some text before or after the percent notation which will be a constant part of the value of the field.
11. Click **OK** to return to the **Asset Field Configuration** dialog box.

Example of a Master Substitution String

If the master substitution string %1 %2MHz %3Mb is defined for the Description field in the asset entry form, where the following index definitions apply:

Index	Field/Description	Display
%1	CPU Data\CPUs\CPU Type	CPU Type
%2	CPU\CPUs\CPU Speed (MHz)	CPU SpeedMHz
%3	Memory Data\Total memory (Mb)	Total MemoryMb

The **Description** field may look as follows:

```
Core i7 2666MHz 3958Mb
```

- **WMI Extract Fields**

  Some data on Windows operating systems is only available via the WMI interface. This type of field allows the scanner to be configured to extract and store specific pieces of WMI data. The Windows scanner will populate this field on computers where WMI is enabled.

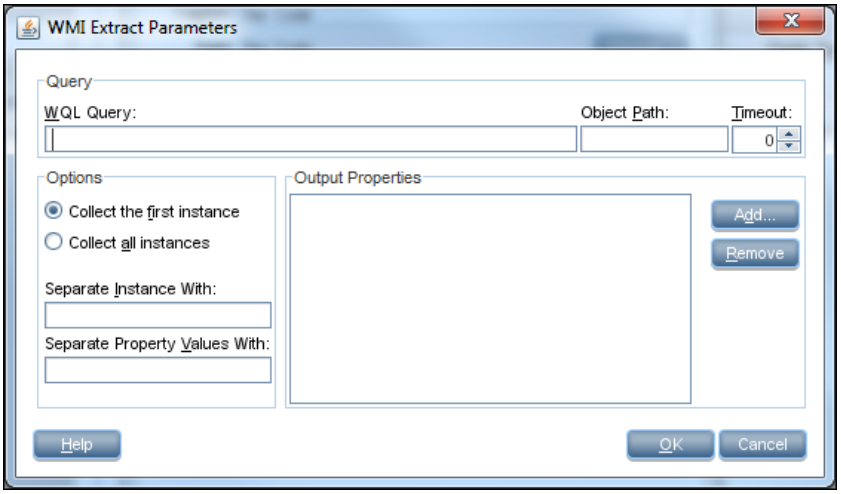
  Windows Management Instrumentation (WMI) is a component of the Microsoft Windows operating system that provides management information.

  Windows Management Instrumentation Query Language (**WQL**) is a subset of SQL that is used to make data queries inside WMI.

  For further information about WMI and WQL refer to the Microsoft MSDN web site.

  To set up a WMI extract field:

  1. After you have selected **WMI Extract Field**as the data field type, click **Change**.

  2. Enter the WQL query.

     For example, `select Name,CurrentClockSpeed from Win32_Processor`

     The above query collects the name and the frequency properties of the installed processor.

  3. Enter the **Object Path**.

     The Object Path should usually be:

     `root\cimv2`

     This is the default path for CIM v2 data provided by WMI.

  4. Enter the **Timeout**. This specifies the number of seconds to wait until the query returns a single instance of the queried data. If no data is returned within this period, the query will return nothing and the value of the field will be blank.

     You can use **-1** to wait indefinitely for the query to return data. However, this is not recommended since it may cause the query to hang.

  5. Enter the **OutputProperties**.

     These are properties whose value is required in the asset field. The WQL query returns an instance of the WMI class which can have many properties. The required ones need to be specified manually.

For example:

```
select * from Win32_Processor
```

This will return all properties for processor, but if **Name** is required, it should be specified in the **OutputProperties** list box.

6. Specify any Options

   Collect the first instance and **Collect all instances**

   These options specify whether the first returned instance or all returned instances should be used.

   For example, if there are several processors in a computer you can choose to have the information about the very first processor or have the information about all processors.

   If all instances are requested, their values will be separated with the string specified in the **Separate Instance With** field.

   When multiple properties are specified, the values returned by the query will be separated with the string specified in the **Separate Property Values With** field.

7. Click **OK** to return to the **Asset Field Configuration** dialog box.

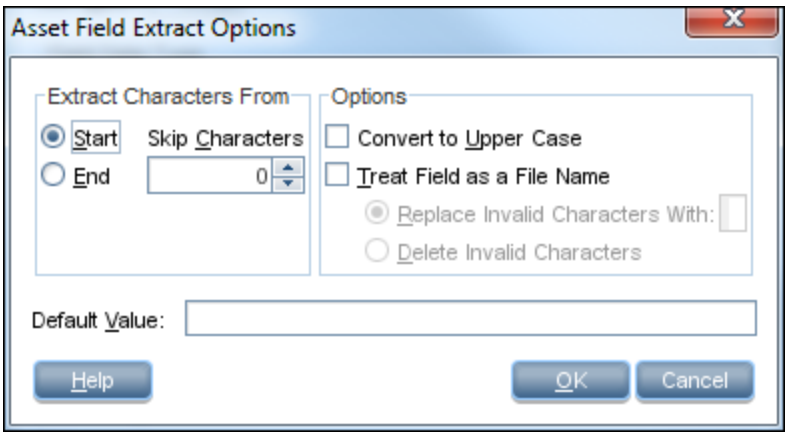
Setting Extract Options

All calculated asset fields defined can be set up so that only part of the string is selected instead of the entire string. They can also be set up, for example, to use the last part rather than the first part of the string. This can be useful for obtaining the last part of a calculated field that is too long.

Various other settings for manipulating the field contents are also available.

To set extract options:

1. After you have selected the field data type, click **Extract**. The button is only enabled for those field that are calculated. This option is not available for user-entered fields. The **Asset Field Extract Options** dialog box is displayed.



2. In the **Extract Characters From** group box, specify whether you want to use the last part or the first part of the string. Select one of the following options:

- **Start** - Uses the first part of the string. Use the arrows next to the **Skip characters** box to specify how many characters are to be skipped from the beginning of the string.
- **End** - Uses the last part of the string. Use the arrows next to the **Skip characters** box to specify how many characters are to be skipped from the end of the string.

For example, **ABCDEF123**. If you select **End** and skip **4** characters, the result is **ABCDE**.

3. In the **Options** group box, select the options as follows:
   - **Convert to Upper Case**- Select this option to convert the alphabetic characters to upper case, if required.
   - **Treat Field as a File Name**- Select this option to treat the string in the asset field as a file name.

   Some characters are invalid in file names, so any invalid characters can be replaced with the character specified in the **Replace Invalid Characters With** box. For example, underscore (_) is a valid file name character and can be used to replace invalid characters.

   If you select the **Delete Invalid Characters** option then any invalid characters are deleted.
4. If the extracted field is empty or is not found, then a default value for the string can be specified in the **Default Value** box. For example, if the text string **Not Found** is entered in this box, then an empty field or a field that has not been found is assigned this default value.

Order of the Fields in the Form

You must consider the order of the fields in the form, and move them round accordingly. The rule is:

A field cannot depend on a field that is placed below it in the form.

That is, if you have set up any derived or automatic fields that require data from fields below them in the form, you must move them to a position in the form that is above these fields.

To correct the order of the field in the form:

1. Re-order the fields by clicking on a row and dragging the selected line to its new location in the form.
2. When you click **Next** in the **Asset Data** page, a confirmation message may be displayed.
3. Click **Yes** to have the Scanner Generator automatically do this for you.
4. Click **No** to do this manually.

How to Configure Analysis Asset Fields

The Analysis Asset Field configuration settings that affect the XML Enricher cannot be modified in the Web UI. You can change these settings by using the Viewer. To do this, follow these steps:

1. Select **Start > All Programs > HP UCMDB > Inventory Tools > Viewer**.
2. Use **File > Options > Asset Fields** to configure the Analysis Asset Fields.

For more information, see the Inventory Tools documentation.

How to Configure Software Utilization

Configure Software Utilization depending on your method of discovery, and it also may depend on your discovery node platform.

To configure software utilization in a Management Zone, perform the following:

Zone-Based Discovery

1. Infrastructure Discovery wizard: On the Agent Deployment page, select a value for **Software Utilization Period**.
2. Inventory Discovery wizard: On the Preferences page, select **Scanner Based Inventory Discovery**. In the **Model Per User Data** box, select or enter the number of users.

> **Note:** The default scanner configuration file is already configured to collect utilization data. However, if you customize the scanner configuration file using the Scanner Generator, on the **Software Details** page ensure that **Software Utilization** is selected.

Manual

- **Windows**. When installing the UD Agent using the Agent Installation wizard, on the **Agent Configuration for Manual Mode** page, ensure that you select a value for the **Software Utilization Period**option. For more details, see "Agent Installation Wizard User Interface" on page 100.
- **UNIX**. Use command line parameters when installing a discovery package on a discovery node. For more information, see "Universal Discovery Resources for UNIX" on page 107.

Agentless Discovery

When configuring and deploying discovery resources using manual methods, in the Scanner Generator > "Directories Tab", ensure that the select the **Software Utilization** option is selected.

How to Map Scan File Attributes to UCMDB

This task describes how to map attributes that are contained in scan files to UCMDB CIs.

This task includes the following steps:

1. "Prerequisites" below
2. "Create a CI to map" below
3. "Add attributes to the CI" on next page
4. "Results" on next page

1. Prerequisites

Before creating a mapping, perform an analysis on what information you want to map, what data element in the scan file contains the information you want to capture, where the data element in the scan file is located, and which UCMDB CI you want to store this information.

2. Create a CI to map

a. Open the Hardware Mapping Configuration dialog box. To do this, perform one of the following:

   i. **Adapter Management > Inventory Discovery by Scanner > Adapter Definition** tab , expand the **Global Configuration Files** pane, click **HardwareMappingConfig** and then click **Edit**  .

   ii. **Inventory Discovery Activity > Preferences Page**, then click the **Custom Mapping** button. For more information, see the section describing the Inventory Discovery Activity in the *HP Universal CMDB Discovery and Integration Content Guide*.

b. Click **Add CI**  to add a CI. The Select CI dialog box opens.

> **Note:** This option is only available when **Hardware Mapping Configuration** is selected in the left pane.

c. Select a CI that you want to create a mapping.

d. In the CI Editor, select properties for the selected CI.

3. ### Add attributes to the CI

a. Click **Add Attributes**  to add attributes to a selected CI. The Select an Attribute dialog box opens.

b. Select properties for the selected attribute in the Attribute Editor.

4. ### Results

Verify that data in the scan file was mapped as expected to UCMDB by using the CI Type Manager. For more information, see the section that describes the CI Type Manager in the *HP Universal CMDB Modeling Guide*.

How to Deploy User-Defined SAI Files

This task describes how to deploy user-defined SAI files.

1. Prerequisite: Ensure you have the tool **saiPackager.cmd** installed on the Probe side's installation directory. For example, **C:\hp\UCMDB\DataFlowProbe\tools**
2. Copy the SAI files to the Probe side's installation directory.
3. Execute **saiPackager.cmd user.zsai**, where **user.zsai** is the name of the SAI file.

> **Note:** If you have multiple SAI files, execute **saiPackager.cmd a.zsai b.zsai c.zsai**, where **a.zsai b.zsai** and **c.zsai** are the names of the SAI files.

   This creates a file: **Sai.zip**.

4. Go to the **UCMDB Package Manager** and deploy **Sai.zip**.

> **Note:** If **Sai.zip** is larger than 500 MB, deploy it using the JMX Console:

a. Copy the file **sai.zip** to a suitable directory in the UCMDB server.

b. Log in to the UCMDB Server's JMX Console. For example, **http://uCMDBserver:8080/jmx-console**.

c. Select **Packing Services**.

You must specify the directory and full file name separately (as stored on the UCMDB Server) when deploying with the JMX Console.

d. Click **deployPackages** and Invoke it.

5. Select **Discovery Control Panel > Discovery Modules/Jobs > Hosts and Resources > Inventory Discovery > Inventory by Scanner > Inventory Discovery by Scanner** job.
6. Click the **Properties** tab in the right pane.
7. In the **Global Configuration Files** pane, click on **EnricherServiceSettings.ini**.
8. Click the  button on the toolbar. The **Software Recognition Configuration** dialog box is displayed.
9. Select the **SAI Recognition** tab. The newly deployed file is displayed in the list. Ensure you have selected the check box for the file and click **OK**.

Inventory Discovery User Interface

This section includes:

Hardware Mapping Configuration Dialog Box

Enables you to map scan file hardware attributes to UCMDB CIs.

To access	Use one of the following: • **Adapter Management** > **Inventory Discovery by Scanner**, click the **Adapter Definition** tab, expand the **Global Configuration Files** pane, click **HardwareMappingConfig** file and click **Edit**  . • From the Inventory Discovery Activity, go to the Preferences Page and then click **Custom Mapping** button. **Note:** This option is available only when the Scanner Based Inventory Discovery option is selected on the Preferences Page.

Important information	Before creating a mapping, perform an analysis on what information you want to map, what data element in the scan file contains the information you want to capture, where the data element in the scan file is located, and which UCMDB CI you want to store this information.
Relevant tasks	"How to Map Scan File Attributes to UCMDB" on page 378

User interface elements are described below:

UI Element	Description
	**Add CI.** Opens the Select CI dialog box, enabling you to create a new mapping between a scan file attribute and UCMDB CI properties. When the Select CI dialog box opens, select a CI that you want to create a mapping. Available: When **Hardware Mapping Configuration** is selected in the left pane.
	**Add an Attribute.** Opens the Add an Attribute dialog box, enabling you to add a mapping between a scan file attribute and a selected UCMDB CI. • **Attribute.** Select an attribute from the drop down list to map to scan file attributes. • **Display Label.** The name of the attribute • **Type.** The data type of the attribute as it appears in the CI Type Manager. For more information, see the section describing the CI Type Manager in the *HP Universal CMDB Modeling Guide*.
	Enables you to delete the selected UCMDB CI or attribute.

CI Editor

Enables you to define attributes of the UCMDB CI that you want to map to scan file attributes.

Important information	This page is displayed when a CI is selected in the left pane.

User interface elements are described below:

UI Element	Description
CI Name	The display name of the CI that is selected in the left pane.

UI Element	Description
Relationship	Click the ellipsis to open the Create Relationship with Node CI dialog box, enabling you to select the relationship that you want for the mapping. If you want to remove the value in this field, click **Delete**. **Note**: • This is an optional field. • If there are no options available in the drop down list, there are no relationships that are created in UCMDB for the selected CI. • Selected values are ignored if they conflict with system values.
Kind	The number of instances of the CI to map. • **Single.** Only one instance of the selected CI is created in UCMDB. • **Multiple.** Multiple instances of the selected CI are created in UCMDB. For example, if three instances that are mapped from the scan file, three instances of the CI are created in UCMDB.
Create New CI	Enables you to create a CI instance for the selected CI. • **Yes.** Create a new CI instance to map scan file information to a CI type when the CI type is not contained in the **ParseEnrichedScanFile.py** script. • **No.** Ignores mapping of the selected CI when the CI type is not contained in the **ParseEnrichedScanFile.py** script. **Default:** No
Parent Shell	Opens the Select a Shell Tag dialog box, enabling you to select a structural part of the scan file where the information that you want to map is located. Select a value for this field if you want to define the value type for the mapped attribute as **array**. Otherwise, this is an optional field.

Attribute Editor

Enables you to define properties of scan file attributes that you want mapped to UCMDB CIs.

Important information	This page is displayed when an attribute is selected in the left pane.

User interface elements are described below:

UI Element	Description
Attribute Name	Displays the name of the attribute that is selected in the left pane. Click to open the Select an Attribute dialog box to edit properties of the attribute. **Note:** If you change the attribute name, the previous attribute values are overwritten.

UI Element	Description
Value Type	The data type of the attributes in your scan file. • **Scalar.** Non-composite value, such as boolean, numeric, or character data types. • **Array.** Collection of values or variables that are selected by one or more indices. **Note:** This option is only available when there is a value for the Parent Shell field in the "CI Editor" on page 381. • **Pre/Post.** Use mappings that are contained in scripts that can map scan file values to UCMB CIs. • **Script.** Customize data parsing by using a jython script.
Value	Values that are displayed correspond to the option that is selected in the **Value Type** field. • **Scalar.** Click the ellipsis  to open the Select a Scalar Tag dialog box and then select a structural part of the scan file where your mapped information is located. • **Array.** Click the ellipsis to open the Select an Array Tag dialog box and then select a tag type that corresponds to the attribute tags in your scan file. **Note:** If this option is selected, the only options that are displayed are tags for the value set for the **Parent Shell** field in "CI Editor" on page 381. • **Pre/Post.** The Scanner reads the output of the pre- and post-scan scripts and captures all lines with the following structure: **<attributename>=<value>** The length of the **<attribute>** tag can be up to 256 characters, and the length of the **<value>** tag can be up to 1024 characters. **Note:** The Scanner captures any script output line that contains an equal sign (=), except if the equal sign is the first character on the line. • **Script.** Enter your Jython script code. For more information, see the section that describes Jython script development in the *HP Universal CMDB Developer Reference Guide*. **Note:** The script must return a value.
Overwrite	Select an option to overwrite values that were generated by the **ParseEnrichedScanFile.py** script when the last Inventory Discovery job ran. • **Yes.** The values generated from this mapping overwrite previous values. • **No.** The values generated from this mapping do not overwrite previous values. **Default:** No

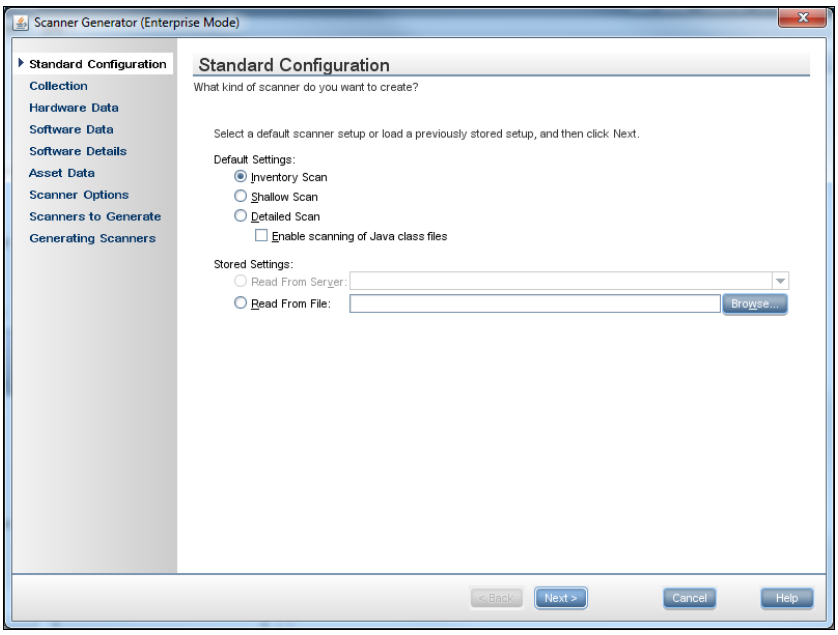
Scanner Generator Wizard

Enables you to configure and generate scanners to collect information.

To access	**To edit existing scanner configuration, or create a new scanner configuration** In configuring the **Inventory Discovery** Activity, on the **Preferences** page. 1. Select **Scanner-based Inventory Discovery**. 2. Click the dropdown button on the **Scanner Configuration** pane. 3. Click **New/Edit Scanner Configuration** in the **Scanner Configuration** pane. **To generate a new Manual Deployment scanner:** 1. Select **Data Flow Management > Adapter Management > Resources > Inventory Discovery >Scanner Configuration Files**. 2. Select the configuration file (.cxz) in the tree on the left, and click the **Generate Scanners...** button in the right pane.
Wizard map	The **Scanner Generator Wizard** contains: "Standard Configuration Page" > "Collection Page" > "Hardware Data Page" > "Software Data Page" > "Software Details Page" > "Asset Data Page " > "Scanner Options Page " > "Scanners to Generate Page" > "Generating Scanners Page"

Standard Configuration Page

Use this page to select a default scanner setup or to select a previously stored setup.



Important Information	General information about the wizard is available in "Scanner Generator Wizard".
Wizard Map	The "Scanner Generator Wizard" contains: "Standard Configuration Page" > "Collection Page" > "Hardware Data Page" > "Software Data Page" > "Software Details Page" > "Asset Data Page " > "Scanner Options Page " > "Scanners to Generate Page" > "Generating Scanners Page"

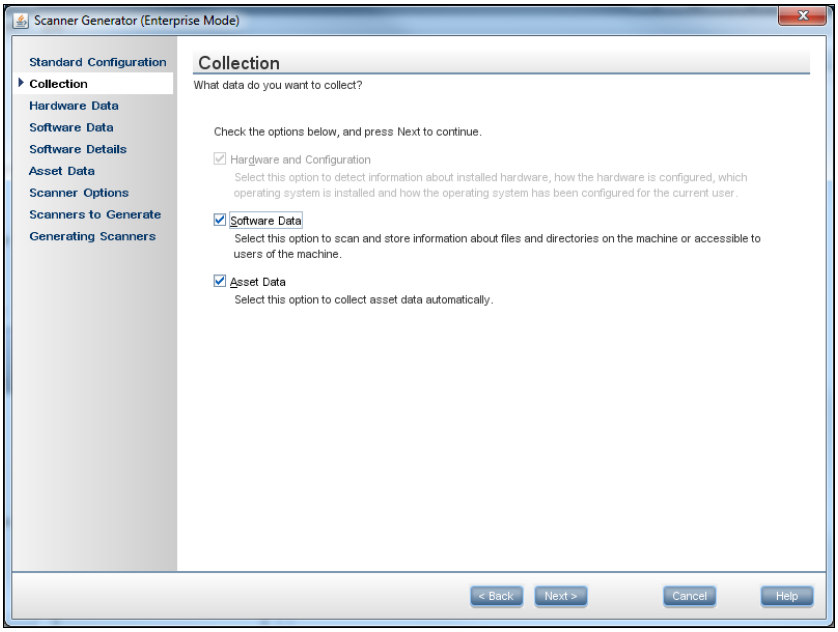
User interface elements are described below:

UI Element (A–Z)	Description
Detailed Scan	If scanning time is not a critical factor, the Detailed Scan option can be used to collect the maximum amount of information. This, however, extends the scanning time significantly. Use this option in special cases only.

UI Element (A–Z)	Description
Enable scanning of Java class file	If you select **Inventory Scan** or **Detailed Scan**, you can choose to **Enable scanning of Java class files**. This setting deals with Java scanning. Enabling this setting does the following: • Java .class files are stored in the scan file • Java specific environment variables for targeted scanning is enabled. • Windows scanner adds the location of the Java Home directory to the list of directories for a targeted scan.
Inventory Scan	Uses default configuration setting for the scanner. Defines a set of options suitable for a general inventory. Enough software information is collected to allow comprehensive inventory analysis. All hardware information is collected and a standard series of asset data fields are defined
Read From File	Replaces various configuration settings by reading information from files on the local machine. It can read parameters from previously generated scanners, scanner configuration files (.cxz), and scan files (.xsf). When the file name is provided, the Scanner Generator determines the type of the file based on the file extension, which eliminates the need to have a separate entry for each.
Read From Server	Reads the settings from a previous Enterprise Mode configuration stored on the server. The drop down combo box shows the list of previously configured scanner configurations. The names displayed with angle brackets around them (for example, <default>) are predefined configurations. It is possible to read predefined configuration settings, but it is not possible to overwrite them when generating the new configuration. If you have chosen a predefined configuration, you will have to rename it when you come to the last page of the Scanner Generator in order to save it to the server. If you save this configuration, it will be available from the server with the other previous configurations.
Shallow Scan	Defines a set of options to allow very quick scans. Because hardware scanning is very fast, most hardware items (as some are disabled by default) are collected, but limited software scanning takes place, and the data collected is not sufficient to perform reliable software license recognition.

Collection Page

The **Collection** page is used to select the type of computer data to collect.The selections you make on this page determine which of the data detail pages are displayed.



When carrying out initial scanner deployments you might want to use hardware and asset data collection to establish basic information for the target machine. This can be followed up later by a more comprehensive scan that includes software data.

Important Information	General information about the wizard is available in "Scanner Generator Wizard".
Wizard Map	The "Scanner Generator Wizard" contains: "Standard Configuration Page" > "Collection Page" > "Hardware Data Page" > "Software Data Page" > "Software Details Page" > "Asset Data Page " > "Scanner Options Page " > "Scanners to Generate Page" > "Generating Scanners Page"

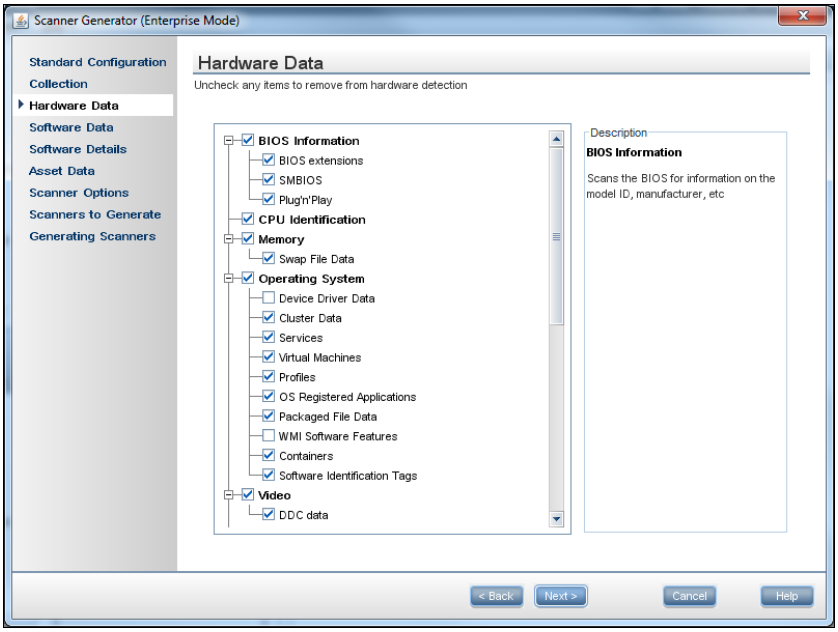
User interface elements are described below:

UI Element (A–Z)	Description
Asset Data	If selected, the scan collects Asset data which consists of asset fields that can be collected automatically. See "Asset Data Page ".

UI Element (A–Z)	Description
Hardware and Configuration	If selected, the scan collects hardware and configuration data, including details of the processor, memory configuration, computer bus, attached cards, hard disks, attached drives, monitor, video adapter, keyboard, mouse, OS version, network protocols and addresses. See "Hardware Data Page". **Note:** For Enterprise Mode, this option is always selected and cannot be disabled.
Software Data	If selected, the scan collects detailed information about files and directories on all scanned drives. The information collected about files can be defined (including the file types inventoried and the level of information collected). It is possible to define which drives are to be scanned, based on the media of the drive, as well as determine which files are included in the scan file and which are ignored. See "Software Data Page".

Hardware Data Page

The **Hardware Data** page displays a subset of the hardware categories the scanner can collect. It is used to disable specific hardware detection routines. Normally all hardware options are selected. Routines only need to be removed if there is a known problem scanning these hardware items. The hardware options have equivalent command line options that can be used at run-time.



Important Information	• General information about the wizard is available in "Scanner Generator Wizard". • For information about scanner command line options, see "Scanner Command Line Parameters and Switches". • For a comprehensive list of hardware data the scanner can collect, click the following link to access the file: DataCollectedByTheScanners.html.
Wizard Map	The "Scanner Generator Wizard" contains: "Standard Configuration Page" > "Collection Page" > "Hardware Data Page" > "Software Data Page" > "Software Details Page" > "Asset Data Page " > "Scanner Options Page " > "Scanners to Generate Page" > "Generating Scanners Page"

Disabling Specific Hardware Detection Routines

You can disable the hardware detection routines for a specific category by clearing the check box next to it. All other hardware detection will take place as usual.

Hardware Categories

Category	Description
BIOS information	Collects information about the computer BIOS, including the computers asset tag, the BIOS date, ID, manufacturer and revision (where applicable). Select this check box if you want to collect data for software license compliancy. For more information, see "Software License Compliancy" on page 342.
BIOS extensions	Detects installed BIOS extensions, such as video or SCSI BIOS. Select this check box if you want to collect data for software license compliancy. For more information, see "Software License Compliancy" on page 342.
SMBIOS	Collects hardware data from System Management BIOS. Select this check box if you want to collect data for software license compliancy. For more information, see "Software License Compliancy" on page 342.
Plug'n'Play	Provides details of whether the BIOS installed on the computer is Plug and Play compatible. If the BIOS supports Plug and Play specification, the version of the specification is collected. Select this check box if you want to collect data for software license compliancy. For more information, see "Software License Compliancy" on page 342.

Category	Description
CPU Identification	Identifies the CPU (model), establishes if it has got FPU (numeric coprocessor), MMX (MultiMedia eXtensions) and ISSE/SSIMD capability and reports the speed of the CPU, cache characteristics. For newer Intel and compatible processors, the manufacturer, model, family and stepping ID are reported. Select this check box if you want to collect data for software license compliancy. For more information, see "Software License Compliancy" on page 342.
Memory	Detects the total amount of memory installed on the computer, including the amount of conventional and extended memory.
Swap File data	Collects data about swap files used for virtual memory.
Operating System	Collects information about the operating system and its configuration.
Device Driver Data	When this option is enabled, the Windows scanner enumerates all devices to determine which files are used as device drivers. Each file in this list is given the 'Device Driver' attribute when stored in the scan file. The device driver option is now disabled by default to increase speed of the hardware scanning.
Cluster Data	Collects information about Windows Server Cluster membership. It detects that the machine is part of a cluster, the name and description of the cluster and the list of nodes connected to the cluster.
Services	Collects information about installed operating system services.
Virtual Machines	Detects whether the scanner is running in VMware, Virtual PC, Terminal Services, Hyper-V, LPAR, vPar, or nPartition. From an asset management point of view, it is important to be able to determine which scanned machines are virtual (for example, so you don't pay too much maintenance for too many machines).
Profiles	Collects data about user profiles.
OS Registered Applications	Collects data about installed applications that are registered with the operating system. On Windows (pre-Vista), it collects data as displayed by the Add/Remove programs item in the Control Panel. On Windows (Vista and later), it collects data as displayed by the Programs and Features item in the Control Panel. On UNIX, it collects data from the system's software package manager.

Category	Description
Packaged File Data	Collects information about the relationship between the installed applications (packages) and the files that belong to them. When this option is set, it causes the scanner to interrogate the native operating system package manager to retrieve the relationship information. This ensures that the installed package rule-based recognition can correctly recognize the files as belonging to the installed package/application.
WMI Software Features	Collects the information about installed applications from WMI as stored in the Win32_SoftwareFeature class. The Win32_SoftwareFeature WMI class is not available on the Windows 2003 Server by default. The WMI provider that supports this class is an optional component on Windows 2003 Server, and it is not installed by default. To enable this WMI provider, you must go to **Control Panel** > **Add Remote Programs** > **Add/Remove Windows Components** > **Management and Monitoring Tools** > **WMI Windows Installer Provider** and install the WMI Windows Installer Provider component. Once this component is installed, the data collected by WMI Software Features hardware detection becomes available.
Containers	Collects data about containers available in the operating system. Currently, this is supported for Solaris zones, HP_UX nPartition/vPar, and AIX LPAR.
Software Identification Tags	Collects the information in software identification tag files, which are XML files that consist of identification and management information about a software product. These tag files uniquely identify the software product, providing data for software inventory and asset management. During the hardware detection phase, the Scanner collects the information from software tag files from the common system location, as well as from the top level directory of the application, in the event that software scanning of the installation locations is done. If you do not select the **Software Identification Tags** check box, the Scanner will not collect any information from tag files during the hardware detection phase. For detailed information, see "Software Identification Tags ".
Video	Records details of the Video Display Adapter, which include the adapter type (EGA, XGA, VGA and so on) and model/manufacturer, where possible. In Windows the current desktop resolution and number of colors are also picked up.
DDC Data	When connected to a VESA DDC compliant monitor, collects full monitor information.
I/O Ports	Detects and reports on the number of serial and parallel ports, the I/O address for each, and for serial ports, the UARTs attached.

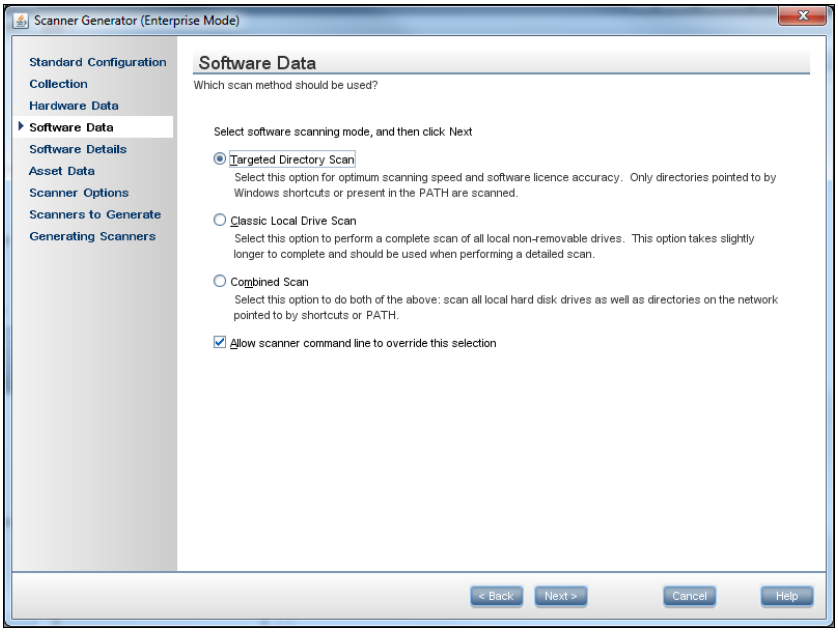
Category	Description
SCSI/ASPI Detection	Checks for the presence of an ASPI (Advanced SCSI Programming Interface) driver for a SCSI adapter. If the driver is available, the host SCSI adapter name is reported.
SCSI/IDE/ATAPI devices	Detects installed devices, such as hard drives, CD-ROMs, tape drives and other such devices. Also detects Serial ATA disks.
SCSI/IDE/ATAPI serial numbers	Detects serial numbers of the installed devices (where available). Also detects the serial number of Serial ATA disks.
Network Information	Detects the network configuration, including Logon Name, Workgroup Name, Machine ID, and Domain Name. Detects information such as multiple network adapters, gateways, DNS servers, subnet masks, DHCP status. Information about installed network protocols (TCP/IP, NetBIOS/NetBEUI, IPX/SPX) and network addresses is also provided. Note: In Enterprise Mode, it is possible to disable subsets of network information. However, you should not disable ALL network information.
TCP/IP	Collects information about an installed TCP/IP protocol. This information includes domain, DNS Servers, Node type, NetBIOS Scope ID, WINS proxy status, NetBIOS resolution status. Network adapter information (including description, IP address, IP routing status, subnet mask, default gateways, DHCP status, DNS suffix, autoconfiguration status) is also provided.
IPX/SPX	Collects information about the IPX/SPX protocol.
NetBIOS/NetBeui	Collects information about the NetBIOS or NetBEUI protocol.
Shared Devices	Collects information about shared devices, such as disks and printers.
Keyboard & Mouse	Reports on the type of keyboard attached (extended or normal); whether a mouse is connected and mouse driver is loaded; the mouse brand and version of the driver, number of buttons and type of connection (serial, PS/2, bus).
Disk Drives	Collects advanced information about all attached disk drives. This information includes the type of the drive (floppy disk, hard disk, CD-ROM, network), the type of the file system (FAT, NTFS, HPFS), amount of total and free space, location of the hard drive partitions on the physical hard disk and so on.

Category	Description
Local USB Hard Drives	Controls the way USB hard drives are treated. If checked (default setting), the USB hard drives are treated as local hard drives, and their size is counted towards the total and free space on the local hard drives, which is recorded in the hwDiskTotalFreeMB and hwDiskTotalSizeMB hardware fields. If the option is unchecked, the USB hard drives are treated as removable drives, and their size will not be counted towards the total size. Also, by default, the USB hard drives will not be scanned during a "classic" local hard drive scan. However, you can enable scanning by checking the **Software Details** > **Drives** > **Removable Drives** > **Other removable drives** check box. This option is currently only applicable to the Windows scanner.
Bus Detection	Detects the architecture of the bus used in the PC – ISA, EISA, PCI, MCA, or PCMCIA. • **EISA** - Detects and reports details of EISA cards. • **MCA** - Detects and reports details of MCA cards. • **PCI** - Detects and reports details of PCI cards. • **PCMCIA** - Detects and reports details of PCMCIA cards. • **ISA PnP Cards** - Detects and reports details of ISA Plug and Play cards. • **USB Data** - Detects and reports details of the USB host adapters, hubs and devices attached to them. If the bus types checked for by the scanner are not available, the tests for checking the cards will not be performed.
Peripherals	Checks for installed peripherals, such as printers, modems and sound cards.
UNIX System Configuration	Collects UNIX, Linux, and Mac OS X configuration information.

Software Data Page

The **Software Data** page is used to select the software scanning method. The choice of scan method determines how extensive the software scan will be, and depending on which of these modes you select, different sets of tab pages are displayed on the **Software Details Page** when you click **Next**.

Under most circumstances, the default settings (which are determined by the presets chosen on the Standard Configuration page) are satisfactory for defining the software information collected, but the Scanner Generator allows the default options to be modified to create custom settings.



Important Information	General information about the wizard is available in "Scanner Generator Wizard".
Wizard Map	The "Scanner Generator Wizard" contains: "Standard Configuration Page" > "Collection Page" > "Hardware Data Page" > "Software Data Page" > "Software Details Page" > "Asset Data Page " > "Scanner Options Page " > "Scanners to Generate Page" > "Generating Scanners Page"

User interface elements are described below:

UI Element (A–Z)	Description
Allow scanner command line to override this selection	If you select this check box, the default drive selection specified can be overridden by specifying a list of drive letters or directories to scan on the command line using the –paths command line option. An example of a command line override is: `Scanwin32-x86 -paths:C:\Windows -paths:D:` If you clear this check box, you cannot change the scan selection by specifying drive letters or paths on the command line. For more information, see "Scanner Command Line Parameters and Switches".
Classic Local Drive Scan	Select this option to perform a complete scan of all local non-removable drives. This option takes longer to complete and is used when performing a detailed scan. The tab pages shown on the **Software Details** page when you click **Next** are: • "Drives Tab" • "File Scanning Tab" • "Stored Files Tab"
Combined Scan	Select this option to do both of the previous options: scan all local hard drives as well as directories on the network pointed to by shortcuts, file associations and environment variables, such as PATH. The tab pages shown on the **Software Details** page when you click **Next** are: • "Drives Tab" • "Directories Tab" • "File Scanning Tab" • "Stored Files Tab"
Targeted Directory Scan	Select this option for optimum scanning speed and software license accuracy. Only selected locations are scanned, which are identified by the scanner from various sources, such as Windows shortcuts, Services, file associations, environment variables, and so on. The tab pages shown on the **Software Details** page when you click **Next** are: • "Directories Tab" • "File Scanning Tab" • "Stored Files Tab"

Software Details Page

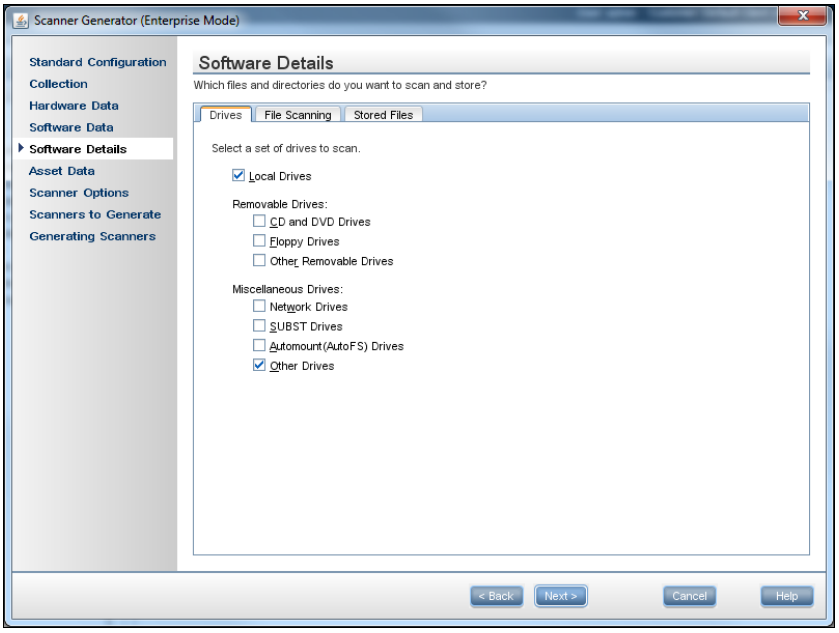
The **Software Details** page shows a set of tab pages according to the selections made on the **Software Data** page.

- "Drives Tab"
- "Directories Tab"
- "File Scanning Tab"
- "Stored Files Tab"

Important Information	General information about the wizard is available in "Scanner Generator Wizard".
Wizard Map	The "Scanner Generator Wizard" contains: "Standard Configuration Page" > "Collection Page" > "Hardware Data Page" > "Software Data Page" > "Software Details Page" > "Asset Data Page " > "Scanner Options Page " > "Scanners to Generate Page" > "Generating Scanners Page"

Drives Tab

The **Drives** tab page is used to define which of the drives are to be scanned when using either **Classic Local Drive Scan** or **Combined Scan.**



Options are provided for scanning all drives or just a particular type of drive.

User interface elements are described below:

Local Drives

These are hard disk drives visible and mounted by the current operating system. In Windows, normal hard disk drives are assigned drive letters by the operating system and are usually included in the scanning process.

Removable Drives

Removable drives are drives with non fixed media that can be removed or exchanged. Removable drives are normally not included for scanning.

UI Element (A-Z)	Description
CD and DVD Drives	Scans the contents of CD and DVD drives. See "Automount (AutoFS) Drives" for detailed information about scanning automatically mounted drives.
Floppy Drives	Scans the contents of floppy drives. See "Automount (AutoFS) Drives" for detailed information about scanning automatically mounted drives.
Other Removable Drives	Scans other removable drives (for example, SyQuest drives). Scanning removable media is not usually recommended, as the content of these drives vary depending on the media currently in the drive.

Miscellaneous Drives

These drives are any drives that do not fall into any of the previous categories, and may or may not have local physical media associated with them

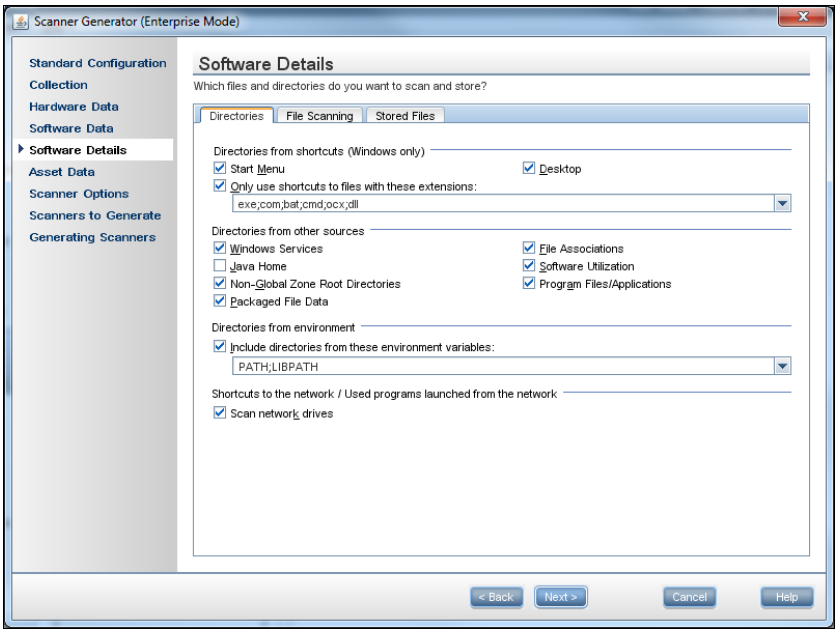
UI Element (A-Z)	Description
Automount (AutoFS) Drives	When not selected (the default setting), the scanner will not scan any auto-mounted drives. The scanner will not attempt to mount any indirect automount drives. It may mount a direct automount drive if it comes across its mount point during the software scanning process, but the direct automount drive itself will not be scanned. When selected, the automount drives are scanned only if all of the following conditions are met: • The directory where the drive's mount point is located is itself getting scanned. For example, it is located on a drive for which the corresponding drive-type check box is checked. • The drive-type check box for the real drive type of the automount drive is also checked. For example, an auto-mounted NFS drive will only be scanned when the **Network Drives** check box is also checked. • The drive is a direct automount drive or if the drive is an indirect automount drive, it has to be either already mounted or during the scanning process the scanner has to encounter a symbolic link pointing to a location within the indirect automount drive's directory structure. The following example shows how these three conditions are met: A direct automount DVD drive mounted under/usr/local/cd (where /usr/local is located on a local hard drive) is scanned only when both **Local Drives** and **CD and DVD Drives** check boxes are checked.
Network Drives	Scans the contents of network drives. Note that network drives can be scanned by multiple computers. Use this option with caution. See "Automount (AutoFS) Drives" for detailed information about scanning automatically mounted drives.
Other Drives	Scans drives created using other devices drives (for example, RAM drives). Note that scanning drives created using device drivers can lead to false reporting of files on a computer. Use this option with caution.
SUBST Drives	Scans 'virtual' drives created using the operating system. substitute command - SUBST. This is not normally desirable as a substituted drive can be scanned using both its true drive letter and substituted letter. Use this option with caution.

Directories Tab

The **Directories** tab is used to specify which directories you want to scan when using **Targeted Scan** or **Combined Scan**.

The settings allow you to specify the directories you want to add to the list of directories to scan. For Windows Operating Systems, you also have the ability to scan desktop and Start menu shortcuts.

By scanning only selected directories rather than complete drives, software scanning is made faster.



User interface elements are described below:

Directories from shortcuts (Windows only) group

UI Element (A-Z)	Detail
Desktop	This option will scan the directories that are pointed to by shortcuts on the desktop.
Only use shortcuts to files with these extensions	When checked, only shortcuts that point to files with one of the extensions specified will be scanned.
Start Menu	This option will scan the directories that are pointed to by shortcuts on the Start menu.

Directories from other sources group

UI Element (A-Z)	Detail
File Associations	Select if you want the scanners to add directories containing applications that are associated with various file types (for example NotePad for .txt files) to the list of directories for a targeted scan. This option applies to Windows scanners only.
Java Home	Select if you want the scanners to add the Java Home directory to the list of directories for a targeted scan. This option applies to Windows scanners only. **Note:** If you checked the Enable scanning of Java class files on the Standard Configuration page, this option is selected by default.
Non-Global Zone Root Directories	Select if you want the scanners to add the Solaris non-global (local) zone root directories to the list of directories for a targeted scan. This ensures that all directories used by non-global zones are scanned during the software scanning process. This option applies to Solaris scanners only.
Packaged File Data	Select if you want to make sure that the directories where the files belonging to installed packages are located are added to the list of directories to be scanned. For this option to work, the **Packaged File Data** option must be enabled on the "Hardware Data Page".
Program Files/Applications	Select if you want the scanners to add the standard location for program files to the list of directories for a targeted scan. On Windows, it is the Program Files directory, which is normally located in the root of the Windows system drive (such as C:\Program Files). On Mac OS X, it is the /Applications directory where the applications are installed by default.
Software Utilization	This setting instructs the scanner to include any directories from where used programs are executed. These directories will be included in the list of directories for a targeted scan. This ensures that the scanner collects the file data required for recognition of used applications. This option applies to all scanners.
Windows Services	Select to include directories containing Windows Services for targeted scanning. As the name implies, this option applies to Windows scanners only.

Directories from environment group

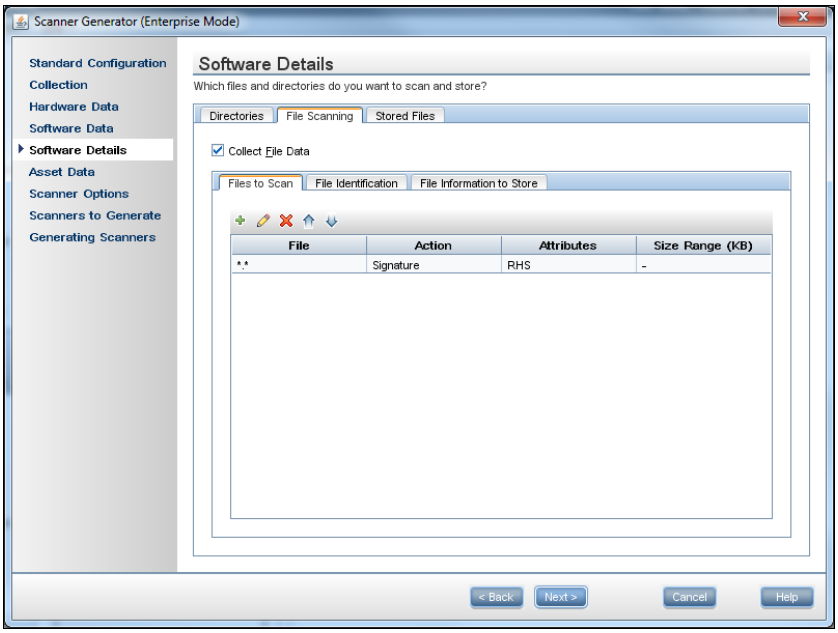
UI Element (A-Z)	Detail
Include directories from these environment variables	If selected, the paths included in the environment variables specified here are also be added to the list to scan. If you specify multiple environment variables, you must separate each name with a semicolon (;).
Shortcuts to excluded drives	This option is available for Combined scans only. • **Scan excluded drives** When selected, this option forces all directories pointed to by shortcuts to be scanned. If not selected , the directories that are located on the drives that are excluded by the drive selection on the Drives and Drive Selection tabs will not be scanned. When selected, the scanners may scan directories on network volumes. This is particularly useful when scanning for software licenses as the scanner will detect files that are part of a network install that is accessible from the machine.
Shortcuts to the network/Used programs launched from the network	This option is available for Targeted Directory Scans only. • **Scan network drives** When selected, this option forces all directories pointed to by shortcuts to be scanned. The scanners may scan directories on network volumes. This is particularly useful when scanning for software licenses as the scanner will detect files that are part of a network install that is accessible from the machine. If not selected, the directories that are located on the drives that are excluded by the drive selection on the Drives and Drive Selection tabs will not be scanned. Usually shortcuts to network drives or network directories from which used programs were executed will not be scanned.

Although the Directories tab page allows you to specify the file systems and directories (known to the Scanner Generator) that you want to include or exclude during scanning, you can override the

settings of the file systems and specific directories and files during software scanning by using the content in the override files. For details on how to add content to the override files, see "Troubleshooting Tab" on page 434.

File Scanning Tab

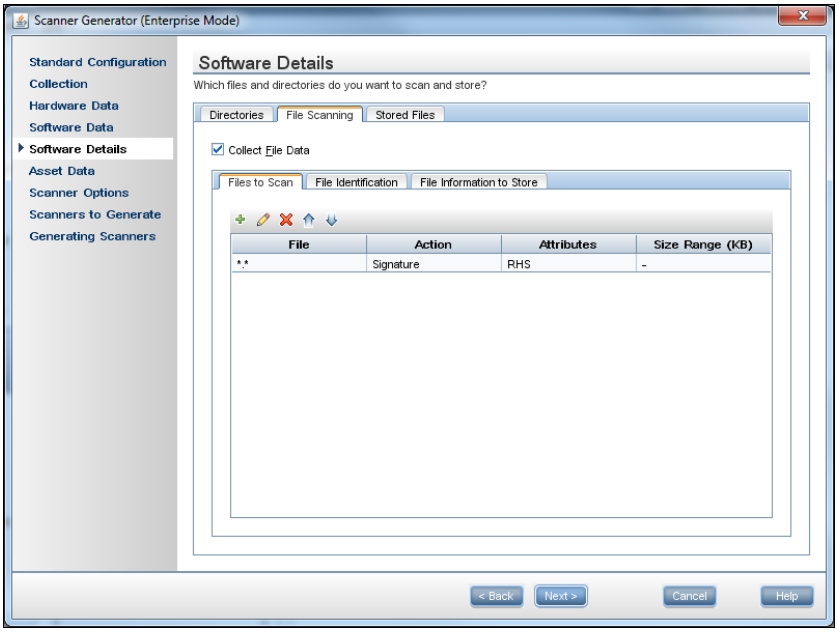
The **File Scanning** tab is used to specify the level of detail for the information collected about files and directories and the methods used to check and identify files.



This tab page contains three sub tabs:

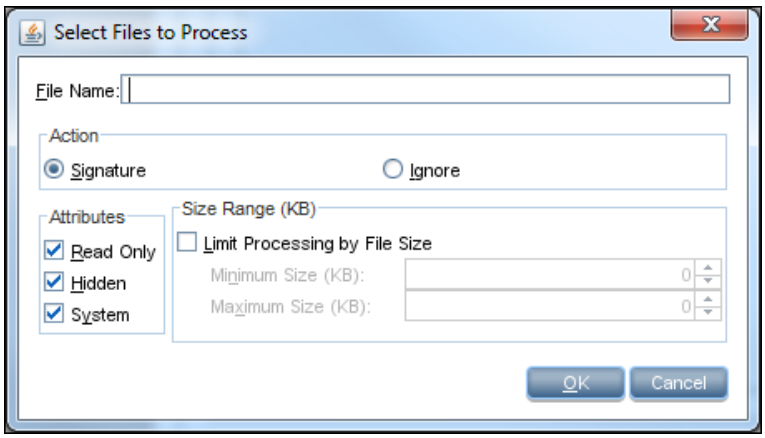
Files to Scan Sub Tab

The **Files to Scan** sub tab is used to specify how much information is collected about files and the checking processes used.



Using the options on this page, it is possible to define which files get their signature calculated and collected, based on criteria such as file extension, attributes or size. See "Timing Considerations".

User interface elements are described below:

UI Element (A-Z)	Detail
	Click to add a new filter. 1. The **Select Files to Process** dialog box is displayed.  2. In the **File Name** box, specify the relevant wildcard file type to process. For example, *.tmp means all files with tmp extension. Multiple specifications, separated with semicolons, are also accepted. 3. In the **Action** group box select one of the following options: ▪ **Signature** Collect file signatures for the specified type of file. See "File Signatures". ▪ **Ignore** Ignore the type of file specified in the File Name box. 4. In the **Attributes** group box, select from the following options as required: ▪ **Read Only** Files with the read-only attribute are capable of being displayed, but not modified or deleted. ▪ **Hidden** Files with the hidden attribute are not normally visible to users. For example, hidden files are not listed when you execute the DOS DIR command. However, most file management utilities allow you to view hidden files. ▪ **System** Files with the System attribute. In general, if a given attribute is not selected, the entry having the attribute will not match, even if the file name does. 5. In the **Size Range (Kb)** group, if required, select the **Limit Processing by File**

UI Element (A-Z)	Detail
	Size check box and specify the maximum and minimum file sizes. Only files within this size range will be processed. 6. Click **OK**.
	Click to edit a filter.
	Click to delete a filter.
	Click to change the order of the filters. See "Importance of the Order of Process Selections ".
Files to Scan List Box	This displays the checking methods used for processing files. You can build up a prioritized list of filters which specify a sequence of checking processes to be used.

- ### Timing Considerations

  Only files that have signatures enabled are opened and are available for further processing. If a copy of the file name is all that is required, use the following command.

  ```
  Ignore *.*
  ```

  The file name, size and attributes may still be picked up in the scan file but no signatures will be calculated. Scanning time will be greatly reduced but because less data is collected, application recognition accuracy may be adversely affected.

- ### File Signatures

  The signature is an ISO checksum (CRC) of the first 8KB of the file. To calculate the signature, the scanner opens the file and reads the first 8KB from it. Collecting signatures helps to establish the file's identity. Two different files rarely have the same signature. Signatures are used by the software recognition in analysis tools to improve software application recognition. Also, only those fields for which signatures were collected can optionally be identified by the scanner (see "File Identification Sub Tab").

- ### Importance of the Order of Process Selections

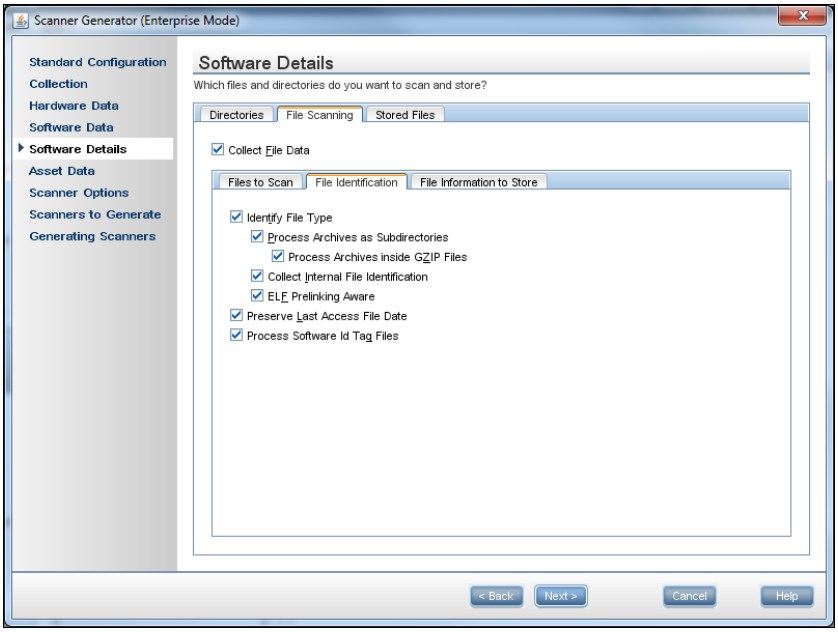
  The order in which process selections occur is important. For example, use Ignore first before making Signature process selections.

  This ensures that the Ignore items are processed first before a file needs to be opened. It may be necessary to ignore certain files, the content of which is constantly changing.

  Examples of files to ignore because of changing content are files that are normally used as swap files, such as pagefile.sys.

File Identification Sub Tab

The **File Identification** sub tab page is used to determine whether the scanner will identify files based on their content.



User interface elements are described below:

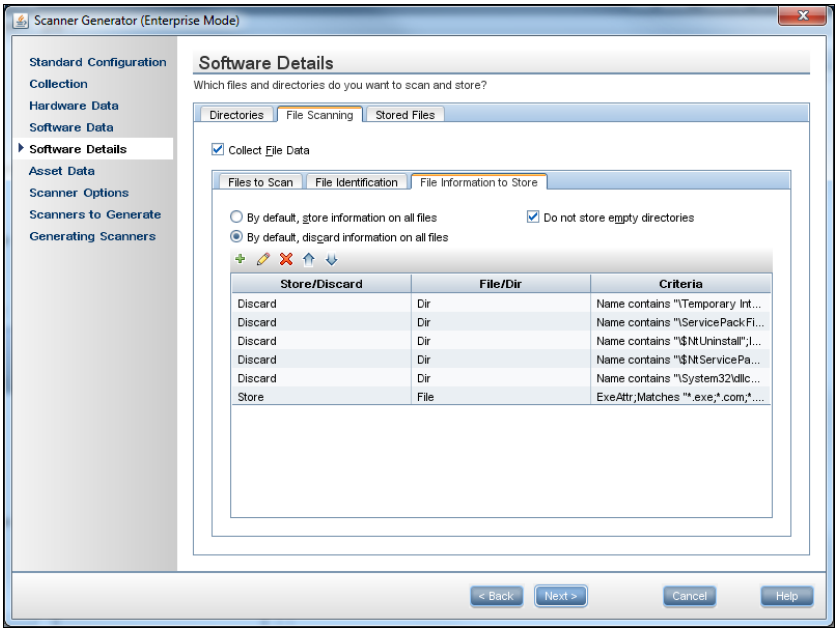
UI Element (A-Z)	Detail
Collect File Data	If selected, the controls on this tab page are activated.

UI Element (A-Z)	Detail
Identify File Type	**Identify File Type** Instructs the scanner to check every file that was selected for signatures to identify all executable and archive files. The scanner can identify LZH, LHA, ZIP, ARJ, ARC and PAK archives. Selecting this enables two further options: • **Process Archives as Subdirectories** Treats archive files as subdirectories and lists the files included in each archive (it does not extract information from within these files). If this check box is not selected, archive files are not scanned for embedded files and directories. A further option is made available: ▪ **Process Archives inside GZIP files** This option enables the handling of archives located in gzip files (such as .tar.gz files). These are tar archives that were compressed using gzip. Checking this option will instruct the scanner to process such archives. • **Collect Internal File Identification** Collects internal file information included in the executable file, for example, version data and legal copyright. • **ELF Prelinking** During software scanning, this option instructs the scanner to check if an executable file has been pre-linked by the ELF Prelinking Utility (prelink). The ELF Prelink Utility is used to speed up loading times of ELF shared libraries and executables by modifying them to reduce the number of the reallocations the dynamic linker needs to do to load them in memory. If this option is enabled, the scanner will calculate the size and signature of the file before it was pre-linked. This is useful for accurate application recognition since the file size and signature are used to perform application matching. However, enabling this option does produce extra overhead during the scan as the scanner needs to run the prelink utility to obtain the original executable file. The prelinked file is not modified by the scanning process; the original file is only reconstructed temporarily in order to collect the size and signature. This is for Linux platforms only.
Preserve Last Access File Date	Collects the Last Accessed time stamp for files (where available). The support for the Last Accessed time stamp varies depending on the Operating System and file system used. When this setting is used on UNIX computers, although the last access time will be preserved, the ctime of the file gets changed. For this reason we recommend that you do not use this setting on Linux, Mac OS X or UNIX computers. When this option is enabled, the XML Enricher can make use of this feature to accurately estimate the time when recognized applications were last executed.

UI Element (A-Z)	Detail
Process Software Id Tag Files	This setting is used to enable or disable the collection of information from software tag files during the software scanning phase. During the hardware detection phase, the information from tag files that are located in the common system location and in the root of the application's installation directory is picked up. The tag files stored in the root of the application's installation directory can be collected only if the application is in a standard package format, or a directory where the application is installed is scanned during the software scanning phase. For more information, see "Software Identification Tags ".

File Information to Store Sub Tab

The **File Information to Store** sub tab is used to define what file details to store in the scan file.



In addition to the default settings, you can define a prioritized list of filters, in a manner similar to that of the **File to Scan** page. Each filter can specify directories or files to be included or excluded from being stored. Each file and directory entry found during scanning is looked up in the list, and the first matching entry determines whether the entry is stored or not.

Multiple filter criteria can be specified on each line if they are separated by a semicolon.

User interface elements are described below:

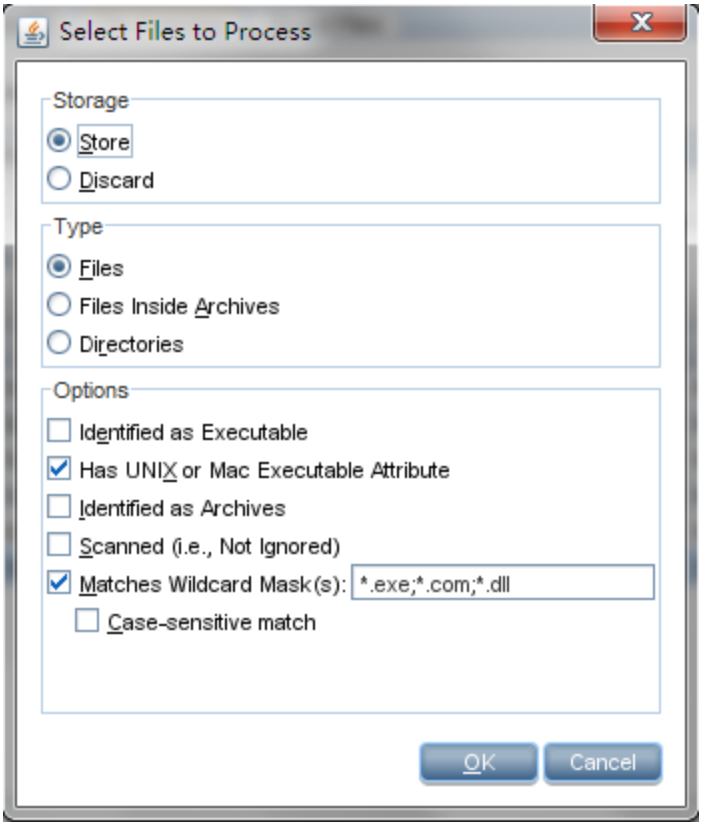
UI Element (A-Z)	Detail
	Click to add a filter criteria. See "How to Select Files to Process".

UI Element (A-Z)	Detail
	Click to edit a filter criteria. See "How to Select Files to Process".
	Click to delete a filter criteria.
	Click to reorder filter criteria.
By default, discard information on all files	If selected, and no other options are specified, then no file data is stored in the scan file.
By default, store information on all files	If selected, and no other options are specified, then information about all files is stored in the scan file.
Do not store empty directories	This option is selected by default. When selected, the scanner discards information about directories that have no files in them. This can include directories that may have files in them, but you have set up the scanner not to scan for these particular types of file.

Note: The options chosen here can dramatically affect both scanning speed and scan file size. Under normal circumstances, the default options are adequate.

How to Select Files to Process

If you clicked  or  in the **File Information to Store** sub tab, the **Select Files to Process** dialog box is displayed.



You may select files to process in one of the following ways:

Including or Excluding Files Based on File Name or Scanned Attributes

1. Choose one of the options **Store** or **Discard** from the **Storage** group box. This determines whether a matching file is stored in the scan file, or discarded. Discarded entries are not available for analysis.
2. Select the **Files** option in the **Type** group box.
3. Check the **Matches wildcard mask(s)** option.
4. Specify a list of wild cards separated by a semicolon (;). For example, when scanning of Java class files is enabled (see "Standard Configuration Page" on page 385), the entry to include *.class files is added to the default configuration. This causes the scanner to only store the information about files with the .class extension.
5. Files can also be stored or discarded based on attributes not known until the file has been scanned. Select from the following in the **Options** group box:
   - **Identified as Executable**

     Files that are identified as any kind of executable (that is, not just .exe and .com files). If Identify file type is not checked this has no effect.
   - **Has Unix or Mac Executable Attribute**

     UNIX allows three different levels of access to a file for three different categories of users: owner, group and other.

Level	Description
Read	View the file or directory without making changes.
Write	Make changes to the file or directory
Execute	Execute the file or list files in a directory.

Checking this option causes the scanner to store or discard files that have executable file access in any of the user categories (namely, owner, group or other.)

- **Identified as Archives**

  Files that are identified as compressed, such as .ZIP, .LZH. If Identify file type is not checked this has no effect.

- **Scanned (i.e. Not Ignored)**

  Includes all files that are not ignored on the File Scanning page.

- **Matches Wildcard mask(s)**

  Includes files that match the wildcards specified here.

- **Case Sensitive Match**

  Includes all files that match regardless of case.

  Note: This option is greyed out if **Matches Wildcard mask(s)** is not selected.

Explanation of the Operation

All file check box options specified are OR-ed together; that is, the entry is considered a match if any of the selected entries match.

The order and content of these options can affect scanning speed and function significantly. If the default is Discard, and a Store - Identified as executable entry is included, all files have to be scanned before the scanner can determine if they are to be discarded.

Including or Excluding Files Based on Files Inside Archives

1. Choose one of the options **Store** or **Discard** from the **Storage** group box. This determines whether a matching file inside an archive is stored in the scan file, or discarded. Discarded entries are not available for analysis.
2. Select the **Files Inside Archives** option in the **Type** group box.
3. Check the **Matches wildcard mask(s)** option.
4. Specify a list of wildcards separated by a semicolon (;). Files discarded in this way are not scanned either, and a wildcard filter can speed up the scanning process.

Including or Excluding Files Based on Directory

1. Choose one of the options **Store** or **Discard**. This determines whether a matching directory is stored in the scan file, or discarded. Discarded entries are not available for analysis.
2. Select the **Directories** option in the **Type** group box.
3. Select from the following in the **Options** group box:

- **Named**

  If this option is selected, the directory name specified in the entry field must match 100% (however, it is not case-sensitive) in order for a match to be established. For windows directories, the directory name must include the drive letter. The path wildcards ***** and **?** can be used for matching the directory name. The root directory \ or / cannot be excluded in this way.

- **Where Name Contains**

  If this option is selected, the name specified in the entry field is a partial string; any directory containing this string in its name is considered a match. Typical examples of entries would be:

  \Private would match any directory where a directory starts with Private.

  Temporary which would match any directory with Temporary anywhere in the name.

- **Include Subdirectories**

  For either of the directory options, there is an option to include subdirectories of matching entries as well. This is particularly useful for discarding entire directory trees, such as recycle folders, temporary Internet files and private directories.

Explanation of the Operation

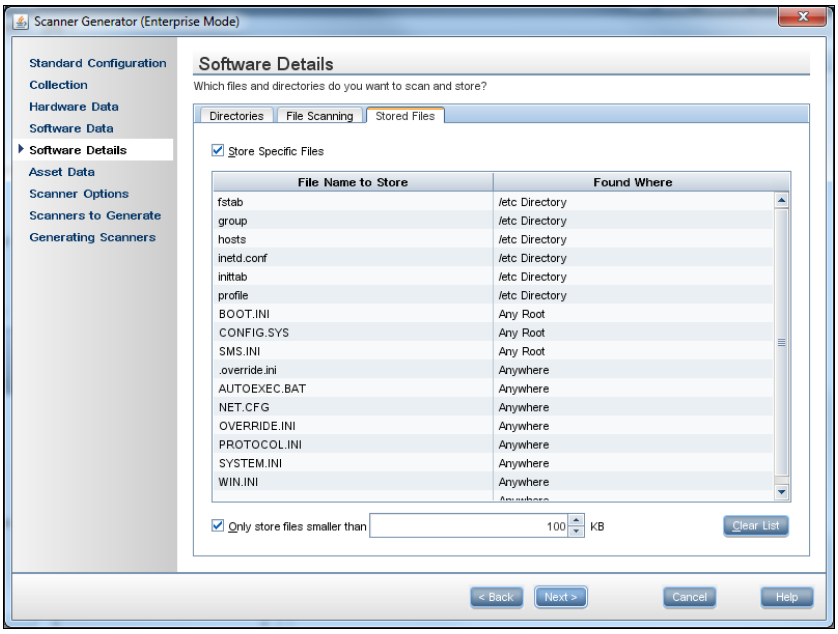
The contents of filtered directories are not stored in the scan file. If the Do not store empty directories option is checked, filtered directories are considered to be empty and are not stored in the scan file either. If this option is unchecked, the filtered directories are represented in the Directories and Files tab of the Viewer application by a no entry icon  .

Directories are filtered prior to scanning (that is, directories that will not be stored are not scanned at all). Consequently, directory filters may speed up scanning.

Stored Files Tab

The **Stored Files** tab is used to allow specific files to be collected and stored (embedded) in the scan file created for each computer scanned. The types of files usually collected are system configuration files. These files can be viewed in Viewer or exported from Analysis Workbench.

If a targeted directory scan selection was made earlier and does not include a specific directory in which a stored file may be found (including the root directory), then any required stored file must be specifically defined here with the full path.



The dialog box shows a list with two columns:

File Name to Store Column

This column displays a default list of system files. The name of the files can include wildcard characters unless a specific directory is used.

For example, collecting the Config.sys file for each computer scanned across a population provides a snapshot of the system configuration for each computer. This enables the analysis and consolidation of system configuration across the computer population.

Other commonly collected files are **Net.cfg**, **Profile.ini**, **AutoExec.Bat**, **Win.ini**, **System.ini** and **Boot.ini**.

The one Universal Discovery specific file included in the list is the override file, which is named **override.ini** on Windows systems and **.override.ini** on UNIX/Mac OS X systems. This is an ASCII file used by the scanner at run-time to store a list of files to be ignored (that is not opened at run-time). See "Directories Tab" on page 399.

The following options are available:

1. **Enabling the Controls on the Stored Files Page**

   Select the **Store Specific Files** check box to enable the controls on this page.

2. **Adding Another File to the list of Files Stored**

   a. Enter a file name at the bottom of the **File Name to Store** column (or overwrite an existing entry)

   b. Select an option from the drop-down list in the **Found Where** column.

3. **Deleting a File From the File Name to Store Column**

   a. Highlight the file name

   b. Press the **Delete** key or right-click on the entry and select the **Delete** option from the shortcut menu.

4. **Clearing Entire List of Files to Be Stored**
   a. Click **Clear List**. A confirmation message is displayed.
   b. Click **Yes** to clear the list.
5. **Limiting Size of Files to Be Stored**
   a. Select the **Only store files smaller than** option.
   b. In the **Kb** box, use the arrows to select a value for the upper size limit or type the value directly into the edit box.

Note: Not restricting the size of files collected could result in very large scan files when large files are collected and stored.

Found Where Column

This column shows the location where the files to be stored can be found.

To change the directories that are scanned to locate the files:

1. Click an entry in the **Found Where** column.
2. Change the setting by selecting an option from the drop-down list.

Setting	Description
Any Root	Only stores the file if it is found in a root directory.
Root of Boot Drive	Only stores the file if it is found in the root of the boot drive.
Anywhere	Store the file wherever it is located.
/etc directory	Only stores the file if it is found in the Unix /etc directory.
/var directory	Only stores the file if it is found in the Unix /var directory.

Specific directory	A specific copy of the file is collected irrespective of whether it is included in the software scan or not.
	For example, the list of specific stored files could be configured to be:
	`C:\Documents\config.txt`
	`Z:\net.ini`
	`/etc/fstab`
	In this case, the scanner will store the config.txt file from the C: drive (when scanning PCs), the net.ini on the Z: drive (if it is available, and only on PCs) and a file named fstab in the /etc directory (when scanning UNIX machines).

Note: Files will only be stored if the directory where the file is located is included in the software scan, unless the specific directory is specified.

Asset Data Page

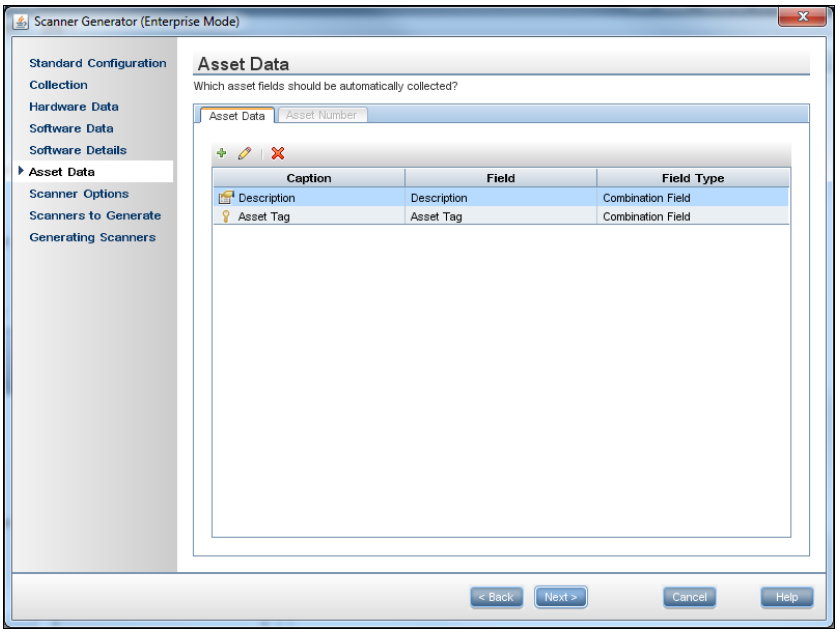
The **Asset Data** page is used to define and set up the asset data collected by the scanners. It has the following tabs:

- "Asset Data Tab"
- "Asset Number Tab" (Only available in Manual deployment Mode.)

Important Information	General information about the wizard is available in "Scanner Generator Wizard".
Wizard Map	The "Scanner Generator Wizard" contains: "Standard Configuration Page" > "Collection Page" on page 387 > "Hardware Data Page" > "Software Data Page" > "Software Details Page" > "Asset Data Page " > "Scanner Options Page " > "Scanners to Generate Page" > "Generating Scanners Page"

Asset Data Tab

The **Asset Data** tab is used to configure customized asset information as each computer is scanned.



A default list of entries is displayed initially. These can be modified to create a custom list of entries. To include other information about the user, see IT Universe Manager in the *HP Universal CMDB Modeling Guide*.

Note: By default, asset fields are not mapped to any of the UCMDB CI attributes, so the data

is only available in the scan files. To map the needed asset fields, you must edit the Universal Discovery mapping script **ParseEnrichedScanFile.py** located in the Inventory Discovery package. There is a commented out sample available in it, that demonstrates how to map the **hwAssetDescription** asset field to the node's description attribute.

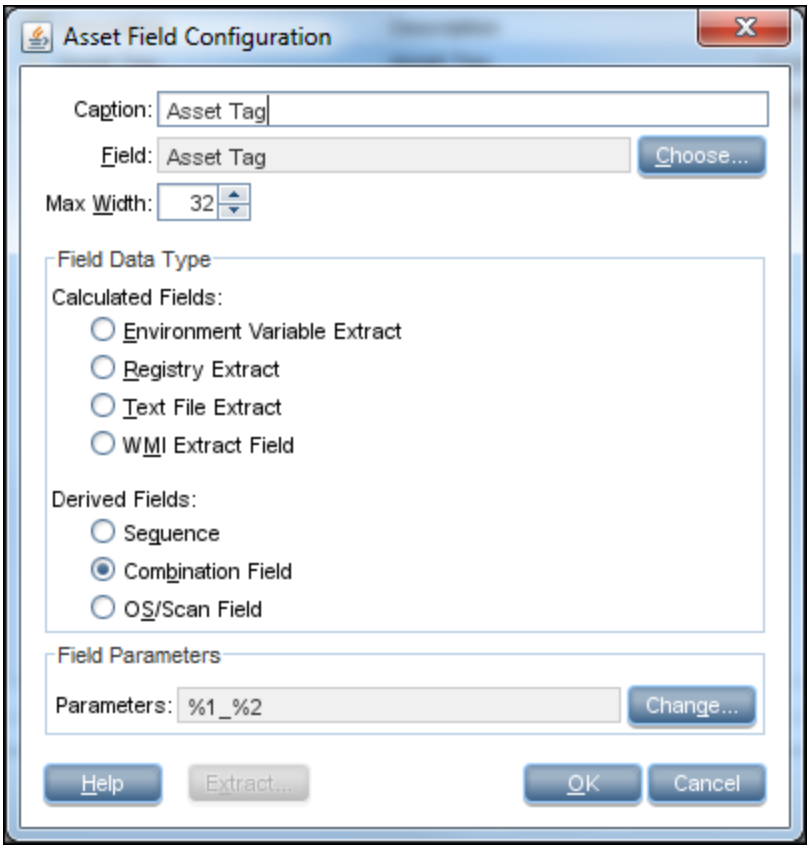
For more information, see "How to Map Scan File Attributes to UCMDB" on page 378.

The **Asset Data** form is made up of a number of rows and three columns. Each row in the form is used to define a piece of asset data and results in one item being collected during the inventory. The form is built up by using a combination of predefined standard fields, user-defined fields and automatic fields. See "How to Set Up an Asset Field".

UI Element	Detail
	Create a new field. The **Choose Field** dialog box is displayed.
	Delete field. You may delete multiple fields by selecting them and then clicking the **Delete** button
	Edit the type and settings for the field. The "Asset Field Configuration Dialog Box" is displayed.

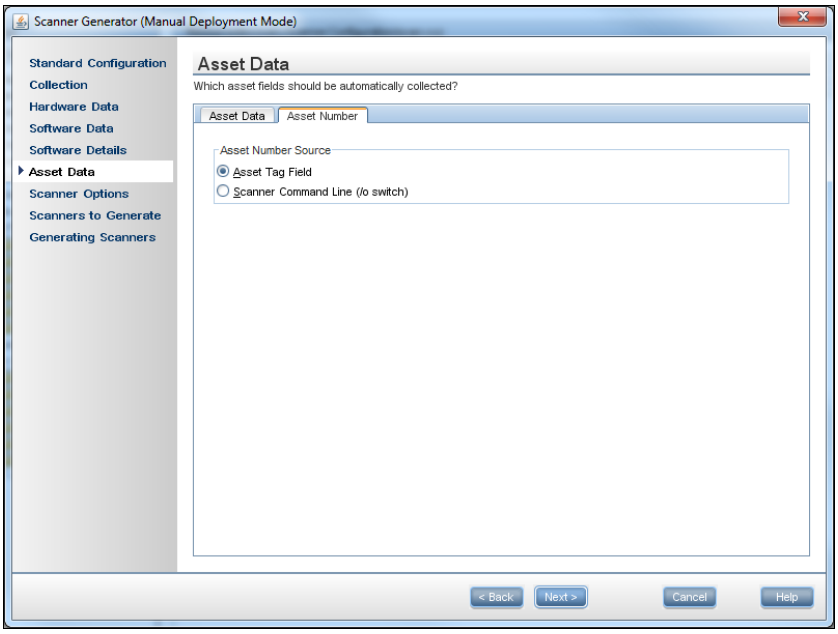
Asset Field Configuration Dialog Box

This dialog box is where the major part of the asset field configuration takes place.



Asset Number Tab

The **Asset Number** tab is used to set options for managing the asset number used to uniquely identify a machine. Each computer that is scanned needs to be identified by a unique tag known as the **Asset Tag**. Asset tags are generally assigned to allow each hardware item to be recorded and identified in an asset management tool, such as Asset Manager. The conventions used depend on the numbering system and asset registering policies adopted by your organization. Ensure that your asset numbers can be reconciled between Universal Discovery and Asset Manager.



Note: In Enterprise Mode the options for selecting the source for asset number source are disabled. The source is always from the **Asset tag** field.

User interface elements are described below:

UI Element (A-Z)	Detail
Asset Tag Field	If selected, this uses the value in the Asset Tag field that was created in the Asset Data tab page. This is usually used as the unique key to identify each computer. When this (the default) is selected and an offsite scan file will be saved, an Asset Tag field must be defined in the Asset Data tab.

UI Element (A-Z)	Detail
Scanner Command Line (/o switch)	An offsite scan file name can also be specified by the -o: command line option. This overrides the scan file name (as well as the path, if specified). To configure this, select the **Scanner Command Line (/o)** option. The scan file name is taken from the command line. This is entered using the -o: command line option when the scanner is started, using the name specified. For example: `Scanwin32-x86 -o:FP00017`

Scanner Options Page

The **Scanner Options** page is used to set options for controlling the behavior of the scanner during the usual scanning process and under exception conditions, as well as options for saving the inventory results.

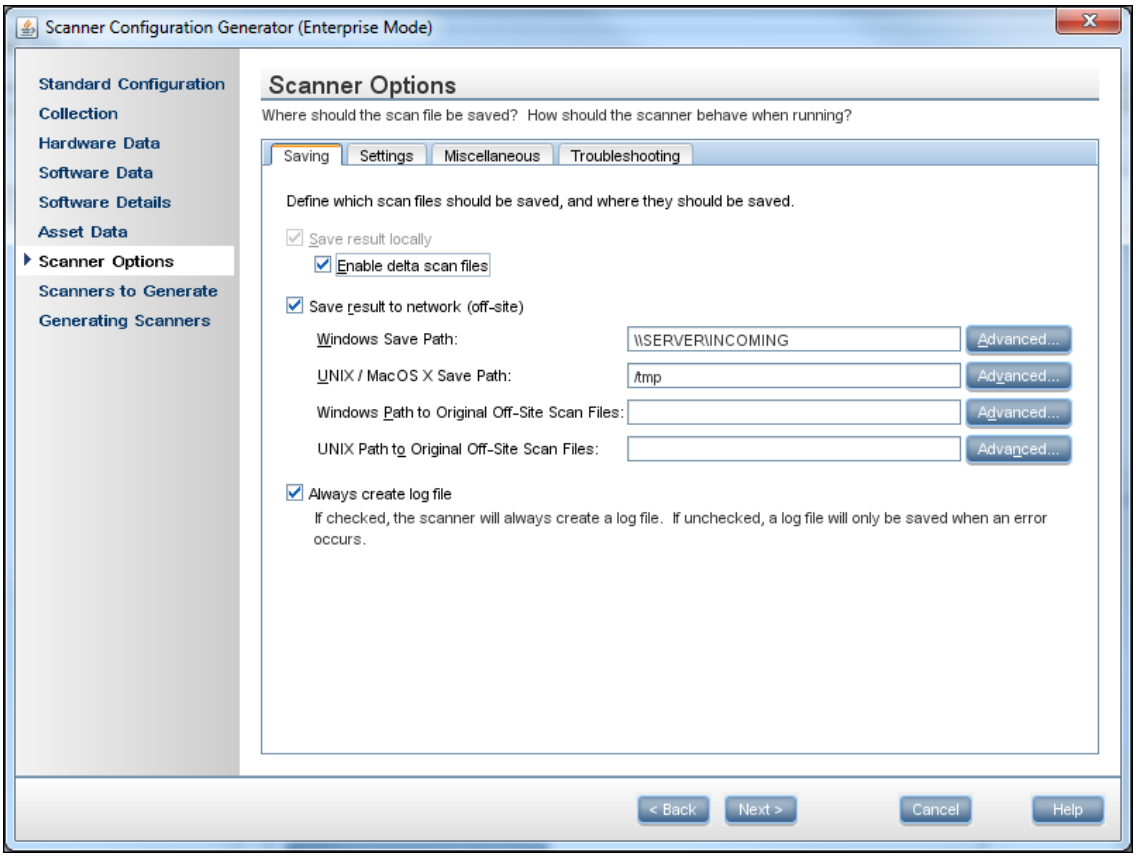
The **Scanner Options** page has the following tabs:

- "Saving Tab"
- "Settings Tab"
- "Miscellaneous Tab"
- "Troubleshooting Tab"

Important Information	General information about the wizard is available in "Scanner Generator Wizard".
Wizard Map	The "Scanner Generator Wizard" contains: "Standard Configuration Page" > "Collection Page" on page 387 > "Hardware Data Page" > "Software Data Page" > "Software Details Page" > "Asset Data Page " > "Scanner Options Page " > "Scanners to Generate Page" > "Generating Scanners Page"

Saving Tab

The **Saving** tab page is used to set options for saving the inventory results.



Note: For **Enterprise Mode** some of the options are pre-set to optimal values and cannot be changed.

Saving Local and Offsite Scan Files

The scanners can save two scan files per scan:

- **Local scan file** - Saved to a local directory.
- **Offsite scan file** - Saved to a specified output directory, with its name being derived from the value in the Asset Tag field specified as the asset number.

The saving of local scan files cannot be disabled in Enterprise Mode (the option is on and is grayed out).

In Manual Deployment Mode, both of these scan files (local and offsite) are saved by default, however, one or the other can be disabled.

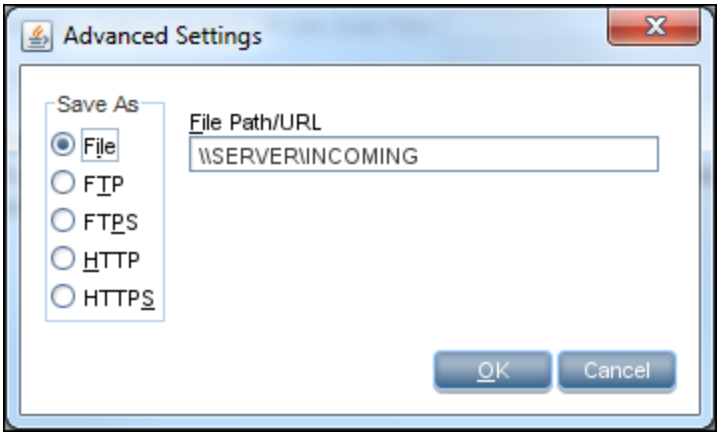
User interface elements are described below:

UI Element (A-Z)	Detail
Always create log file	The log file stores progress messages for scanner hardware detection, indicates what directory data is scanned, how long the software scanning took, and contains the status of the scan file saving. A log file is always created if this option is selected (which indicates the successful completion of the scan if no errors are encountered). Otherwise, a log file is only created if an error is encountered. Depending on the saving options chosen, the log file is saved to the following locations: • The same location as the local scan file. • The same location as the offsite scan file (if an offsite location has been specified). • In the scan file itself (as a stored file). The name given to the log file is the same as the name of the scan file. For example, if the scan file is called: **XSF014.xsf**, then the log file generated will be called: **XSF014.log**.

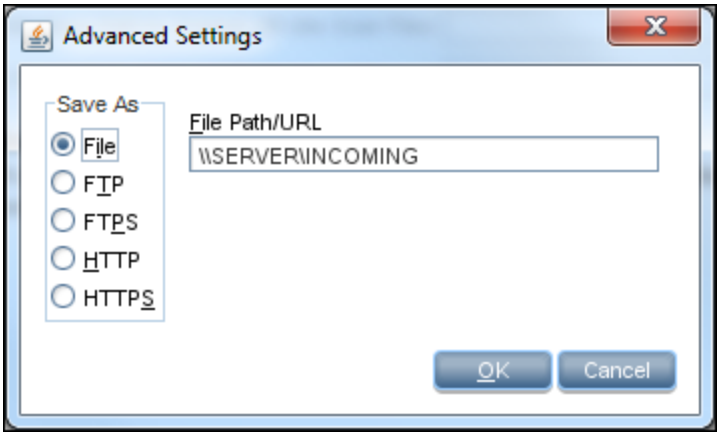
UI Element (A-Z)	Detail

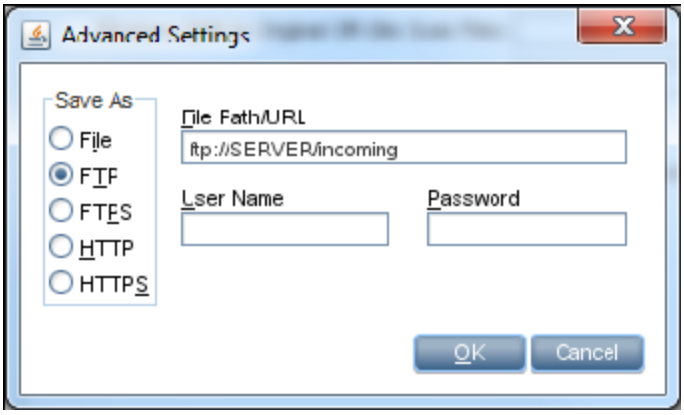
Enable delta scan files	**Enabling Delta Scanning**
	This option can only be enabled if a local scan file is saved. When delta file scanning is enabled, the scanner first saves the complete scan file copy offsite by copying the local scan file.
	
	Instead of sending a full scan file to a server after every scan, the scanners calculate the difference (the delta) between the last full scan and the current one - and transfer just this data. This can dramatically reduce the amount of network bandwidth used when using Universal Discovery. By default, delta scanning is enabled.
	
	The XML Enricher re-assembles the full scan files based on the previous scan and the delta scan. No other Universal Discovery component uses the delta scan file. The re-assembled scan can however, be used in Viewer and Analysis Workbench.
	
	How to Setup the Scanner to Handle Delta Scan Files
	
	Only possible in Manual Deployment Mode.
	
	In Manual Deployment Mode for the delta scan file processing in the XML Enricher to work correctly, ensure that you do the following:
	
	1. Configure the scanner to save results to the XML Enricher incoming directory. This directory can be found in the following location on the Data Flow Probe by default:
	
	`C:\hp\UCMD-B\DataFlowProbe\runtime\xmlenricher\Scans\incoming`
	
	Create a share on the Data Flow Probe to share this disk and specify its UNC path in the Save result to network (offsite) field on this page. See the next section for more information about offsite saving.
	
	2. Set the **Path to original offsite scan files** to the **Original** directory. This directory can be found in the following place by default:
	
	`C:\hp\UCMD-B\DataFlowProbe\runtime\xmlenricher\Scans\original`
	
	Create a share for this directory and specify its UNC location in the **Path to original offsite scan files:** field to do this. The format for the UNC path is:
	
	`\\Servername\ShareName\path\`
	
	For example:
	
	`\\DataFlowProbe\ScansOriginal`

UI Element (A-Z)	Detail
Save result locally	This option determines whether the scan file is saved to the local machine. By default, the local scan file is called **local$.xsf**. This default name can be changed by using the -l scanner command line option. The Windows scanner uses the **Hewlett-Packard\Universal-Discovery** subdirectory of the application data directory for all users. The location of this directory varies. For example, on Windows XP installed on C:\, it could be: `C:\Documents and Settings\All Users\Application Data\Hewlett-Packard\Universal-Discovery`

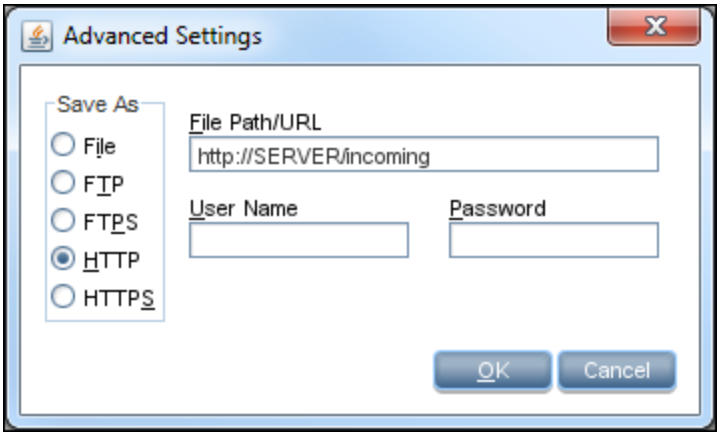
UI Element (A-Z)	Detail
Save result to network (offsite)	Selecting this option saves the scan file to remote (offsite) disk (such as floppy disk or network drive). The **Offsite Save Path** can take the following four types of values: Save to a Normal File Path **To save to a normal file path:** 1. Click the **Advanced** button next to the path you want to configure. The **Advanced Settings** dialog box appears.  2. Select the **File** option and enter the path in the **File Path/URL** field. The full path name (beginning with the drive letter) must be specified. For example: `c:\Inventory\Scans` 3. Click **OK** to return to the **Saving** tab page. Save to a UNC Path A UNC path can be entered as the offsite save path. **To save to a UNC path:** 1. Click the **Advanced** button next to the path you want to configure. The **Advanced Settings** dialog box appears.

UI Element (A-Z)	Detail

	
	2. Select the **File** option and enter the **UNC path** in the **File Path/URL** field.
	The format for the UNC path is:
	`\\servername\sharename\path\`
	For example:
	`\\DataFlowProbe\ScansIncoming`
	The specified UNC path must have write access. Do not specify a file name here.
	The offsite save location can be overridden by using the -p: or /p: command line option. For example:
	`Scanwin32-x86 -p:C:\Scanners\`
	A UNC path can also be entered as the argument to this option. The format for the UNC path is:
	`\\servername\sharename\path\`
	For example:
	`Scanwin32-x86 -p:\\DataFlowProbe\ScansIncoming`
	In Windows, if the UNC name specified is visible to the machine, the scan file will be saved to the specified location, even if it is not mapped to a drive letter.
	On UNIX and Mac OS X machines, the UNIX/Mac OS X save path is used instead, allowing UNIX-style syntax for specifying directories to be used. On UNIX/Mac OS X, do not use drive letters, and the save path must instead start with '/' (root) and point to a directory writable by the scanner.
	3. Click **OK** to return to the **Saving** tab page.
	Save to an FTP or FTPS URL
	The scanners can save to any FTP or FTPS server.

UI Element (A-Z)	Detail
	To save to an FTP or FTPS server: 1. Click the **Advanced** button next to the path you want to configure. The **Advanced Settings** dialog box appears.  2. Select the **FTP** or **FTPS** option as appropriate. 3. Enter the FTP or FTPS path in the **File Path/URL** field, and enter a User Name (and Password if one is to be supplied). 4. Click **OK** to return to the **Saving** tab page. When an FTP location is specified with the -p scanner command line option, the User Name and Password can be encoded into the URL as follows: `ftp://user:password@host:port/dir` For detailed information, refer to the description of `-p:<path>` in "Command Line Parameters for Scanners". Save to an HTTP or HTTPS URL The scanners can save to a Web server if one has been configured to allow writing to a particular directory. **To save to a Web server using HTTP or HTTPS protocols:** 1. Click the **Advanced** button next to the path you want to configure. The **Advanced Settings** dialog box appears.

UI Element (A-Z)	Detail

	
	2. Select the **HTTP** or **HTTPS** option as appropriate.
	3. Enter the HTTP or HTTPS path in the **File Path/URL** field, and enter a User Name (and Password if one is to be supplied).
	4. Click **OK** to return to the **Saving** tab page.
	HTTP Saving for Apache and IIS Web Servers
	The Web Server needs to be configured to allow execution of the PUT command. Usually, by default web servers are set to enable POST and GET commands. You will need to ensure that if you are using HTTP saving that the PUT command is enabled in the directory.
	The following is a quick description of what you would have to enable for HTTP saving on both IIS and Apache.
	Setup of Apache 1.3
	If you are using basic authentication:
	In the bin directory run:
	`htpasswd -c "<path>\htpass" Username`
	You will need to put the following in the **htaccess** file of the directory that you intend to save in:
	`PUT_EnablePut On`
	`PUT_EnableDelete Off`
	`AuthType Basic`
	`AuthName "Write" AuthUserFile "<path>\htpass"`
	`Require user Username`
	Download the **mod_put.so** file and put it into the modules directory.

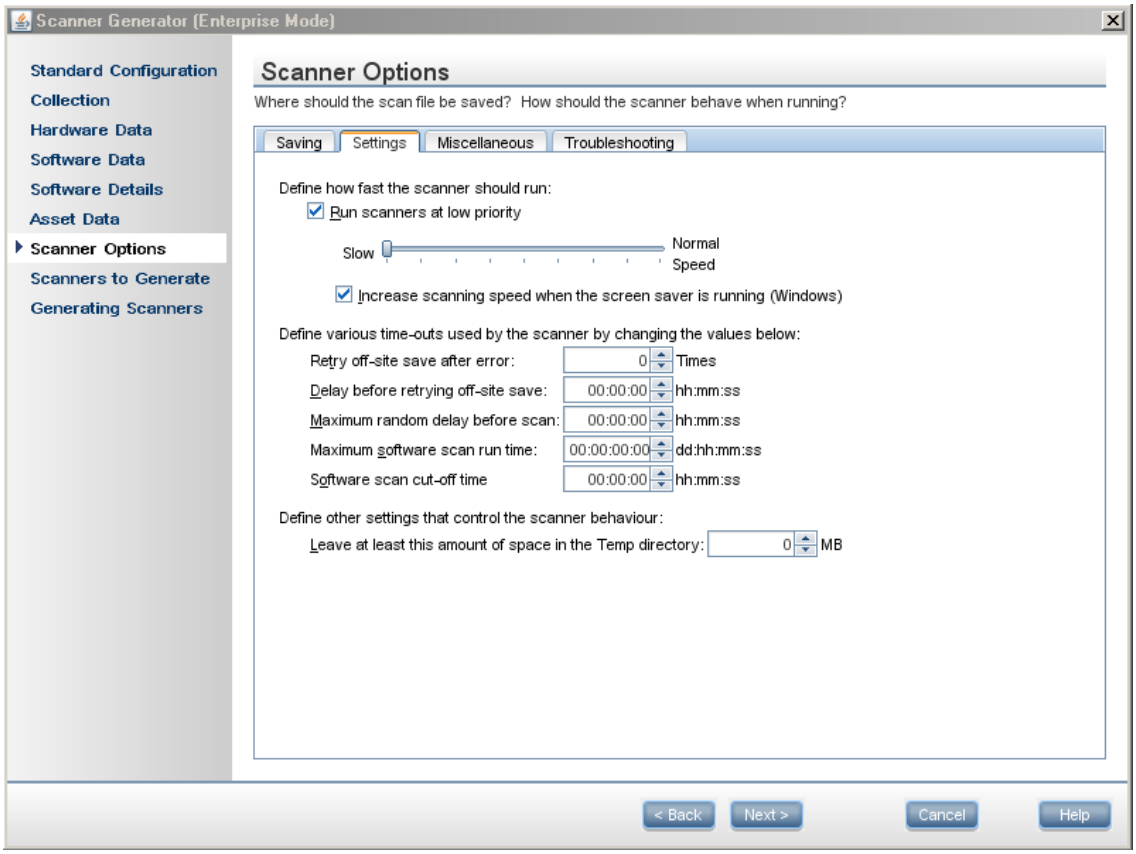
UI Element (A-Z)	Detail

	Enter the following into the **httpd.conf** file:
	`LoadModule put_module modules/mod_put.so`
	Setup of Apache 2.x
	• As **mod_put** is Apache 1.3 specific and is no longer available in Apache 2.x, the **mod_dav** should be used instead to provide the HTTP PUT capabilities
	• Make sure that mod_dav is loaded. For example, the following line in the Apache web server configuration can be used to enable it:
	`LoadModule dav_module modules/mod_dav.so`
	• Then for a particular location you can enable mod_dav with the following setting:
	`DAV On`
	Refer to the documentation for Apache's mod_dav module for more details.
	Setup for IIS
	Check the option that allows writing to the desired save directory. Ensure that you have given write access to the Username and Password that you plan on adding to the scanner's http save path.

Note: By default both the Incoming and Original directories of the XML Enricher are shared via HTTP. This can be changed to HTTPS by adjusting the Data Flow Probe configuration. See "Processing Scan Files"

Settings Tab

The options on the **Settings** tab of the Scanner Options page are used to control the behavior of the scanner as it scans each computer, and how it interacts with users. By default, the scanner is made to run with the lowest priority, but will go to full speed when the screen saver is active.



User interface elements are described below:

Defining How Fast the Scanner Should Run

UI Element (A-Z)	Detail
Increase scanning speed when the screen saver is running (Windows)	Only available if **Run scanners at low priority** is selected. This option allows the scanner to run at an increased speed when a screen saver is enabled. When selected, the scanner runs slower. It increases its speed to normal when it detects that the screen saver is running. As soon as the screen saver disappears, the scanner runs slower again.

UI Element (A-Z)	Detail
Run scanners at low priority	The scanners can be set to run at slower than normal speed, so that they do not impact on the users work. Use the slider control to specify how slow or how fast the scanner will run. When selected, PC-based scanners allocate CPU resources less aggressively and wait much longer between each file scanned. In UNIX and Mac OS X, the scanner performs a renice of itself to run at a lower priority.

Define various time-outs used by the scanner by changing the values below

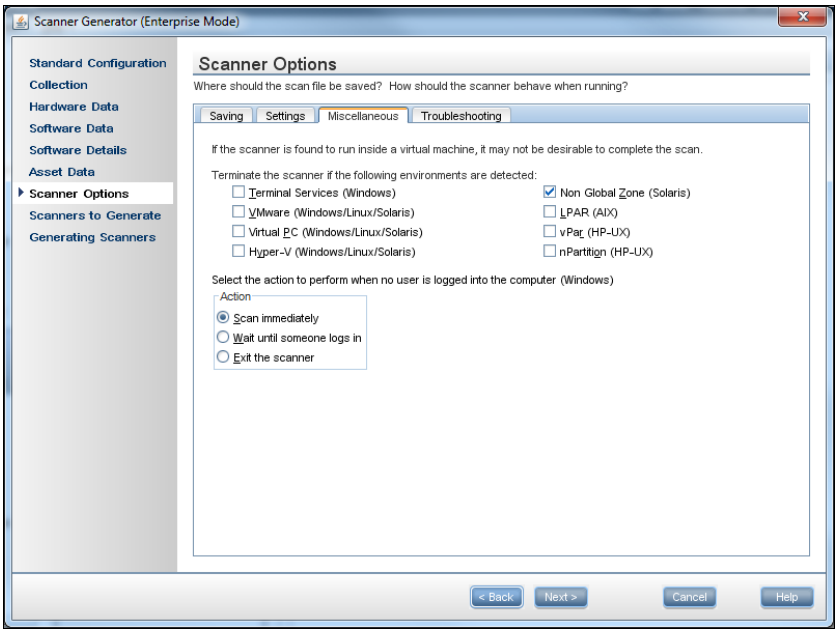
UI Element (A-Z)	Detail
Delay Before Retrying Offsite Save	The scanners will wait for the time specified here before retrying the offsite scan file saving, if an error previously occurred in this process.
Maximum Random Delay Before Scan	This setting is applicable to the Windows scanner only. The scanner can wait for the amount of time specified here before doing anything on the machine. The default setting for this is 00:00:00 with a maximum allowed value of 23:59:59 If the scanner is launched via a login script, using this option allows the saving of scan files to be spread over a longer period to avoid overloading the network at busy periods. For example, in the morning, when all users come to work, power up their computers, and start the scanners at approximately the same time.
Maximum Software Scan Run Time	Sets the maximum amount of time that the scanner runs. This setting is useful in protecting the scanner from scanning large volumes which were inadvertently included into the software scanning scope. If the scanner reaches the configured maximum time, it saves the scan files with the partial software details recorded right to that moment, and exists with the exit code 7. **Default:** 0 (No limit applies.)
Retry Offsite Save After Error	The scanner attempts to retry the offsite scan file saving if an error occurs the number of times specified here.

UI Element (A-Z)	Detail
Software Scan Cut Off Time	Sets the local time of the day on the managed computer (using the 24-hour clock) when the software scan has to stop. This setting is useful as a safety feature in those cases when there are certain periods of the day during which the scanning must not be performed. When the cut-off time is reached, the scanner saves the scan file containing the partial software inventory, and exits with the exit code 7. This option needs to be used with great care to avoid incomplete results to be saved regularly. The inventory has to be scheduled early on during the day to allow the scanner to complete the full software inventory. **Default**: 00:00:00 meaning the scan is not stopped. If, for example, you want to stop the scan before midnight, type 23:59:59.

Define other settings that control the scanner behaviour

UI Element	Detail
Leave at least this amount of space in the Temp directory	Sets the amount of the disk space (MB) the scanner reserves to be available in the Temp directory before failing. During software scanning the scanner stores the partial software scan result in the temp directory. If the amount of disk space available in the Temp directory is too low, normally the scanner will use all the available space and when none is left, it fails. However, during the time when no Temp space is available, other processes running on the system may start failing as well. This setting ensures that at least the specified amount of space is left reserved for other processes to continue their normal operation. For example, if 5MB is specified, the scanner will use the space in the Temp directory until there is 5MB of free disk space left, and when this limit is reached, the scanner will fail. **Note**: This number must be an integer. **Default**: 0 meaning no limitation.

Miscellaneous Tab



User interface elements are described below:

Terminate the scanner if the following environments are detected

When the scanner is run inside a virtual environment, you may not want a full software scan to take place, because this would scan the server for every virtual machine. The following settings can instruct the scanner to exit without doing any processing with a special error level 20, allowing a script that launches the scanner to handle this situation and launch another scanner tailored for the virtual environment, if required.

UI Element (A-Z)	Detail
Hyper-V (Windows/Linux/Solaris)	If selected, the scanner terminates if launched in a Microsoft Hyper-V's virtual machine.
LPAR (AIX)	If selected, the scanner terminates if launched in an LPAR partition on the AIX operation systems.
Non Global Zone (Solaris)	If selected, the scanner terminates if launched in a non global zone on the Solaris operating systems supporting zones.
nPartition (HP-UX)	If selected, the scanner terminates if launched in an nPartition partition on the HP-UX operation systems.
Terminal Services (Windows)	If selected, the scanner terminates if launched in a Windows terminal services session.
Virtual PC (Windows/Linux/Solaris)	If selected, the scanner terminates if launched in a Virtual PC's virtual machine.

UI Element (A-Z)	Detail
VMware (Windows/Linux/Solaris)	If selected, the scanner terminates if launched in a VMware virtual machine.
vPar (HP-UX)	If selected, the scanner terminates if launched in a vPar partition on the HP-UX operation systems.

Select the action to perform when no user is logged into the computer (Windows)

This option is for the Windows scanner only.

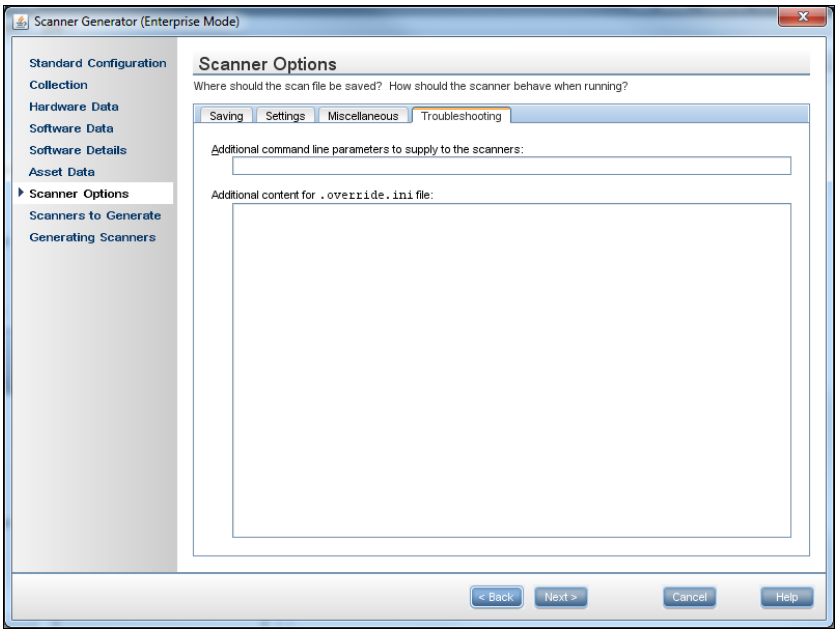
UI Element (A-Z)	Detail
Exit the scanner	The scanner simply exits without scanning the computer.
Scan immediately	Forces the scanner to run under the local system account. However, it will not be able to collect the environment information for a particular user. The environment settings for the local system account will be detected. Also any program running under the local system account does not have access to network resources, so the scanner will not be able to access any files or directories on the network.
Wait until someone logs in	This instructs the scanner to wait until an interactive user logs into the system. When this is detected, the scanner impersonates this user and executes using this user's account. This allows the scanner to collect environment information for the user. However, this setting is not suitable for standalone servers where interactive users rarely log in.

Note:
In **Enterprise Mode** The Windows scanner is launched via the Universal Discovery agent or by agentless NTCMD protocol. The agent itself, or the NTCMD protocol component, runs as a Windows service under the LocalSystem account. However, the scanner always tries to impersonate the account of the currently logged in user in order to collect the required network, environment, and other configuration information for the user. This setting specifies the scanner behavior when no user is logged in at the time the scan is scheduled.

In **Manual Deployment Mode** the scanner runs under the account of the currently logged in user, so normally these settings do not apply. They may only take effect when the scanner is launched by a software distribution tool that can run it under the LocalSystem account. In this case, the above logic for Enterprise Mode applies.

Troubleshooting Tab

The **Troubleshooting** tab is used to set up additional troubleshooting options for the scanners.



User interface elements are described below:

Additional command line parameters to supply to the scanners

You can specify additional content for the override files here. Although the options for the scanner are normally set using the Scanner Generator, it may be necessary to change some settings to allow better operation on some machines. The operation of a scanner can be modified with the use of the various command line parameters.

Additional file scanning configuration specified in the override.ini (Windows) file and the .override.ini file (UNIX/Mac OS X) can be entered in this field. The content specified here is processed by the scanner before processing the content of the override file (if available on the system where the scanner runs).

Additional content for .override.ini file

You can override the settings of the file systems, directories and files during the software scanning process by specifying additional settings in the override file. As indicated, on Windows systems, the name of this file is override.ini. On UNIX and Mac OS X systems, the name of this file is .override.ini. The override file must be located in the same directory as the scanner executable.

File Systems

Because it is always possible, particularly on UNIX and Mac OS X systems, that some file systems are not in the list, you can create a file where you can specify any additional names of file systems that you want to include or exclude during scanning.

You can also specify names of existing file systems in case you want to change the inclusion/exclusion of such file systems after the scanner has been generated.

The format of the file is as follows:

```
[include]
fs=<name of a file system>
[exclude]
fs=<name of a file system>
```

There can be several **fs** entries in each section.

For example, to ensure that all **afs** mount points are scanned, and that **nfs** and **swap** volumes are not, create the override file with the following contents and place it in the same directory as the scanner prior to running:

```
[include]
fs=afs
[exclude]
fs=nfs
fs=swapfs
```

Note:

- The name of the file, the sections and the files systems are case-sensitive
- For the feature to work correctly, the override file must be present in the directory in which the scanner resides.

Directories and Files

The override file can also be used to exclude specific directories or files from being scanned without regenerating the scanner.

Note: Files can only be excluded; they cannot be included.

To make use of this file, add one or more

```
dir = <name>
```

or

```
file = <name>
```

entries to the `[exclude]` section of the override file. Excluded directory names must be fully qualified. Excluded file names can contain wild cards.

Note: When excluding files using the override file, the scanner may still store information about the excluded files in the scan file. Adding file entries to the override file ensures that the file will not be opened for any reason, so no file identification, signatures, or archive processing will happen for excluded files.

Example 1

Exclude a specific file system, two directories and all files with **exe** extension.

```
[exclude]
fs=autofs
dir=/temp
dir=/etc
file=*.exe
```

Example 2

This runs a scan without software on a Windows machine.

```
[exclude]
fs=FAT
fs=NTFS
```

Example 3 Virus Warning

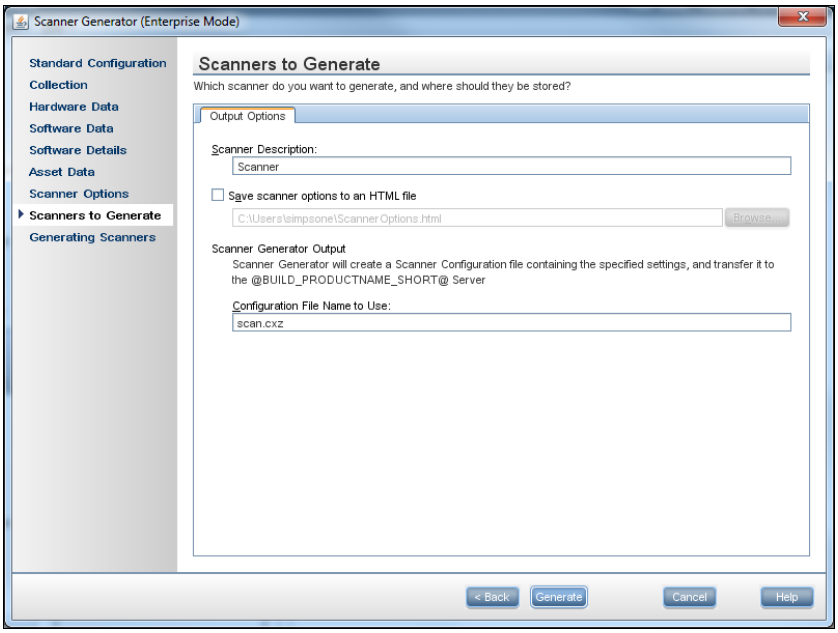
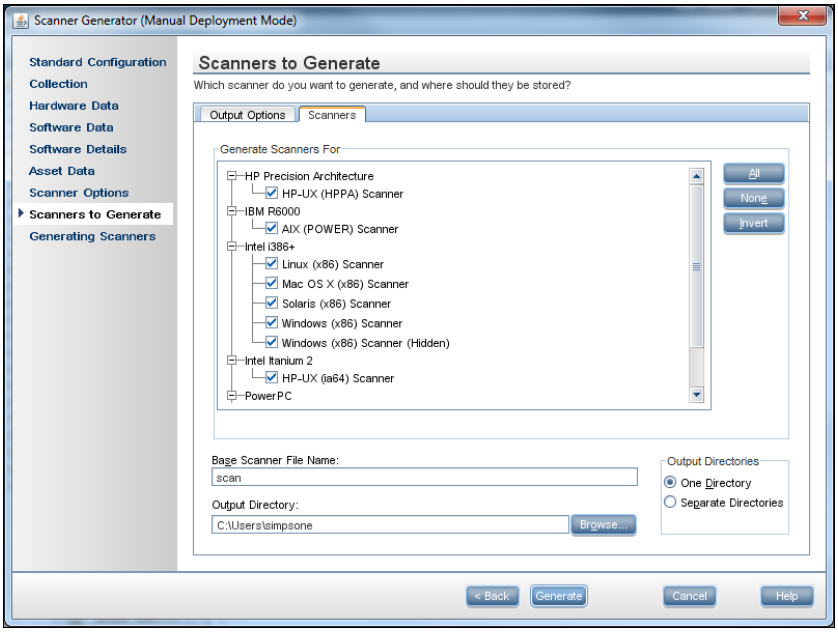
Since the scanner opens files on the computer, if real-time antivirus software is in operation, it may detect a virus being present in a file.

Depending on the virus product being used, actions will have been defined to deal with an encountered virus. Some will try to deal with the problem and immediately disinfect the file. Others will try to move the infected file to a quarantine directory and rename its file extension. In this case, the quarantine directory may be scanned by the scanner later during its scan.

To prevent this from happening, use the override file with `*.vir` specified for exclusion (where `.vir` is a typical quarantine file extension). Check the specific virus product to find the extension for this type of file.

Scanners to Generate Page

The **Scanners to Generate** page is used to specify which scanners to generate and where they will be stored.

Important Information	General information about the wizard is available in "Scanner Generator Wizard". In Enterprise Mode only the **"Output Options Tab"** is displayed.  In Manual Deployment Mode, both the **"Output Options Tab"** and **"Scanners Tab"** are displayed. 
Wizard Map	The "Scanner Generator Wizard" contains: "Standard Configuration Page" > "Collection Page" > "Hardware Data Page" > "Software Data Page" > "Software Details Page" > "Asset Data Page " > "Scanner Options Page " > "Scanners to Generate Page" > "Generating Scanners Page"

Output Options Tab

The **Output Options** page is used to set up scanner descriptions, save the configuration to an HTML file if required, and, for Enterprise Mode only, name the configuration (**.cxz**) file.

Having a scanner description is very useful for change control if different scanners are being developed for different circumstances. It is useful for documentation purposes, to have a file with the scanner's configuration stored in a file. If this step is missed, then load the scanner or a scan file derived from it into Scanner Generator and produce the documentation from this

User interface elements are described below:

UI Element	Detail
Scanner Description	Enter a description to identify the scanner. For example: **Standard PC Inventory – May 18, 2012** The scanner description is saved in the scan file as the **hwScannerDescription** hardware field and subsequently in the UCMDB in the description attribute of the inventory_scanner CI.
Save scanner options to an HTML file	To save to an HTML file, select this option, and specify the path and file name to which the scanner options will be saved to. Selecting this instructs the Scanner Generator to output an HTML file containing a complete listing of all settings defined elsewhere in the program. The HTML file cannot be used by the Scanner Generator, but is intended for user/internal documentation purposes.

Example of the ScannerOptions.html File

You can look at a ScannerOptions.html file using an Internet browser such as the Microsoft Internet Explorer. The following shows the first few sections that you will find in the file:

Scanner Configuration

General

- Product Version: 10.00 (01 Oct 2011)
- Scan File Version: 7.60 (2011-10-01 15:56:52)
- Platform: Win32 Scanner
- Description: Scanner
- Types of Data Collected: Software, Hardware, Asset Data
- Default Scan File Name: DEFAULT

Hardware and Configuration

- Excluded Hardware: Compaq Asset Tag, Device Drivers, Installed Applications (WMI)

Software Data

- Allow scanner command-line to override this selection: Yes
- Drives: Default
- Drive Selection: Local hard disk, File, Unknown
- Filesystem Types: FAT, Device Driven, HPFS, NTFS, ext, ext2, ufs, tmpfs, vxfs, hfs, hfs Extended, jfs, ext3, DVD-ROM

Directories

- Environment Variables: PATH;LIBPATH
- Options: Scan subdirectories
- Windows Only
  - Shortcuts: Start Menu, Desktop
  - Shortcut Extensions: exe;com;bat;cmd;ocx;dll
  - Windows Services: Yes
  - File Associations: Yes
  - Software Utilization: Yes

Naming the Configuration (.cxz) File

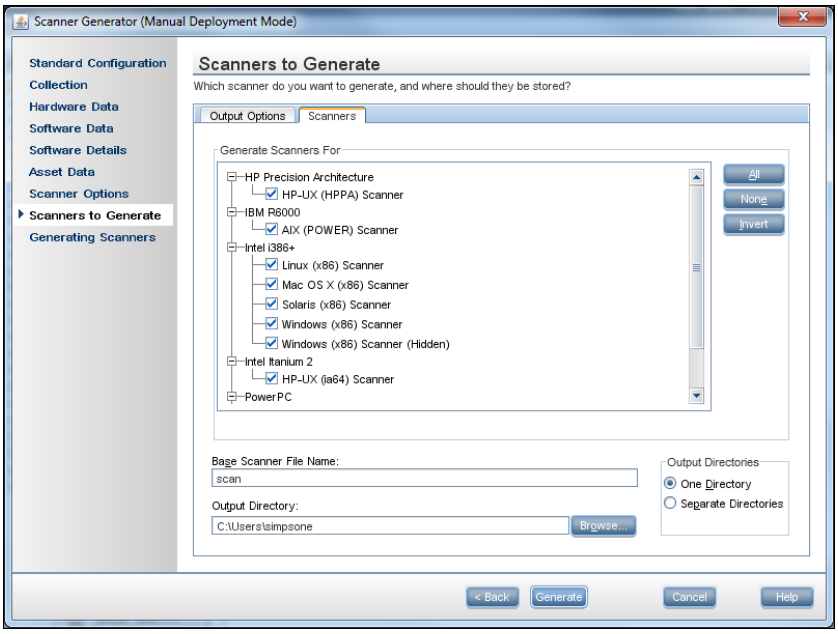
In Enterprise Mode the configuration file is saved on the UCMDB database (resources for the InventoryDiscovery adapter) as well, using the same file name as the copy specified in the Configuration file name to use field.

The configuration file is a compressed XML file containing the settings for the scanner you are currently configuring.

When the scanners are used in the Enterprise Mode, they read the configuration from a separate configuration file. This is a binary file with a **.cxz** extension. The typical size of the configuration file is about 3KB. As the size of the configuration file is significantly smaller than the size of the complete scanner, a separate scanner configuration is useful for repetitive inventory collection when the configuration of the scanner has been altered. In this case only a small configuration file is delivered to the user's computer to run with the original scanner instead of delivering the entire new scanner.

Scanners Tab

The **Scanners** tab is only available in Manual Deployment Mode. It is used to select which of the scanners to generate.



How to Select Which Scanners to Generate

The scanners are presented in a tree view in the **Generate Scanners For** list box.

As the mouse pointer passes over a scanner in the list, the status bar (just below the list box) displays the following information for that particular scanner:

- Whether the scanner is enabled (the check box next to it is checked).
- The full scan file name of where - on the local computer that runs the browser session - the scanner will be generated.

To select which scanners to generate:

Click one of the buttons to the right of the list box:.

- **All** - Selects all scanners
- **None** - Deselects all scanners
- **Invert** - The Invert button allows the selections to be reversed. This saves having to deselect all the scanners one by one, when only a single scanner is required. If all the scanners are selected, just deselect the one you want and choose Invert.

How to Specify Base Scanner File Name and Output Directory

You can define the base name of the scanner (up to 5 characters). Alternatively for each scanner, you can either have a file name to identify the operating system, or you can use a separate directory for each operating system.

To specify the base scanner file name and output directory:

1. For all selected scanners, specify a fully qualified file name. The initial part of this file name can be entered in the **Base Scanner File Name** box. The remaining three characters of the file name are used to describe the scanner executable.

For example, by entering **scan** (the default setting) in the **Base Scanner File Name (Max 5 characters)** box, the following scanners can be generated (if they have been selected in the **Generate scanners for** list box):

Base scanner file names and output directories:

Scanner File Name	Scanner Type
scanwin32-x86.exe	Windows (x86)
scanwin32h-x86.exe	Windows (x86, hidden)
scansolaris-sparc	Solaris (SPARC)
scansolaris-x86	Solaris (x86)
scanhpux-hppa	HP-UX (HPPA)
scanhpux-ia64	HP-UX (ia64)
scanaix-ppc	AIX (POWER)
scanlinux-x86	Linux (x86)
scanmacosx-x86	Mac OS X (x86)

2. In the **Output Directory** box, type in or click the **Browse** button to specify the directory that the generated scanners will be saved to.

Output Directories Options

The **Output Directories** options determine the manner in which scanner files are named:

To set naming conventions for the scanners:

1. Select one of the following:
   - **One Directory**

     This option incorporates the scanner name with the operating system. For example:

     scanwin32h-x86.exe
   - **Separate Directories**

     This option dictates that the names of each scanner generated are the same, but are copied into individual subdirectories which are named as per the operating system.

     For example, a scanner named **scan.exe** (Windows)/**scan** (other platforms) would appear in directories for all operating system options selected:

     ```
     C:\TEMP\win32-x86
     C:\TEMP\solaris-sparc
     C:\TEMP\hpux-hppa
     C:\TEMP\hpux-ia64
     C:\TEMP\aix-ppc
     ```

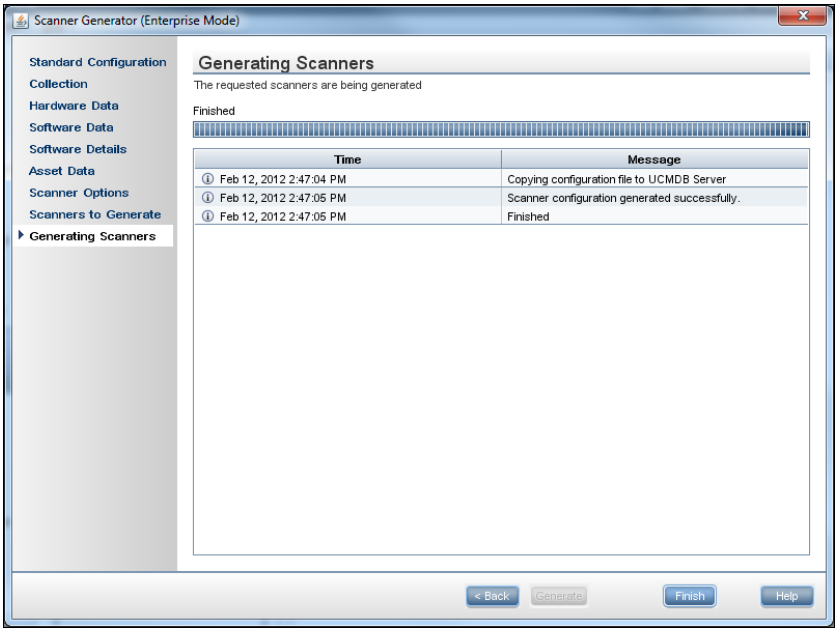
```
C:\TEMP\linux-x86

C:\TEMP\macosx-x86
```

2. Click **Generate** to create the scanner executable files.

Generating Scanners Page

After you have selected the scanners to be generated and have clicked **Generate**, the last page of the Scanner Generator wizard is displayed. This page shows the progress information during the generation of the actual scanner executable.



Important Information	General information about the wizard is available in "Scanner Generator Wizard". In Enterprise Mode, the scanner configuration is generated instead of stand-alone scanners, and the configuration is uploaded to the UCMDB server and stored in the UCMDB database as the Scanner Configuration resource files in the InventoryDiscovery adapter. If you chose to generate your scanner from a stored default predefined configuration on the server when you were on the Standard Configuration page, you will be told to rename it, since default predefined configurations cannot be overwritten. Right-clicking anywhere in the log window displays a shortcut menu which allows you to: • Save the contents of the window to a log file. • Copy the contents of the log window to the clipboard. • Clear the log window. If a scanner already exists with the same name in the chosen directory, a confirmation message is displayed. This allows you to choose whether to overwrite the existing scanner. After the scanners have been generated, click **Finish** to exit the Scanner Generator. The generated scanners can be found in the directory specified in the **Scanners** tab of the **Scanners to Generate** page.

Wizard Map	The "Scanner Generator Wizard" contains: "Standard Configuration Page" > "Collection Page" > "Hardware Data Page" > "Software Data Page" > "Software Details Page" > "Asset Data Page " > "Scanner Options Page " > "Scanners to Generate Page" > "Generating Scanners Page"

XML Enricher: Software Recognition Configuration Dialog Box

To access	Use one of the following: • **Discovery Control Panel > Discovery Modules/Jobs > Dicovery Modules** pane **> Inventory Discovery > Inventory Discovery by Scanner** job > **Properties** tab > **Global Configuration Files** pane > Double-click **EnricherServiceSettings.ini** • When creating or editing an Inventory Discovery activity, in the Preferences tab click **Mapping Options**. For details, see the *HP Universal CMDB Discovery and Integration Content Guide*.

User interface elements are described below:

UI Element (A–Z)	Description
Restore To Default	Restores the XML Enricher settings to the default setting.
General tab	Enables you to set general XML Enrichment options. See "General Tab" below.
SAI Recognition tab	Enables you determine how the XML Enricher uses the SAI files for application recognition. See "SAI Recognition Tab" below.

General Tab

User interface elements are described below:

UI Element (A–Z)	Description
Basic	• **Process Utilization Data.** By default this option is set to **Yes**. If you want to stop processing utilization data, change this option to **No**. • **Application Recognition.** There are the following options for Application recognition: ▪ **Software application index (SAI).** This is the default setting. Instructs the XML Enricher to use the Software Application Index files (.zsai) to perform application recognition. The SAI files contain a database of software applications. By default, only executable files are sent to the recognition engine for processing. You can set this so that all files are sent to the recognition engine by modifying the filter settings. See "Filtering" on page 451. ▪ **No recognition.** Disables any application recognition. When recognition is disabled, scan file processing is slightly faster as no file information is sent to the recognition engine for processing. However, the processed scan files are not enriched with application data, and no application data is added to the UCMDB database.
Scan File Management	Enables you to configure how to manage the scan files. **Group Processed Scan Files.** The grouping commands help you organize your scan files in the processed directory. You can group your scan files based on the value of the hardware fields collected by the Scanners. For example, if the grouping is done on the **hwHostOS** field, all scan files for computers having the same operating systems are grouped in the corresponding directory for that operating system. Clicking the  button opens the **Scan File Group** dialog box, enabling you to create a scan file group: • **Group processed scan files by hardware field.** Select a hardware field from the dropdown list.Details of the field are displayed in the **Detail** pane. **Note:** The value of the selected hardware field is used as the name of a subdirectory under the **Processed** directory. If the chosen field is blank in a scan file, that file is moved to a **Blank** directory. • **Value to use if hardware field is blank.** Because the directory name cannot be empty, when the value of the selected hardware field is empty, the string configured in this field is used instead to name the subdirectory.

SAI Recognition Tab

User interface elements are described below:

UI Element (A–Z)	Description
SAI Files	Enables you to specify the SAI files that the XML Enricher uses to recognize applications. The master SAI set comes with the latest Content Pack and is available in the **sai.zip** package. For details about deploying your own SAI files, see "How to Deploy User-Defined SAI Files" on page 379. • **<SAI Files grid>**.For each SAI file that appears in the list, the following information is displayed: ▪ **Use.** Specifies whether an SAI file is used by the XML Enricher. The XML Enricher only uses the selected SAI files. ▪ **File**. The name of the SAI file. ▪ **ID.** The ID for the user SAI file. **Note:** Because a master SAI file does not have an ID, it displays an ID of **N/A**. Each user SAI receives an integer ID on creation. The ID must be unique within the organization. The UD tools (including XML Enricher and Inventory Tools) need all user SAIs they load to have a different ID. It is therefore important to ensure IDs are unique. ▪ **Size.** The size (in kilobytes) ▪ **Applications.** The number of unique application versions the SAI file contains ▪ **Type.** The file type: **Master** (read-only) or **User** (editable) ▪ **Date.** ○ Master SAI files: The date the file was created. ○ User SAI files: The date the file was last saved. ▪ **Description.** The description given to the SAI file when it was created. • **SAI File Used to Store Rule-Created Items.** Specifies the SAI file to which items created by rules are added. These rules are present within the SAI files themselves. You can specify additional rules by using the SAI Editor. If this field is left blank, Universal Discovery creates a file called **Auto.zsai** and puts this in the same location as the first Master SAI. **Note:** For more information about SAI files and the process of application recognition, see the SAI Editor documentation.

UI Element (A–Z)	Description
Advanced SAI Options	Determine how the XML Enricher performs the SAI application recognition. The available options are as follows: • **Level 3 recognition heuristics.** This option determines when the XML Enricher processes scan files for a particular machine. ▪ **Yes.** The XML Enricher waits until all the files in all the directories on that machine have been read before issuing its final recognition information. More accurate recognition is achieved. ▪ **No.** Machine-based recognition does not take place, and recognition data is returned after each directory is loaded. A time overhead of about 10% is normal when Level 3 recognition heuristics is enabled. **Default:** Yes. • **Auto-identify unrecognized device driver file.** If this option is set to **Yes**, it instructs the XML Enricher to mark files that meet the following criteria as recognized in the enriched scan file: ▪ They cannot be identified by standard SAI recognition. ▪ They have the **Device Driver** attribute. Files used as Device Drivers represent a large portion of the files that are not identified by the Application Library. Being able to identify these automatically can significantly reduce the effort required to achieve good recognition rates. **Default:** Yes. • **Override OS language.** Works in conjunction with the **Preferred language** option (below). If you specify a **Preferred language**, and you set the **Override OS language** option to **Yes**, the recognition engine overlooks the OS locale setting and uses the **Preferred language** that you specify. **Default:** No • **Preferred language.** Enables you to specify the language that the XML Enricher uses when it encounters more than one language version of the same application. For example: if there are two application versions in the SAI (one English and one French) that are very similar, or the same in terms of the comprising files, setting the preferred language to French favors French applications if the recognition ratings for these application versions are the same. This option works in conjunction with the Override OS Language option (above). **Default:** Neutral. No preferred language is set.

UI Element (A–Z)	Description
Filtering	Determines what types of files the XML Enricher processes: • **Use only files with the following extensions.** Specifies the extensions of the particular file types processed by the XML Enricher. Type the extensions that you want to use directly into the box. Separate extensions with commas or semicolons. Only these file types are processed. • **Use only executable files.** Specifies that only executable files should be processed by the recognition engine. This includes ***.exe, *.com, *.dll** and other files containing executable code. **Default:** Yes • **Look also for files within archives.** Specifies that files within archive files should be processed. The following archive file types are supported: **ARJ, ZIP v1, ZIP v2, LHA, LZH, ARC, CAB, TAR, GZIP, TAR/GZIP,** and **PAK**. **Default:** No • **Regular expressions used to filter junk files.** Some files may be executable but are of no interest for licensing or other purposes. These files are often identifiable by file name. For example: **TMP[0-9]*\.\$\$\$**. This option enables you to specify file names that should be ignored by the XML Enricher. Do this by entering regular expressions in the multi-line edit box - one expression on each line. Files whose names match the regular expressions are ignored. When the XML Enricher matches a file name against a junk filter regular expression, the file name is first converted to lowercase. For this reason, all letters entered as part of the regular expression must be in lowercase for a match to successfully occur.

Store and Forward Installation Wizard

Enables you to install and configure the Store and Forward server on a computer that is running Windows.

To access	From the UCMDB installation media, copy the following file to your local computer and then double click to launch the wizard: **HP Universal Discovery Store and Forward server (x86) 10.01.000.xxx.msi**.
Important information	This MSI installer is used for Windows computers only. The Windows computer must be running Microsoft Installer version 2.0 or above.

This section includes:

- "Destination Folder Page" on next page
- "Data Files Page" on next page

- "Store and Forward Configuration Page" below
- "SSL Certificate Generation Page" on next page

Destination Folder Page

Enables you to select a folder for the Store and Forward server program files.

Important Information	The Windows computer must be running Microsoft Installer version 2.0 or later.
Wizard Map	The "Store and Forward Installation Wizard" contains: **Destination Folder Page** > "Data Files Page" > "Store and Forward Configuration Page" > "SSL Certificate Generation Page"

UI Element (A–Z)	Description
Change	Click to browse to a folder that you want to contain the program files.

Data Files Page

Enables you to select a folder for the Store and Forward data files.

Important Information	The Windows computer must be running Microsoft Installer version 2.0 or later.
Wizard Map	The "Store and Forward Installation Wizard" contains: "Destination Folder Page" > **Data Files Page** > "Store and Forward Configuration Page" > "SSL Certificate Generation Page"

UI Element (A–Z)	Description
Change	Click to browse to a folder that you want to contain the data files.

Store and Forward Configuration Page

Enables you to make configurations for the Store and Forward server.

Important Information	The Windows computer must be running Microsoft Installer version 2.0 or later.
Wizard Map	The "Store and Forward Installation Wizard" contains: "Destination Folder Page" > "Data Files Page" > **Store and Forward Configuration Page** > "SSL Certificate Generation Page"

UI Element	Description
TCP Port	Type a port number that listens for incoming scan files from downstream servers. **Default:** 5005
User name	Type a user name to use to for the service. **Default:** hpud
Password	Type a password to use for the service. **Note:** This is a mandatory field.
Communication Protocol	Select a communication protocol that you want to use as the transport mechanism when uploading scan files. • HTTPS (secure) • HTTP (plain)

SSL Certificate Generation Page

Enables you to make configurations to the certificate file if HTTPS is selected as the communication protocol.

Important Information	The Windows computer must be running Microsoft Installer version 2.0 or later.
Wizard Map	The "Store and Forward Installation Wizard" contains: "Destination Folder Page" > "Data Files Page" > "Store and Forward Configuration Page" > **SSL Certificate Generation Page**

UI Element (A–Z)	Description
DNS Name	Enter the full computer name of the computer that is running the Store and Forward server. For example,somehost.example.com

Scanner Command Line Parameters and Switches

Although the options for the scanner are normally set using the Scanner Generator, it may be necessary to change some settings to allow better operation on some machines. The operation of a scanner can be modified with the use of the various command line parameters.

Reasons for Overriding the Options in a Configured Scanner

- The scanner may encounter a problem with a particular piece of hardware. Using command line options, the problem hardware can be circumvented.
- Command line parameters can change the configured options such as save path. This allows the scan results to be saved to a local machine without a full network path having to be defined.

How to Use a Command Line Parameter

You can specify command line parameters and switches by:

- Typing the command from a command line (for example, the Windows command prompt, or the UNIX/Mac OS X shell). In UNIX/Mac OS X make sure you specify the path to the scanner.

  For example:

  ```
  /tmp/scanlinux-x86 -?
  ```

  launches the Linux scanner from the /tmp directory and displays a list of valid command line options.

- Creating a Windows shortcut. Type the command line options (if any) after the quotation marks.

  For example:

  ```
  "C:\TEMP\Scanwin32-x86.exe" -?
  ```

  launches the Win32 scanner and displays a list of valid command line options.

- Typing the command in the Windows Run command in the Start menu. Type in or navigate to the location where the scanner executable is located. Type the command line parameter or switch after the quotation marks.

  For example:

  ```
  "C:\TEMP\Scanwin32-x86.exe" -?
  ```

Command Line Parameters for Scanners

Valid command line parameters for the scanners are shown in the following table:

Command Line Parameter	Function
-force	Do not check disk space when saving off-site Scan File. This may be useful in situations where the operating system reports insufficient space, but this is actually due to access rights.

Command Line Parameter	Function

-p:<path>	Override default off-site save path. The path can be one of the following types of values, depending on the destination of the scan file:
	• Normal file path - The full path name, beginning with the drive letter.
	For example:
	`-p:c:\Inventory\Scans`
	• UNC path - When running on Windows, a UNC path can be entered as the argument to this option. The format of a UNC path is:
	`\\servername\sharename\path\`
	For example:
	`-p:\\DDMIServer\Incoming\`
	The user running the scanner must have Write permissions to the specified path.
	• FTP/S URL - A destination URL of an FTP server. The format of the URL is:
	`ftp://<username>:<password>@<hostname>:<port>/dir`
	For example:
	`-p:ftp://scanuser:scanpasswd@ddmiserver.mycompany.com/nm/scanner/uploadscans`
	• HTTP/s URL - A destination URL of an HTTP server. The format of the URL is:
	http://<hostname>:<port>/dir
	For example:
	`-p:http://ddmiserver.mycompany.com/nm/scanner/uploadscan`
	The username and password is not supported here. If the username and password is required with HTTP saving, specify it in the Advanced Settings dialog in the Saving tab of the Scanner Generator. For detailed information, see "Save to an HTTP or HTTPS URL".
	The scanners support URL encoding in usernames, passwords, and directory names. In a URL, you can replace @ with %40, and the scanner translates %40 to @ before it calls the FTP server. For

Command Line Parameter	Function
	example, if you type scanuser%40mycompany, the scanner will translate that as scanuser@mycompany when it logs in to the FTP server.

-r:<path>	Override the default path to the original scan files. A UNC path can also be entered as the argument to this option. The format for a UNC path is:
	`\\servername\sharename\path\`
	For example:
	`Scanwin32-x86 -r:\\Hewlett-Packard\ED\scanfiles\`
	The user running the scanner must have read permissions to the specified UNC path.

-scandays:<Count>	Scan only if previous scan was more than Count days ago. Forces the scanner to perform the scan only if the previous scan was <Count> or more days ago. For example:
	`-scandays:7`
	For example, if the scanner is launched from a login script every day, it will only perform the scan every week.
	When the scandays:<Count> parameter is specified, the scanner attempts to check when the last scan was run. If no previous scan file is found, no messages are displayed and the scan runs. If a scan file is found, the following message is added to the log file:
	`"Checking the age of Scan File "%s"`
	Where %s is the full name of the scan file it checks. If there is a problem determining the age of the scan file (for example, if it is a newer version or it is corrupt), it then outputs:
	`The age of the Scan File cannot be determined.`
	If it does manage to obtain the date, it outputs:
	`Last scan was %d days ago`
	Where %d is an integer number.

-incl:<switch>	Switches for re-enabling individual hardware tests that were disabled in the Scanner Generator. See "Using Command Line Switches to Enable and Disable Specific Hardware Tests". To include tests 10, 20 and 50, you would run: `-incl:10 -incl:20 -incl:50`

Command Line Parameter	Function
-excl:< switch >	Switches for disabling individual hardware tests. See "Using Command Line Switches to Enable and Disable Specific Hardware Tests". To exclude tests 10, 20 and 50, you would run: `-excl:10 -excl:20 -excl:50`

-scan-dayofweek:<Number>	Scan only on specified day of week (0-Sun,1-Mon, etc.). <Number> can be one of the following:
	`0-Sunday`
	`1-Monday`
	`2-Tuesday`
	`3-Wednesday`
	`4-Thursday`
	`5-Friday`
	`6-Saturday`
	For example:
	`-scandayofweek:5`
	This will cause the scan to be performed on Fridays only. The scandays: and scandayofweek: options can be combined. For example:
	`Scanwin32-x86 -scandays:14 -scandayofweek:3`
	This causes the scan to be performed every other Wednesday.

-paths	Using this switch, it is possible to define exactly which directories to scan; the parameter can be repeated as many times as necessary. For example: `scan -paths:/etc -paths:/var -paths:/bin` scans just /etc, /var and /bin and their subdirectories. **Note:** You must ensure that the **Allow scanner command line to override this selection** option is checked in the Scanner Generator Software Data pagefor this to work.
-l:<filename>	Override the default file name of the local scan file, local$.xsf. If the path is specified in the file name, then the default path for storing the local scan file is also overridden.
-t:<path>	Override the default path for storing temporary files.
-v	Tell the scanner not to make the local scan file read-only or hidden.

Command Line Parameter	Function

-o:<filename>	Takes the off-site scan file name from the command line.
	
	For example (non UNIX):
	
	`Scanwin32-x86 -o:r:\results\SC002154`
	
	Where `r:\results\SC002154` is the path to the file SC002154.
	
	If a file name is not entered, the file is named Default.xsf. If the path is not specified, the file is placed in the directory configured for off-site scan files in the Scanner Generator. If the path is specified on the command line (even if it is relative), it replaces the path configured in the Scanner Generator. Here are some examples.
	
	`scanlinux-x86 -o:newname`
	
	Saves the off-site scan file, newname.xsf, to the location configured in the Scanner Generator.
	
	`scanlinux-x86 -o:/tmp/newname`
	
	Saves the off-site scan file to /tmp/newname.xsf.
	
	`scanlinux-x86 -o:subdir/newname`
	
	Saves the off-site scan file, newname.xsf, to the subdir subdirectory of the current directory.

-log:<level>	Specifies the level of debugging information that will be written to the scanner log when the scanner is running. The log is saved in the scan file and also as a separate file: • In most cases, you can view the scanner log by using the Viewer. • If a problem has occurred that prevents the scanner from saving the scan file, you can view the scanner log file from the Diagnostic panel in the Device Manager. <level> can be one of the following: • off: Detailed logging is turned off. This is the default. • debug: Debug messages are logged in addition to the regular scanner messages. They are more-detailed providing additional information. • trace: All regular, debug, and detailed messages are logged. The detailed messages provide tracing details as to scan runs, returned error codes, and software scanning. This option automatically enables the generation of the error log file.

Command Line Parameter	Function
-cert	Specifies the path to the certificate file. This path is used with offsite scan saving when performed using the secure SSL-based protocol, such as ftps or https, to specify the certificate file (for self-signed certificates) or the file containing certificate authority files (for ftps/web sites running with the regular certificate issued by a certificate authority). To obtain the file containing all recent certificate authorities extracted from the Mozilla browser, see: http://curl.haxx.se/docs/caextract.html If the -cert command line option is not specified, the scanner still tries to save scan files using ftps/https, but without using any certificates.
-d	This overrides the setting for delta scanning in the configuration file. If set to **on**, this enables delta scanning if it is disabled in the scanner generator. If set to **off**, this disables delta scanning if it is enabled in the scanner generator. If the setting fails to specify on or off, the scanner prints the help message and returns.
-?	The full list of command line options can be obtained by running the scanners with the -? or /? command line option.

Viewing Command Line Options in Viewer or Analysis Workbench

If a command line option or switch has been used, it can be viewed in Analysis Workbench or Viewer.

This can be very useful when you want to check if the scan results were obtained from a scanner that had been run with any special command line options.

For example, if the scanner had been run with the -paths command:

```
scan -paths:/etc -paths:/var -paths:/bin
```

The -paths command line option will be displayed in Viewer (System Data folder in the Hardware and Configuration tab page).

Using Command Line Switches to Enable and Disable Specific Hardware Tests

Hardware test numbers that can be used for enabling/disabling hardware tests in the scanners as part of the -excl and -incl command line switches are shown in the following table:

Hardware Test	
10: BIOS data	**11: BIOS extension**
12: SMBIOS Information	**13: Compaq Asset Tag**
14: Plug and Play Version	**30: Video data**
31: Monitors	**40: Port data**
50: Keyboard and mouse data	**60: Disk data**
62: Local USB hard drives	**70: Memory data**
72: Swap files	**80: CPU data**
90: Operating system data	**91: Device driver files**
92: Cluster data	**93: Services**
94: Virtual machine data	**95: User profiles**
96: OS registered applications	**97: Containers**
98: WMI software features	**99: Packaged file data**
901: Software identification tags	**100: Storage data**
101: Devices	**102: SCSI/IDE serial numbers**
110: Network data	**111: TCP/IP data**
112: IPX data	**113: Netbios data**
114: Network shares	**120: Bus data**
121: PCI cards	**122: PCMCIA cards**
123: MCA cards	**124: EISA cards**
125: ISA PnP card detection	**126: USB data**
130: Peripherals	**150: System configuration**

Scanner File Locations

When you use activities to automate discovery, the Scanner is copied to the discovery node according to the default value in the Inventory Discovery by Scanner job adapter.

The default file location of the Scanner is as follows:

Platform	File Location Path
Windows	%SystemRoot% **Note:** %SystemRoot% is normally located at C:\Windows.
Solaris Sparc	$HOME/.discagnt **Note:** $HOME is normally “/”, so the directory is “/.discagnt/”.
MacOS	~/.discagnt/ **Note:** The "~" symbol normally is “/var/root”, so the directory is “/var/root/.discagnt/.
Linux	
HP-UX	
AIX	

Scan File Formats

The information collected from each computer can be stored in two formats:

Compressed XML (XSF) - with the file extension .xsf

This scan file format allows the scan data to be augmented with application recognition information. The XML data inside these scan files is compressed using gzip compression. The files can be uncompressed using gzip, WinZip, or any other program that supports gzip decompression.

For more information about the XSF format, see "Enriched XSF File Structure" on page 466.

Delta Scan File (DSF) - with the extension .dsf

Instead of sending a full scan file to a probe after every scan, the scanners can calculate the difference (the *delta*) between the last full scan and the current one and transfer just this in Delta Scan File format (DSF). This can dramatically reduce the network bandwidth used when using Universal Discovery. Delta Scan files cannot be viewed or used in the analysis tools (Analysis Workbench, SAI Editor, and Viewer).

Example of How Data is Stored

The following is an example of several sections of an xsf file.

```
<?xml version="1.0" encoding = "UTF-8" ?>
<inventory codepage="1251" locale="English (United States)"
fsfmajorver="7" fsfminorver="6" enricherver="10.00.000.555">

<hardwaredata>
 <hwAssetData type="shell">
 <hwAssetDescription type="attrib">tbrown - Xeon, 2800MHz,
 3712Mb</hwAssetDescription>
 <hwAssetTag type="attrib">000590 </hwAssetTag>
 </hwAssetData>
 <hwMemoryData type="shell">
 <hwMemTotalMB type="attrib">3712</hwMemTotalMB>
 <hwSwapFiles type="shell">
 <hwSwapFiles_value type="shell_value">
 <hwMemSwapFileName
        type="attrib">C:\pagefile.sys</hwMemSwapFileName>
 <hwMemSwapFileSize type="attrib">1534</hwMemSwapFileSize>
 </hwSwapFiles_value>
 </hwSwapFiles>
 <hwDOSMemoryData type="shell">
 <hwMemConventional type="attrib">640</hwMemConventional>
 </hwDOSMemoryData>
 <hwCMOSMemory type="shell">
 <hwMemExtended type="attrib">3799944</hwMemExtended>
 <hwMemCMOSTotal type="attrib">3800584</hwMemCMOSTotal>
 <hwMemCMOSConventional type="attrib">640</hwMemCMOSConventional>
```

```
 </hwCMOSMemory>
 </hwMemoryData>
 </hardwaredata>

<applicationdata>
<recogconfig>
 <sai name="C:\hp\UCMDB\DataFlowProbe\runtime\probeManager\
        discoverySaiResources\saiRuntime\User.zsai"
        desc="User SAI File" date="04/06/2011" type="User"/>
 <sai name="C:\hp\UCMDB\DataFlowProbe\runtime\probeManager\
        discoverySaiResources\saiRuntime\Master.zsai"
        desc="" date="07/05/2011" type="Master"/>
 </recogconfig>
 <application version="6.4.09"
 release="6.4"
 name="Windows Media Player"
 publisher="Microsoft"
 language="English"
 os="Windows 2000"
 type="Ambient music or advertising messaging software"
 typeid="143033"
 maindir="C:\Program Files\Windows Media Player"
 lastUsed="2011-08-26 00:00:00"
 versionid="9978"
 releaseid="582"
 licencedby="11907"
 licencedbyrelease="84"/>
 <application version="6.0 sp1"
 release="6.0"
 name="Internet Explorer"
 desc="Microsoft Internet Explorer"
 publisher="Microsoft"
 language="English"
 os="Windows 98/NT/2K/ME/XP"
 type="Internet browser software"
 typeid="122252"
 maindir="C:\Program Files\Internet Explorer"
 lastUsed="2011-05-07 00:00:00"
 versionid="12790" releaseid="131"/>
</applicationdata>

<filedata>
 <dir name="C:\" date="2011-07-03 03:23:04" contains="-1">
 <file name="AUTOEXEC.BAT" size="0" modified="2011-04-03
13:51:04" attr="a"/>
 <file name="BOOT.INI" size="288" modified="2011-04-03
15:14:38" attr="rsa"/>
 <file name="sd_settings.ini" size="462" msdos="SD_
SET~1.INI" modified="2011-06-14 09:08:44" attr="a">
```

```
 <verinfo name="DOS 8.3 Name" value="SD_SET~1.INI"/>
 </file>
 </dir>
</filedata>

<storedfiles>
 <storedfile type="storedfile" name="SYSTEM.INI" size="217"
istext="1" istruncated="0" dir="C:\WINNT\SYSTEM.INI">
 <contents encoding="text">; for 16-bit app support
 [386Enh]
 woafont=dosapp.fon
 EGA80WOA.FON=EGA80WOA.FON
 EGA40WOA.FON=EGA40WOA.FON
 CGA80WOA.FON=CGA80WOA.FON
 CGA40WOA.FON=CGA40WOA.FON
 [drivers]
 wave=mmdrv.dll
 timer=timer.drv
 [mci]
 </contents>
 </storedfile>
</storedfiles>
</inventory>
```

XML Enricher Directory Structure

The XML Enricher uses a directory structure on the Data Flow Probe computer under the probe's installation directory. By default, the root of this directory structure is:

`C:\hp\UCMDB\DataFlowProbe\runtime\xmlenricher.`

The following table shows various directories that are used by the XML Enricher.

Directory	Explanation
`Scans`	The base directory.
`Scans\Failed`	The base failure directory. Failed scans are moved to a subdirectory of this one.
`Scans\Failed\Corrupt`	Scans that cannot be read or may not be scan files are moved here.
`Scans\Failed\Delta`	If the original scan file is missing or there is an error applying the delta scan file to the original one, then those delta scan files will be moved here.
`Scans\Failed\Error`	When any other error occurs, scan files are moved here.
`Scans\Incoming`	The incoming directory. The Enricher looks for new scan files here.
`Scans\Logs`	Stores the log files. Manual deployment Scanners may save the log into the off-site location.
`Scans\Original`	This folder is used for delta scanning. It stores copies of original scan files, which are then used in conjunction with delta scan files to recreate the new version of the scan file.
`Scans\Processed`	The processed directory. Enriched scan files are created here.
`Scans\Processed\[user defined]`	You can group the scan files based on Hardware fields. This is user-defined. Define the setting as follows: • Go to **Inventory Discovery by Scanner job > Properties > Global Configuration Files** • Select **EnricherServiceSettings.ini** • Click the  button The **XML Enricher Configuration** dialog is displayed • On the **General** tab, use the **Scan File Management** part See "Scan File Management" on page 448.
`Scans\ProcessedCore`	Stores the processed core files.
`Scans\Sending`	The Inventory Discovery job moves the new processed core files here for further processing.
`Scans\Temp`	This is where the XML Enricher stores its temporary files.

The following flowchart shows how the enrichment process works for XSF and delta (DSF) scan files.

Enriched XSF File Structure

Scanfile.dtd describes the structure of the scan file in standard DTD format.

> **Note:** The file is a text file, but is easiest to read with an XML reader.

An XSF scan file contains a sequence of elements, each of which have various attributes. Root elements are:

- **<hardwaredata>**
- **<applicationdata>**

- **<users>**
- **<applicationusage>**
- **<filedata>**
- **<storedfiles>**
- **<configurationdata>**

XML Enricher Log Files

Whenever enrichment of a scan file fails, an entry describing the occurrence is added to a file named **log.txt** in the relevant failed subdirectory.

The format of a line in the log file is:

```
<date> <time> - <AssetTag> (<Failure reason>).
```

The XML Enricher also adds entries to the **XmlEnricherService.log** (by default located in the **C:\hp\UCMDB\DataFlowProbe\runtime\log** directory) in the following circumstances:

- When it starts up and shuts down
- When it starts enrichment of a new scan file
- If an error occurs

Scanner Scheduler Resources

File Locations

Platform	Installation Location	Log File Location
Windows 32-Bit	<ProgramFiles>\Hewlett-Packard\Universal Discovery\10.01\Scanner Scheduler **Note:** • This location can be configured by using the following command: INSTALLDIR=C:\ScannerScheduler • The <ProgramFiles> environment variable is normally located at C:\Program Files	<ALLUSERSPROFILE>\Hewlett-Packard\Universal Discovery
Windows 64-Bit	<ProgramFiles(x86)>\Hewlett-Packard\Universal Discovery\10.01\Scanner Scheduler **Note:** • This location can be configured by using the following command: INSTALLDIR=C:\ScannerScheduler • The <ProgramFiles(x86)> environment variable is normally located at C:\Program Files(x86)	
UNIX	/opt/HP/ScannerScheduler	$HOME/.discagnt directory
Mac	/Library/StartupItems/HPScannerScheduler	
AIX	/usr/lpp/HP/ScannerScheduler	

Configuration File Parameters

The config.ini file contains parameters for managing the scanner schedule and for downloading a configuration file on a remote server. The parameters are as follows:

Configuration File Parameter	Description
Monday|Tuesday|Wednesday|Thursday Friday| Saturday| Sunday	For each day of the week, enter the range of hours you want your scheduled event to run. If you specify multiple time intervals, use commas to separate each interval. For example: 10:00-12:00,14:00-18:00 **Note:**The 24-hour clock is used.

Configuration File Parameter	Description
FrequencyHours	Indicates how frequently the scheduled event occurs. Assume you want to use a weekly interval for your scheduled event. In this scenario, set the value to 168. If this parameter is set to 0, scheduling is disabled. **Note:** This is a mandatory field
RandomDelayMinutes	Specifies a random delay to the start time for load balancing purposes. Assume that the scanner is scheduled to run at 9:00 and the random delay is 60 minutes. In this scenario, the scanner runs at a random point in time between 9:00 and 10:00. If this parameter is set to 0, no random delay is used.
CommandLine	Enter a command line to run the scanner or to run a program that will download the config.ini file from a remote server. In the [Scan] section of the config.ini file, enter a command line to run the scanner. If no path is specified, the Scanner Scheduler attempts to start the scanner from the same directory as the Scanner Scheduler executable is located. In the [DownloadConfig] section, enter a command line to run Curl, or any other data transfer tool, to download a remote config.ini file.

Windows Specific Resources

File name	Description
ScannerScheduler.exe	Executable file of the Scanner Scheduler service
config.ini	Configuration file that contains parameters that manages the scanning schedule of the scanner. It also manages, together with a third party program, the download schedule of another config.ini file that is located on a remote server.
curl.exe	Executable file of Curl. This third party program can be used to download a new configuration file from a remote server.
libeay32.dll	OpenSSL DLL to enable Curl to work over HTTPS
libssl32.dll	OpenSSL DLL to enable Curl to work over HTTPS
curl-ca-bundle.crt	Root CA certificates to enable Curl to work over HTTPS

UNIX Specific Resources

File Name	Description
bin/scansched	Executable file of the Scanner Scheduler service.
bin/config.ini	Configuration file that contains parameters that manages the scanning schedule of the scanner. It also manages, together with a third party program, the download schedule of another config.ini file that is located on a remote server.
bin/curl	Executable file of Curl. This third party program can be used to download a new configuration file from a remote server.
bin/curl-ca-bundle.crt	Root CA certificates to enable Curl to work over HTTPS.
discscannerscheduler	Script to manage the scanner scheduler. For more information about available parameters that you can use in this script, see "Scanner Scheduler Parameters" below

Scanner Scheduler Parameters

To manage the Scanner Scheduler for nodes that are running Unix, enter the following command:

discscannerscheduler <ParameterName>

Note: Ensure that you run the command from the installation location.

Parameter Name	Description
start	Starts the Scanner Scheduler service.
stop	Stops the Scanner Scheduler service.
restart	Restarts the Scanner Scheduler service.
status	Indicates running status information of the Scanner Scheduler service. • If the Scanner Scheduler is running, it returns “Universal Discovery Scanner scheduler (pid xxxx) is running”. • If the Scanner Scheduler is not running, it returns “Universal Discovery Scanner scheduler stopped.”.

Store and Forward Commands

Commands that are available for the Store and Forward server service are as follows:

Windows

Description	Command
Restart	**net start ovedStoreAndForward**
Stop	**net stop ovedStoreAndForward**
Uninstall	**Control Panel** > **Add/Remove Programs**

Linux

Description	Command
Restart	**/etc/init.d/hpudsaf restart**
Stop	**/etc/init.d/hpudsaf stop**
Uninstall	1. **/sbin/chkconfig --del hpudsaf** 2. **rm -rf /etc/init.d/hpudsaf**

Store and Forward Resources

Windows

By default, program files are installed in the following location:

<Program Files>\Hewlett-Packard\Universal Discovery\10.01\Store and Forward

By default, data files, log files, and scan files that are in transit are stored in the following location:

<ALLUSERSPROFILE>\Application Data\Hewlett-Packard\Universal Discovery S&F

In addition, the following directories are created after installation.

Subdirectory	Description
bin	Contains the Apache web server executable files, DLL files, and the Store and Forward server executable files
conf	Contains the configuration files, including **httpd.conf** (the configuration file for the Apache web server) **Note:** The **httpd.conf** file contains parameters that control bandwidth throttling
modules	Contains the Apache web server modules
Logs	Contains the logs for the Apache web server and the Store and Forward server

Subdirectory	Description
Incoming	Contains incoming scan files
InProgress	Contains the files that the server is processing
Status	Contains status files
Resume	Contains scan files that are partially uploaded

The Windows service is registered with the following parameters:

Service attribute	Value
Apache Service Name	ovedApacheSF
Apache Display Name	HP Universal Discovery Store and Forward Web Server
Apache Startup Type	Automatic
Store and Forward Service Name	ovedStoreAndForward
Store and Forward Display Name	HP Universal Discovery Store and Forward Server
Store and Forward Startup Type	Automatic

Linux

The following directories are created in the installation folder after installation.

File name	Comment
bin	Contains the Apache web server executable files, DLL files, and the Store and Forward server executable files.
conf	Contains the configuration files, including **httpd.conf** (the configuration file for the Apache web server). **Note:** The **httpd.conf** file contains parameters that control bandwidth throttling.
data	Parent data directory.
data/Logs	Contains Apache web server and Store and Forward server log files.
data/Incoming	Contains incoming scan files.
data/InProgress	Contains the files that the server is processing.
data/Status	Contains status files.
data/Resume	Contains scan files that are partially uploaded.
modules	Contains the Apache web server modules.

The Linux service is registered with the following parameters:

Service attribute	Value
Linux Service Name	StoreNForward
Apache Service Name	httpd

Status Information XML File Printout

In addition to using web-based methods to access status file information, data that is contained in this file can also be accessed by external programs or scripts. The file resembles the following:

```
<?xml version="1.0" encoding="UTF-8"?>
<?xml-stylesheet type="text/xsl" href="server_status.xsl"?>
<StoreAndForwardStatus version="1.0">
<statusDirBytes>0</statusDirBytes>
<incomingDirBytes>0</incomingDirBytes>
<inProgressDirBytes>0</inProgressDirBytes>
<resumeDirBytes>0</resumeDirBytes>
<freeDiskSpaceBytes>50882215936</freeDiskSpaceBytes>
<numIncomingFiles>0</numIncomingFiles>
<numInProgressFiles>0</numInProgressFiles>
<numResumeFiles>0</numResumeFiles>
<modifiedTime>12/22/10 08:23:30</modifiedTime>
</StoreAndForwardStatus>
```

Configuration File

The structure of the **config.ini** file is as follows.

Section Name	Parameter Name	Description
Log	filterLevel	Type **default** or **debug**. When **debug** is specified, detailed logging is enabled.
	rotateSizeMB	Specifies the size of each log file. The Store and Forward server can store the log information in several log files.
	rotationFileCount	Specifies the number of log files to keep. When the parameter value is reached, the oldest log file is discarded.

Section Name	Parameter Name	Description
[BaseDirectories]	dataDir	Specifies the location of the **data** directory. Normally, it is not necessary to modify this setting because it is configured automatically by the installer.
	incomingDir	Specifies the location of the **Incoming** directory. Normally, it is not necessary to modify this setting, as it is configured automatically by the installer.
[Channels]	channelX	Specifies the name for each channel. Channel names are used to name the top level directory of the Store and Forward server. The corresponding physical directory is created under the **Incoming** directory of the Store and Forward server.
[UpstreamProviders]	providerX	Specifies the URLs for upstream Store and Forward servers. The URL should include the HTTP username and password required to access the URL. When the HTTPS protocol is used, the host name of the Store and Forward server supplied in this URL must match the host name given during the installation of that Store and Forward server, as this host name is encoded in the HTTPS certificate. When configuring a Store and Forward server that is installed together with the Data Flow Probe, use the following configuration: This key specifies the full path to a local directory. In this case, the received file is copied to that directory, or moved if the channel is mapped to only one upstream provider. The only provider that is listed should be the incoming directory of the XML Enricher, as all files received by this Store and Forward server will be moved automatically to the Incoming directory of the XML Enricher.
[ChannelMapping]	channelX	Specifies how the files arriving to this channel will be forwarded. One or more upstream Store and Forward servers from the [UpstreamProviders] section should be specified. Multiple servers are separated with commas.

Section Name	Parameter Name	Description
[StatusPage]	updateFrequencyMins	Specifies how frequently (in minutes) the status page is updated. The default is **20**. If the setting is set to **0**, the status page is not updated.

Sample Configuration File

The following is a sample **config.ini** file that has two upstream Store and Forward servers configured, two channels, and three providers:

[Log]

filterLevel=default

rotateSizeMB=10

rotationFileCount=5

[BaseDirectories]

dataDir=C:\ProgramData\Hewlett-Packard\DDMI S&F\

incomingDir=C:\ProgramData\Hewlett-Packard\DDMI S&F\Incoming\

[Channels]

channel0=ddmi

channel1=hpca

[UpstreamProviders]

provider0=http://ddmi:ddm1passw0rd@ForwardS&Fserver1:5005/ddmi/

provider1=http://ddmi:ddm1passw0rd@ForwardS&Fserver2:5005/hpca/

provider2=http://ddmi:ddm1passw0rd@ForwardS&Fserver3>:5005/ddmi/

[ChannelMappings]

channel0=provider0,provider2

channel1=provider1

[StatusPage]

updateFrequencyMins=20

Chapter 14

Just-In-Time Discovery

This chapter includes:

Just-In-Time Discovery Overview

Universal Discovery integrates with RUM to provide real time, passive discovery and monitoring of topology changes in a given environment. This is known as the Just-In-Time (JIT) discovery mechanism.

One or more RUM Engines can be configured to interact with Universal Discovery's Data Flow Probes. The RUM Engine gathers information from RUM Probes in its network, and passes relevant information on to the Data Flow Probes. From the Universal Discovery perspective, the RUM Engines behave as passive discovery probes, where the Data Flow Probes are the active probes.

The passive probes also send notifications about discovered information to the Data Flow Probes. Notifications can include, for example, changes in environment topology, such as an unseen IP address, or software that is not running. You configure these notifications in Universal Discovery. Based on these notifications, the Data Flow Probes report, add, or remove relevant CIs to or from the UCMDB Server, or designate them as candidates for deletion.

For details about setting up the passive discovery probes and running JIT Discovery, see "How to Configure Just-In-Time Discovery" below.

How to Configure Just-In-Time Discovery

This task describes how to set up Just-in-Time discovery to provide passive, real-time discovery and monitoring of traffic in a given environment.

To learn more about Just-In-Time discovery, see "Just-In-Time Discovery Overview" above.

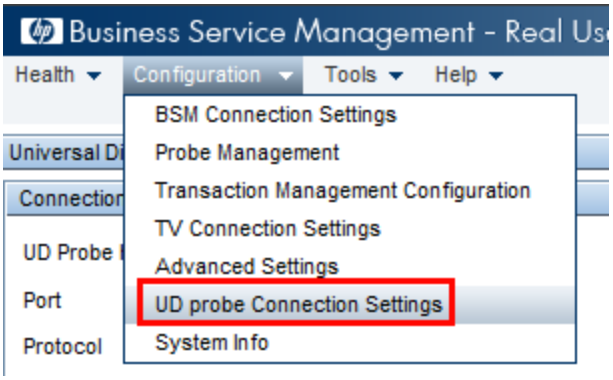
1. **Prerequisites**

   HP Real User Monitor (HP RUM) version 9.20 or later must be installed on a separate server, and must be running and configured to integrate with a Data Flow Probe.

   Note: The HP RUM Installation can be downloaded from the HP Software Support Online Portal (http://support.openview.hp.com/selfsolve/patches). Search for **Application Performance Management (BAC)** > **BAC Real User Monitor**

   To configure HP RUM to integrate with a Data Flow Probe:

a. In HP RUM, select **Configuration > UD Probe Connection Settings**.



b. Enter the host name of the Data Flow Probe to which the RUM Engine is to report, and port through which it is to send data to the Data Flow Probe.

c. Select a connection protocol.

d. Leave Authentication, Proxy, and SSL settings empty.

e. Save your configuration.

2. ## Configure passive discovery probe notifications and removal verification policy

a. In **Data Flow Management > Data Flow Probe Setup >**, select the domain where the passive discovery probe (RUM Engine) resides.

b. In the Domain and Probes pane, click **Passive Discovery Probes**.

c. In the **Passive Discovery Probes Pane** configure the passive probe notification options and removal verification policy. For details see "Passive Discovery Probes Pane" on page 83.

d. In the **Domains and Probes** pane select the passive discovery probe that you want to configure

e. In the **Passive Discovery Probe details > Passive Discovery Integrated Ranges** pane, configure the ranges over which the passive discovery probe should perform discovery, and the ports it should monitor. For details, see "Passive Discovery Probe Details Pane" on page 80.

f. Ensure that the passive probe status is **Connected**, If it is suspended, click the **Resume Probe** button in the Domains and Probes pane toolbar.

3. ## Activate passive Just-in-Time discovery

a. Go to the **Discovery Control Panel > Discovery Modules/Jobs** tab.

b. Under **Network Infrastructure > JIT Discovery** select **JIT Passive Discovery**.

c. Click the **Activate Selected Discovery Jobs** button. When the passive probes are activated, they download configuration (ranges and notifications) and start to report notifications to the Data Flow Probe.

Reconciliation

Chapter 15

Entity Reconciliation

This chapter includes:

Reconciliation Overview

Reconciliation is the process of identifying and matching entities from different data repositories (for example, UCMDB Discovery, DDMI, ticketing, or BSM). This process is designed to avoid duplicate CIs in UCMDB.

Many different data collectors can send CIs to UCMDB. In actuality, each different source might be providing information about the same CI. The reconciliation engine is responsible for identifying and matching entities from different data collectors and storing them, without duplicating CIs, in UCMDB.

Three main services provide support for the reconciliation engine:

- **Data Identification**. Responsible for comparing input CIs, according to reconciliation rules. For details, see "Identification Service" on page 484.
- **Data In**. Responsible for inserting data into UCMDB. This service decides whether to:
  - merge data into existing CIs in UCMDB
  - ignore input CIs in the case of multiple matches

  For details, see "Data-In Service" on page 507.
- **Merge**. Responsible for merging CIs (used in Federation and Data In flows). Merging is done according to the reconciliation priority definitions. For details, see "Merge Service" on page 485.

These services operate during reconciliation for inserting data from different sources into UCMDB, 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

UCMDB 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 485.

The following rules are used during reconciliation:

- **Identification criteria.** A set of criteria that defines all possible conditions to find all candidate CIs for matching to a newly introduced CI.
- **Match criteria.** There are two types of match criteria:
  - **Match verification criteria,** A set of criteria that are applied to all candidates left over after performing identification (in the previous step). Match verification ends successfully only when all applied verification criteria are true or NA (missing data).
  - **Match validation criteria.** An ordered set of criteria that is applied to all candidates left over after performing match verification. For each criterion, the following results are possible:
    - a true result implies a match
    - a false result implies no match
    - 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.

See also:

- "Identification and Match Criteria Configuration " below
- "Examples of Identification Configuration" on page 482

Identification and Match Criteria Configuration

Depending on your data source, available credentials, and specific system security settings, an integration point may have access to only a limited set of attributes when identifying a CI.

For example, IP range discovery detects two IP addresses (10.12.123.101 and 16.45.77.145), and creates two nodes. However, detailed system discovery may detect that those two IP addresses are actually configured on two network interfaces in the same node.

This means that you cannot always rely on a single matching set of attributes for identification – other possible attributes that can potentially help to identify the CI should also be listed. In the previous example, the node identification attributes can be the IP address and the network

interface. If you use the IP address to identify the CI, you see that all three discovered nodes are the same node.

Suppose that detailed system discovery detects a node with IP address 10.12.123.101 and network interface MAC1. At some point, that node was shut down, and the same IP address (10.12.123.101) was given to another node with network interface MAC2. These two nodes have the same IP address; however; it is obviously not the same CI. Performing match validation on the network interface data helps us to realize that it is not the same node.

The identification criteria are used to select candidates, and the match criteria are used to approve the identification result or dismiss it. For example, while handling input CI `A`, we may get identification candidates `B` and `C`, and the match criteria will dismiss `B`. In that case, we are left with `C`, which means that `A` is identified as `C`.

Identification Criteria

Data that the reconciliation engine receives from different data sources may contain different subsets of the attributes (topology) necessary for identifying a CI. The identification criteria should contain all potential attributes on which CI matching can be done.

Specifications

Each identification criterion defines a potential condition for CI matching. The criterion can be an attribute such as node name, or topology such as IP address. A criterion may contain two or more conditions, to create a more complex matching rule. It may also contain different condition operators such as equals or contains, or it may contain some master value that defines a value in the CI that will always allow a match.

During the identification process, all identification criteria are running to find all candidate CIs for matching.

Possible Node Identification Criteria

- HW ID
- Network interface (containing a condition operator)
- Node name
- IP address (containing a condition operator)

Match Criteria

While identification criteria list all potential attributes for matching the data, match criteria contain the attributes that are essential for matching CIs, if any exist. This means that if two CIs are marked as candidates to be matched by the identification criteria, the match criteria will check if the data exists in both CIs in order to match the condition.

Match criteria are also used during the Data In process in case of multiple matches, to make the decision to merge CIs from the CMDB. The CIs are merged only if the match criteria are satisfied. If one of the CIs does not satisfy the match criteria, the merge is not performed.

Specifications

A match criterion is satisfied if two candidate CIs have the same essential data (as defined in the that criterion), the data matches the condition, or if at least one of the CIs has no essential data.

Match criteria can be divided into two categories:

- Match verification criteria – if the verification criterion is not satisfied on two candidate CIs, these CIs are not matched.
- Match validation criterion – if the criterion with higher priority is satisfied (without missing data) on two candidate CIs, the validation criterion with lower priority is even not checked and the CIs are marked as matched. Similarly, if the validation criterion with higher priority is refuted on two candidate CIs, the criterion with lower priority is even not checked and the CIs are marked as not matched.

Possible Node Match Criteria

- Match verification criteria uses the discovered OS data for verification. This means that if two nodes have discovered OS data and this data does not match, these two nodes are not matched.
- Match validation criteria (ordered from highest to lowest priority):
  - Network interface with a **contains** operator
  - Node name with an **equals** operator
  - HW ID 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:\St-
arTeam\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 the 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, in turn, 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 criterion 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 criterion that returns `false`, that is, 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 are satisfied, and a validation criterion returns `false`, the two CIs are unmatched.
    c. If none of the validation criteria are `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
UCMDB 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 UCMDB node, run the identification criteria:
   - Node N1 does not match any identification criteria, so it will not be added to the candidates list.
   - Node N2 matches the IP identification criterion of the input node, so it will be added to the candidates list.
   - Node N3 does not match the input node by the IP identification criterion, but does match by the MAC address identification criterion, so it will be added to the candidates list.

   Therefore, the candidates list is: N2 and N3.
2. For each node in the candidates list, run OS match verification criteria. Node N3 does not satisfy this rule, since its OS is UNIX and the input node's OS is NT. Therefore, N3 will be removed from the candidates list.

   The candidates list is: N2.
3. Run the match validation criteria one by one on node N2. Since node N2 has no data conflicts, the match validation criteria are approved and N2 is marked as matched.

   The result of the identification process is: N2 = ip_address=ip1,ip2, MAC address=m1, os_family=nt.

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.

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 488.

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 **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 linkType="composition" ciType="interface">
            <overlap-operator match-percent="66"/>
            <attribute-condition autoExcludeThreshold="50" conditionType="approveAndContradict"
includeNullValue="false" attributeName="mac_address"/>
         </connected-ci-condition>
      </identification-criterion>
      <identification-criterion>
         <connected-ci-condition linkType="containment" ciType="ip_address">
            <overlap-operator match-percent="66"/>
            <attribute-condition conditionType="approveAndContradict" includeNullValue="false"
attributeName="ip_lease_time">
               <include-only>
                  <value>0</value>
               </include-only>
            </attribute-condition>
            <attribute-condition conditionType="approveAndContradict" includeNullValue="false"
attributeName="authoritative_dns_name"/>
         </connected-ci-condition>
      </identification-criterion>
      <identification-criterion>
         <attribute-condition conditionType="approveAndContradict" includeNullValue="false"
operator="EqualIgnoreCase" attributeName="name"/>
      </identification-criterion>
      <identification-criterion>
         <attribute-condition conditionType="approveAndContradict" includeNullValue="false"
attributeName="snmp_sys_name"/>
      </identification-criterion>
      <identification-criterion>
         <attribute-condition conditionType="approveAndContradict" includeNullValue="false"
attributeName="net_bios_name"/>
      </identification-criterion>
</identification-criteria>
```

In this example:

- A 66% match of **mac_address** from the connected **interface** CI types is required.
- If the number of identification candidates vs the CMDB with the same value of **mac_adress** is equal to or greater than 50, then this value is automatically excluded from further identification process.
- The **name** attribute must be the same.
- The **name** attribute is not case sensitive.
- A 66% match of the connected IP addresses is required.
- Both **name** and **routing_domain** of the connected IP address must be the same in order to match.

- The **bios_uuid** attribute must be the same.
- Only one of the identification criteria needs to be fulfilled for the reconciliation engine to find a possible match.

Example of the match 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.

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 *HP Universal CMDB 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 485.

Identification Rule Schema

Element		
Name and Path	**Description**	**Attributes**
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 481. The identification criteria may contain many **identification-criterion** elements. Can appear at most once.	
match (Identification-config)	The parent element for all the possible match criteria for the CI type. For details, see "Match Criteria" on page 481. 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

Element		
Name and Path	**Description**	**Attributes**
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
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

Element		
Name and Path	**Description**	**Attributes**
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		
Name and Path	**Description**	**Attributes**
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. autoExcludeThreshold **Description.** If the number of identification candidates with the same attribute value exceeds this threshold, then that value is automatically excluded from the identification process. **Is required.** Optional **Type:** • Positive integer. • A value of **0** disables this feature.
		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

Element		
Name and Path	**Description**	**Attributes**
		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
		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.

Element		
Name and Path	**Description**	**Attributes**
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
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

Element		
Name and Path	**Description**	**Attributes**
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 481. The verification criteria must contain at least one verification-criterion element. Can appear at most once.	
verification-criterion (Identification-config > match > verification-criteria)	This element defines a single verification criterion. The criterion may contain many conditions for verification.	**Name.** targetType **Description.** The derived CI type for which this criterion is valid. If this attribute is omitted, then the criterion is applied to any derived type. **Is required.** Optional **Type.** String
		Name. isTargetTypeDerived **Description.** Specifies whether the target type is a derived type of the current CI type. **Is required.** Optional **Type.** Boolean
		Name. numberOfConflictsToFail Identification **Description.** The number of conflicting conditions that will cause the current criterion to fail. Default Value: 1. **Is required.** Optional **Type.** Integer

Element		
Name and Path	**Description**	**Attributes**
validation-criteria (Identification-config > match)	The parent element for all possible validation criteria for the CI type. For details, see "Match Criteria" on page 481. The validation criteria must contain at least one validation-criterion element. Can appear at most once.	
validation-criterion (Identification-config > match > validation-criteria)	This element defines a single validation criterion. The criterion may contain many conditions for validation.	**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. numberOfConflictsToFail Identification **Description.** The number of conflicting conditions that will cause the current criterion to fail. Default Value: 1. **Is required.** Optional **Type.** Integer

Chapter 16

Reconciliation Priority

This chapter includes:

Reconciliation Priority Overview

Reconciliation Priority (conflict resolution) specifies how matched CIs are merged. You set these priorities in the Reconciliation Priority Manager.

For details about the reconciliation process and its rules, see "Entity Reconciliation" on page 479.

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 CMDB.
- 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 502.

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 498.

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. We first define a priority value for all attributes of **node**. This is optional. If omitted, the default value is 100.
2. 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.

How to Add Reconciliation Priorities to an Existing CIT

1. In Reconciliation Priority, select the required CI type in the CI Types pane.
2. In the CI Type Overrides pane, select the required integration and change the value in the **Priority** field to modify the integration's priority.
3. If you want to set the priority for a specific attribute of that CIT, click the **Add**  button in the Attribute Overrides pane to open the Add Attribute dialog box.
4. Select the required attribute from the list and click **OK**.
5. Modify the value in the Priority field. If you add the wrong attribute to the list, use the **Reset Attribute**  button to reset the Attribute Overrides list.

   Caution: This action clears all values in the Attribute Overrides list.
6. When all the changes for the selected CIT are finished, click the **Save**  button in the CI Types pane to save your changes.

Reconciliation Priority Schema

Element		
Name and Path	**Description**	**Attributes**
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 **Value:** -1,000,000 to 1,000,000 **Default**: 100
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.	

Element		
Name and Path	**Description**	**Attributes**
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:

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 *HP Universal CMDB Modeling Guide*. To change the priority of an attribute, do the following: • Click in the **Priority** field and enter a new value. This value can range from -1,000,000 to 1,000,000. • 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
	Click to expand the entire hierarchical tree structure.
	Click to collapse the hierarchical tree structure.

UI Element (A-Z)	Description
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 499.
	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. This value can range from -1,000,000 to 1,000,000. The default priority level for all items is 100. If you change the priority of an entry, the new value propagates downwards to all descendants of that particular CI type. 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. This value can range from -1,000,000 to 1,000,000. The default priority level for all items is 100. If you change the priority of an entry, the new value propagates downwards to all descendants of that particular CI type. 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 203.

For details about the reconciliation engine, see "Entity Reconciliation" on page 479.

To access	Do one of the following: • Select **Data Flow Management > Reconciliation Priority.** • Select **Data Flow Management > Integration Studio**, right-click an Integration point and select **Reconciliation Priority Manager** .
Relevant tasks	• "How to Work with Federated Data" on page 183 • "How to Work with Population Jobs" on page 183 • "How to Work with Data Push Jobs" on page 184

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.

Chapter 17

Populating UCMDB (Data-In)

This chapter includes:

Range Types

Range types apply different reconciliation rules and workflows to different environment types. There are two types that are available when configuring ranges- Data Center and Client.

To support different types of environments, the IP Address CI contains an attribute named **Lease Time** which stores the range type value. This value together with the routing domain determines the reconciliation rules and workflows that are applied to that range.

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

For information on how to configure range types, see "New/Edit Range Dialog Box" on page 62.

Data Center Type Ranges

The Data Center type is suitable for environments that have the following characteristics:

- IP addresses are stable due to long lease times or due to the consistent availability characteristics of the nodes and network.
- Nodes connects to the network using the same interfaces due to a single access technology.
- Few or no mobile users.
- Single domain environment.

Traffic Case

The traffic case is as follows:

1. Ping Sweep by ICMP job runs.
2. Node CI is created.
3. Host Connection jobs run.
4. Inventory Discovery jobs and Universal Discovery Agent related jobs run.

Reconciliation

Reconciliation behavior that occurs for Data Center type ranges is as follows:

If the IP addresses that are discovered during two unique discovery jobs are identical, the data is merged into a single IP Address CI.

Client Type Ranges

The Client type is suitable for environments that have the following characteristics:

- IP addresses are not stable due to short lease times or due to the inconsistent availability characteristics of the nodes and network.
- Nodes connects to the network using different interfaces due to multiple access technologies, therefore, the same IP address is bound to different interfaces at different times.
- Mobile users access the network from different domains in a multi-domain environment.
- IP addresses are not stable due to short lease times or due to the inconsistent availability characteristics of the nodes and network.
- Nodes connects to the network using different interfaces due to multiple access technologies, therefore, the same IP address is bound to different interfaces at different times.
- Mobile users access the network from different domains in a multi-domain environment.

Traffic Case

The traffic case is as follows:

1. Client SNMP Discovery job runs to discover ARP-enabled devices that provide IP/MAC pair information.
2. IP/MAC Address Harvesting job runs against SNMP devices to retrieve IP/MAC pair information.
3. New or updated IP/MAC pair information and a CallHomeEvent CI is reported to UCMDB.
4. The Host Connection job and the Call Home Processing job runs.
5. Inventory Discovery jobs and Universal Discovery Agent-related jobs run. However, if the Data Flow Probe cannot establish a connection with the discovery node or a job is waiting for other tasks to complete, the workflow is put into a parked state. A CallHomeEvent CI is received by UCMDB when the Universal Discovery Agent sends a call home message to the Data Flow Probe, or when a new IP/MAC address pair is harvested from an ARP cache job. As a result, a Call Home Processing job is triggered and the parked workflow is put into an activated state. Then, the Inventory Discovery jobs and Universal Discovery Agent-related jobs run. For more information on parked workflows and other traffic cases, see "Call Home Overview" on page 91.

Reconciliation

Reconciliation behavior that occurs for Client type ranges is as follows:

- If the IP Addresses that are discovered during two unique discovery jobs are different but the ARP/MAC values are identical, the data is merged into a single IP Address CI.
- If the IP Addresses that are discovered during two unique discovery jobs are different and the ARP/MAC addresses are null or undetermined, the data is merged into a single IP Address CI if the Interface IDs are identical.

Server-Side Data Normalization

Before populating the CMDB with new CIs, the server normalizes the incoming data as follows:

- When a CI of type **ip_address** is reported, if one of the **name** or the **ip_address_value** attributes contains data, the other is populated automatically.
- When a CI of type **ip_subnet** is reported, if one of the **network_netmask** or **ip_prefix_length** attributes is contains data, the other is populated automatically.
- When the **REPLACE_VALUE_WITH_VALUE_FROM_SYSTEM_PROPERTY** qualifier is defined for a particular attribute, the attribute is normalized with the specified system property value.

  For example, the **routing_domain** attribute, by default, contains the **REPLACE_VALUE_WITH_VALUE_FROM_SYSTEM_PROPERTY** qualifier where:

  - **CONSTANT_TO_REPLACE** data item is defined as **${DefaultDomain}**
  - **SYSTEM_PROPERTY_NAME** data item is defined as **default.domain**

  This means that if a CI of type **ip_address** is reported with **${DefaultDomain}** in the **routing_domain** attribute, then the **routing_domain** attribute is populated with the value in the **default.domain** setting.
- If the CI attribute's **Discovery Auto Truncate** (DDM_AUTOTRUNCATE) qualifier is enabled, then results of type STRING are truncated according to the database encoding setting.

  Note: By default, the database encoding is defined as UTF-8. This encoding can be changed in the Infrastructure Settings Manager, in the **Reconciliation Settings > Database Encoding** setting (**reconciliation.auto.truncate.db.encoding**). To access the Infrastructure Settings Manager, go to **Administration > Infrastructure Settings Manager**. For more details, see "Infrastructure Settings Manager Page" in the *HP Universal CMDB Administration Guide*.
- If the CI attribute has a case qualifier that is enabled, then the case of all of the results are normalized. The case qualifiers are:

Qualifier	Display Name	Description
TO_UPPER_CASE	**Upper Case**	Normalizes all results to upper case
TO_LOWER_CASE	**Lower Case**	Normalizes all results to lower case

  Note: The deprecated qualifiers, **DDM_AUTOUPPERCASE** and **DDM_AUTOLOWERCASE**, can also be used to normalize results (to upper case or lower case respectively, if enabled.
- If the **Discovery Auto Trim** (DDM_AUTOTRIM) qualifier for the attribute is enabled, any leading and trailing spaces and tabs removed from the string.

For more information about attributes, see "CI Type Attributes" in the *HP Universal CMDB Modeling Guide*.

Data-In Service

After the Identification service runs, the identified data is merged and inserted into the UCMDB 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 UCMDB CIs. The service can:

- merge all matched CIs into one CI
- ignore the input CI

To make this decision, the Data In service uses match criteria. The process is as follows:

1. Input CIs are merged with each matching UCMDB CI.
2. For each pair of CIs resulting from this merge, match (verification and validation) criteria are run.
   - If at least one pair does not pass the match criteria check, the CIs are not merged.
   - If all pairs pass the match criteria check, the CIs are merged.
3. If the CIs are not merged, the Data In service 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.

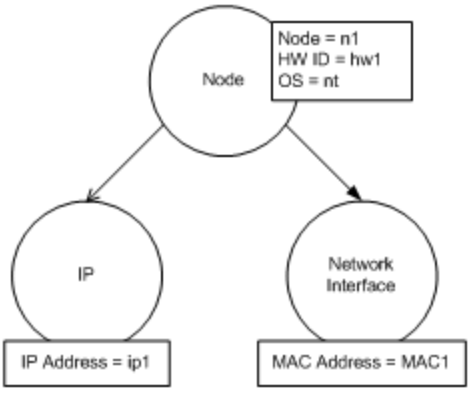
For an example of multiple CI matching, see:

- "Multiple CI Matching - Example 1" below
- "Multiple CI Matching Example 2" on next page

Multiple CI Matching - Example 1

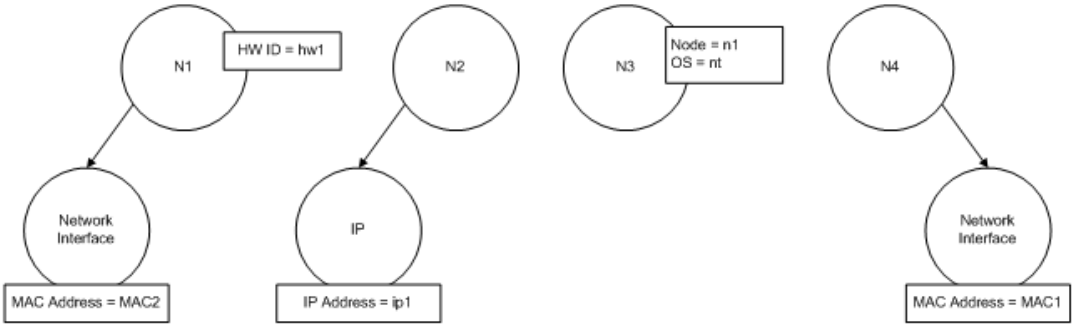
The following example demonstrates how the Data-In service matches multiple with different identification criteria where there are no conflicts.

1. The input bulk data is received.

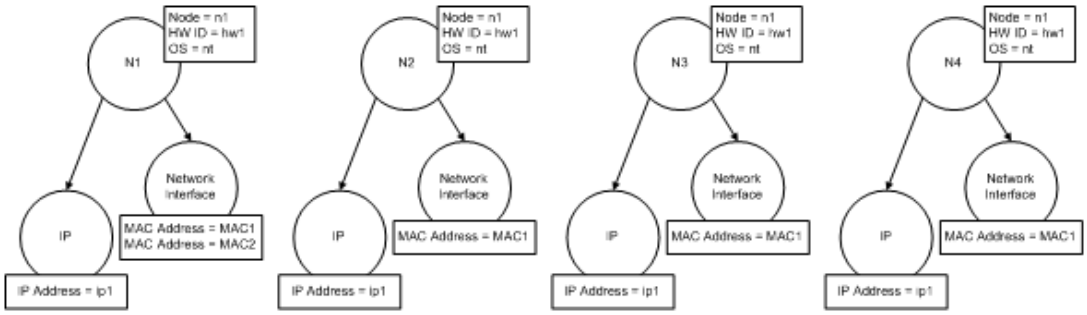


2. The service identifies matching CIs in the CMDB

In this example, the input node matches four nodes in the CMDB having different identification criteria.



3. The service merges the input CI with each matching CI in the CMDB.



4. The service checks for conflicts between the resulting merged CIs.

   Nodes N2, N3, and N4 are the same CI; therefore, it is obvious that there is no conflict between them. The only difference between nodes N1 and N2 is the additional MAC address in N1. Since the MAC address match validation criterion uses the **contains** operator, there is no conflict between nodes N1 and N2 either.

   Conclusion: There are no conflicts with any of the CMDB matching nodes.

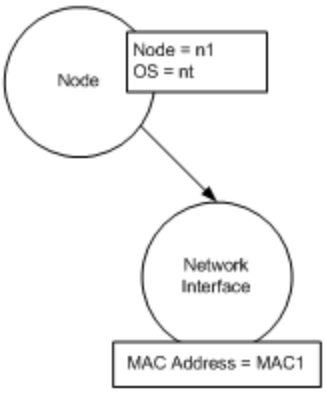
5. **Decision:** The Data-In service merges all of the CIs into one CI.

   For details on how the CIs are merged into one CI, see "Reconciliation Priority Overview " on page 496

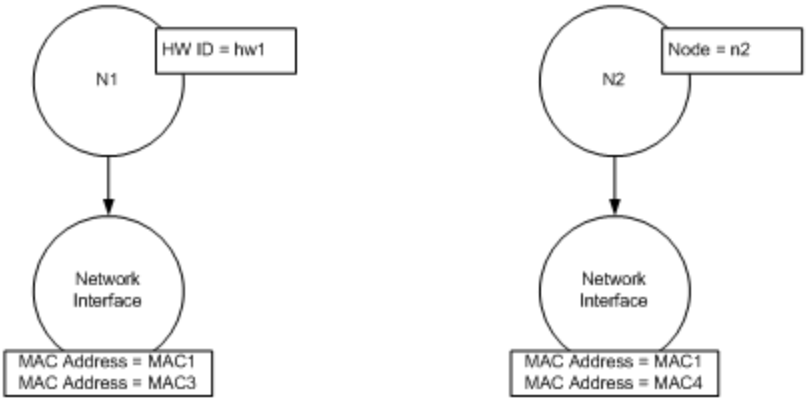
Multiple CI Matching Example 2

The following example demonstrates how the Data-In service handles multiple CIs with different identification criteria where there are conflicts.

1. The input bulk data is received.

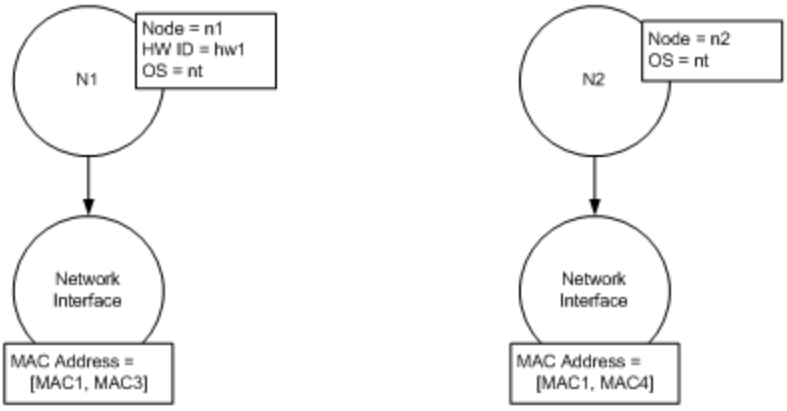


2. The service identifies matching CIs in the CMDB



3. The service merges the input CI with each matching CI in the CMDB.

   In this example, the input node matches two nodes in the CMDB having different identification criteria, but there are conflicts with the matching nodes in CMDB: N1 and N2 have conflicting MAC address match criteria.



4. **Decision:** The CIs are not all merged to one CI.

Note: 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.

Appendix: Troubleshooting and Limitations

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

- "Troubleshooting" below
- "Universal Discovery Limitations" on page 513

Note:

- For details on using the log files to perform basic troubleshooting, see:
  - "Data Flow Probe Log Files" on page 59
  - "Data Flow Management Log Files" in the *HP Universal CMDB Administration Guide*

Troubleshooting

- "Troubleshooting" above
- "Discovery Results Do Not Appear in the Topology Map" below
- "Networks and IPs" below
- "TCP Ports" on next page
- "Discover Resources on a Windows XP Machine" on next page
- "Troubleshooting" above

Discovery Results Do Not Appear in the Topology Map

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

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

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

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.

Universal Discovery Limitations

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

  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.


Java™
COMPATIBLE