HP Universal CMDB Configuration Manager

For the Windows and Linux

Software Version: 9.30

User Guide

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 - 2011 Hewlett-Packard Development Company, L.P.

Trademark Notices

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

Oracle is a registered trademark of Oracle and/or its affiliates.

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

HP Universal CMDB Configuration Manager (9.30)

Chapter 1

Introduction to Configuration Manager

This chapter includes:

HP Universal CMDB Configuration Manager Overview

Configuration Management is the ITIL V3 process responsible for the organization's single source of information for the IT which supports the business (the CMS - Configuration Management System). It ensures that there is a complete and accurate picture of the IT infrastructure and software, thus improving the quality of most ITIL processes and better facilitating business decision-making. In addition, Configuration Management ensures the health of the organizational IT, in order to minimize disruptions to the business.

HP Universal CMDB Configuration Manager (Configuration Manager) provides the tools to help the system manager better control the CMS data. It focuses primarily on analyzing and controlling the data in the CMS, as the ITIL v3 directs. Configuration Manager provides an environment for controlling the CMS infrastructure, which encompasses many data sources and serves a variety of products and applications.

Configuration control ensures that there are adequate control mechanisms over CIs while maintaining a record of changes to CIs, versions, location and custodianship/ownership. Control of the physical or electronic assets and components of the infrastructure ensures that the configuration data is aligned and up to date with the physical world.

Configuration Modeling and Analysis

One of the basic areas of functionality in Configuration Manager is the ability to measure your IT environment against set standards. The underlying theory is that CIs serving the same purpose should have a similar configuration, to reduce maintenance costs and improve predictability. The Configuration Analysis module enables you to compare selected composite CIs to a configuration model which captures a standard in the organization. This can help you measure how similar they are.

The analysis consists of a comparison between the selected CIs and a custom configuration model which you construct to meet your organization's needs. The criteria for determining the degree of similarity between the CIs and the model include both the topology of the composite CIs as well as selected attributes of the CIs. The analysis is an iterative process that consists of two steps - model definition and comparison analysis. You determine a model, compare it against a given set of CIs, and drill down into the details of the comparison to locate configuration discrepancies or refine the model and rerun the comparison.

One use-case of this analysis is the ability to compare the configuration of different CIs in different environments. For example, comparing an application in the production environment to the same application in the staging environment could help to provide an explanation for production incidents originating under a tested configuration.

For details on the configuration analysis process, see .

Offline Analysis

Configuration Manager performs an asynchronous offline analysis process that updates the information appearing in managed views. Periodically, UCMDB is polled for updated CIs. The next time a view is opened in Configuration Manager, the updated information is displayed. According to the refresh rate that you specify, this analysis can occur either:

- daily at a time that you specify

- each time a change is detected on one of the CIs, according to the Offline Analysis repeat interval.

For details about the refresh rate and how to specify the offline analysis settings, see "System Settings Page" (on page 172).

Configuration Policies

Configuration policies are rules that define standards for an organization. These standards can be applied to the managed environments (views) to continuously monitor their compliance with those standards. When you apply a policy to a view, Configuration Manager checks whether the CIs in the view satisfy the policy or not. You can apply several policies to a view simultaneously.

The **policy status level** of a view is based on the sum of all the policies applied to the view. The view's policy status level is the percentage of CIs in the view that satisfy the relevant policies.

One type of configuration policy you can apply is the **baseline policy**, which extends the Configuration Analysis functionality by saving a configuration model to serve as the baseline definition of a policy. Instead of comparing an individual CI to a baseline, you can compare all the CIs of that type in the view to the baseline by applying the policy to the view. In this way, you can ensure that CIs of the same type comply with the defined baseline, and that new CIs added to your system are also constructed in accordance with the baseline. For details on baselining, see "Baselining" (on page 63).

Another type of configuration policy is the **topology policy,** which is based on the Topology Query Language (TQL) used in UCMDB. A topology policy defines the desired topological configuration (the set of CIs and relationships between CIs).

An example of a use-case for defining a policy is the ability to ensure that any business-critical application is highly available and that the supporting servers do not physically reside in the same place in order to improve its resiliency in case of disaster.

For details on defining and managing policies, see "Configuration Policy Management" (on page 61).

Data Control - Actual and Authorized States

Configuration Manager enables you to control the data in your configuration management system by managing different states of the views.

The **actual state** is the service topology and configuration as it is currently being reported by the data sources of the configuration management system (for example, the Discovery module).

The **authorized state** is a controlled state of the service which indicates the correct configuration of the service according to its configuration manager.

Different products, processes and people are interested in different information regarding the CI, according to their needs. For example, when responding to an application error, there is a need to see the actual state of the servers running this application. This involves identifying the servers and the software installed on them. In addition, when signing a Service Level Agreement, it is important to define the authorized configuration of the servers. The actual configuration is not necessarily the same as the authorized one (perhaps an unauthorized change has occurred), and the configuration will not necessarily be the same a month from now (perhaps additional changes will be made by then). The authorized state provides a protected environment for the consumption of the portfolio with data that is less current but more stable and reliable.

Configuration Manager displays changes in the actual state of the service and enables you to authorize them. When you authorize changes in the actual state of a view, the state becomes the new authorized state of the view.

You can review the changes to composite CIs manually, and choose to authorize them on an individual basis. Alternatively, you can set conditions for automatic state transition for the entire view. All the changes in the view can then be authorized when the automatic state transition is executed, if all the conditions are satisfied.

For details on managing the different states, see "State Management" (on page 107). For details on automatic state transition, see "View Management" (on page 46).

Historical Comparison

A configuration manager often needs to view configuration data from the past or a history of changes in order to understand the root cause of a problem and avoid repeating mistakes. Configuration Manager enables you to look into the past of either the actual or the authorized state using the Historical Comparison modules.

A snapshot is a configuration of a view recorded at a specific date and time. Comparing snapshots enables you to scan for a specific change that occurred in the past using an advanced user interface that highlights the changes between snapshots taken at different times as well as changes from the current configuration.

Configuration Manager automatically takes snapshots of the actual state of a view whenever a change occurs. It also takes a snapshot of the view at each authorization. The snapshots are recorded in the CMS and remain as a fixed historical record. You can then compare two snapshots of the same view in the same state to track changes in the environment over time. The Actual State Historical Comparison module displays snapshots of the actual state of a view and the Authorized State Historical Comparison module displays snapshots of the authorized state of a view.

An example of a scenario where snapshot comparison could be helpful might be a company's portal whose performance has been degraded over the past week. In response to customer complaints, the administrator would investigate it by comparing the current state of the environment with its snapshot from a week ago. He can then examine all the changes to determine which change may have caused the performance degradation.

For details on snapshot comparison, see "Historical Comparison" (on page 120).

Topology Mode and Inventory Mode

Configuration management can be conducted from a topology perspective or from an inventory perspective. A service owner may prefer to view the complete service topology from the highest level business service CI down to the hardware CIs, while a manager focusing on a specific CI type, such as the database administrator, may want to see a list consisting of many CIs of the same type.

To address this issue, Configuration Manager offers two different modes for viewing each managed environment:

- **Inventory mode.** A filterable list of CIs
- **Topology mode.** A topological graph

Inventory mode enables you to filter large lists of composite CIs and to focus on subsets of interesting CIs, such as CIs that have changed or CIs that are in breach of a policy. Topology mode provides a broader graphical presentation of the service topology.

System Operation Automation

Configuration Manager provides the ability to use predefined flows from HP Operations Orchestration to automate standard system operations. You create an automation by importing a flow from HP Operations Orchestration.

You can run a controlled or non-controlled automation. The controlled automation functionality is also referred to as automatic risk visualization. A controlled automation provides an awareness of the possible risk involved in automation executions implemented from within Configuration Manager.

Automation policies enable you to determine when there is a high risk in running an automation. All automation policies are managed from the Automation Policy Management module. They enable you to define restrictions based on the automation execution information and the impact on the CI on which the automation was run.

For information on how to run a controlled or non-controlled automation, see "Run a Controlled or Non-Controlled Automation" (on page 134).

For information on how to define an automation policy, see "Define an Automation Policy" (on page 71).

Use Cases

The following are some examples of how Configuration Manager can be used:

- **View your servers**

  As a system administrator, you can view your servers and their details (attributes, CPUs, file systems, and IP addresses), as well as the high-level relationships between them.

- **Investigate your hardware**

  As a system administrator, you can quickly see the different types of CPUs used in your physical servers.

- **Establish a configuration baseline for a lab**

  As a lab administrator, you can analyze the configuration of your servers and establish a baseline that best represents the current configuration of (most of) your servers.

- **Model and view an application service tree**

  As an application owner, you can model and view your application service tree from the business layer through your application and software layers down to your infrastructure layers.

- **Investigate and isolate configuration changes that may have caused problems in your application.**

  As an application owner, you may have an application that suffers from degraded performance that started some time ago. You can isolate configuration changes that happened in your application service tree during that time period that may have caused the problem.

- **Track changes that occur in your application service tree**

  As an application owner, you can track and acknowledge changes that occur in your application service tree.

- **Automatically acknowledge changes (reduce manual tracking)**

  As an application owner, you can track and acknowledge changes that happen in your application service tree, but you want an option to manually track only interesting changes while automatically acknowledging changes that do not violate predefined conditions.

- **Create a compliance stack for your application service tree**

  As an application owner, you can create policies that cover your applications' configuration compliance.

Best Practices for Working with Configuration Manager

The following approach is recommended as a best practice for adopting the authorized state for applications that require high quality configuration data:

- Begin by determining the data you need to consume. Define views accordingly and add these views to be managed in Configuration Manager.

- Set automatic state transition conditions for those views to authorize all changes in the view. This essentially copies the configuration of the actual state to the authorized state.

- Configure your applications to consume data from the authorized state of the views, rather than the actual state.

- Gradually begin controlling the data in these views by applying policies, changing the automatic state transition rules, and manually authorizing changes. In this way, you can adopt the configuration authorization process while maintaining the ability to consume your data.

Chapter 2

Content Management

This chapter includes:

Content Management Overview

To work with managed views in Configuration Manager, you first need to prepare the content coming from UCMDB. The managed views contain IT elements organized such that you can analyze and control the CMS data using Configuration Manager.

One of the methods of restructuring the content in preparation for Configuration Manager is **CI composition**. CI composition is a process whereby a specific CI type is selected as the leading CI, and all the CIs which are part of that CI are grouped under it as component CIs. For example, CPUs are part of a host, so the composite CI of a host encompasses the CPUs as well.

Using composite CIs to display the content:

- is a more intuitive way of presenting the data. You would usually refer to a CPU only in the context of its host.

- helps to simplify the topology, since the topology is only mapped on the level of the composite CIs. Because composite CIs can be composed of many component CIs, the topology map is much simpler.

- enables you to manage a group of related CIs from the leading CI. All changes in the component CIs are captured as a change to the leading CI. You can drill down from there to see details of the component CIs.

The composite CIs that form the content of the managed views are defined by folding rules that detail which CI types are treated as components of composite CIs. You set the folding rules for your composite CIs in the CI Type Manager in HP Universal CMDB. For details, see "Set Folding Rules for Composite CIs" (on page 137).

Another method of organizing the data is by setting the layer and classification definitions for the composite CITs. **Layers** are categories used for grouping composite CITs functionally. Examples of layers include Business, Software, and Infrastructure. **Classifications** are categories for grouping the composite CITs into finer divisions.

A further step in preparing the UCMDB content for Configuration Manager involves defining managed and comparable attributes for the CITs. **Managed** attributes are the CIT attributes which you want to manage in Configuration Manager. They are the attributes that are copied to the authorized state when a change is authorized as well as tracked for their history. You can use them in defining policies. **Comparable** attributes are those managed attributes which are used for CI Baseline comparisons in Configuration Manager.

The values for layers and classifications, as well as the managed attributes and comparable attributes, are defined in the CI type definition in UCMDB.

Requests for Change

Configuration Manager imports from UCMDB requests for change (RFCs) that were opened in Service Manager. Every RFC is associated with at least one CI. The RFCs for a CI are displayed in the Related RFCs tab of the Comparison Details pane in the State Management and Historical Comparison modules.

You can filter the RFCs retrieved based on the RFC properties, the CI types, and the number of days since the RFC was scheduled to be completed using the settings in **System > Settings > Application Management > RFC** under **Fetched RFCs Criteria**. You can also select the RFC properties to be displayed using the settings under **RFC Display**.

Note: The filter by the scheduled RFC completion date is relevant for the State Management module. In the Historical Comparison modules, only RFCs scheduled for completion within the range of the selected snapshots are displayed.

It is a best practice to check the Related RFCs tab for a CI indicated as in breach of a policy, as part of the investigation of the causes of the breach.

Configuration Manager Content Workflow

This task describes the workflow for managing Configuration Manager content.

This task includes the following steps:

1. **Prerequisites**

   Start by examining a view in UCMDB. Consider the purpose of the view and how you want to display the data in composite CIs.

2. **Define the CI Composition**

   When you have decided on rules for the scope of the composite CIs, edit the existing folding rule definitions for the relevant composite CIs. For details, see "Set Folding Rules for Composite CIs" (on page 137).

   When Configuration Manager is started, or when the folding rules in HP   Universal CMDB are modified, Configuration Manager automatically generates relevant perspectives in UCMDB based on the folding rules defined in HP Universal CMDB. These perspectives are located in the **Configuration Manager - Do not change** folder in the Resources pane of Modeling Studio.

   After defining your folding rules, go to the Configuration Explorer in Configuration Manager and verify that the view is appearing correctly according to the defined rules.

3. **Define Layers and Classifications**

   Consider the layers and classifications in which each composite CIT belongs. Set these definitions for the composite CITs using the **layer** and **classification** static attributes in the CI Type Manager in UCMDB. The colors of the layers and classifications are defined in Configuration Manager in **System > Settings > Application Management > Topology Presentation > Topology Layout**.

   Note: It is not necessary to define layers and classifications for the component CITs.

4. **Define Managed Attributes**

   Decide which CI Type attributes of all CI types (both composite and component) should be defined as managed attributes. Set these definitions by selecting the **Change Monitored** qualifier for the selected attributes in the CI Type Manager in UCMDB.

   It is recommended that key attributes of CITs be defined as managed attributes, unless they do not contain meaningful values for users (such as Root Container).

   > **Note:** Only managed attributes are visible in Configuration Manager and are copied to the authorized state of the view during authorization.

5. **Define Comparable Attributes**

   Decide which managed attributes of all CI types (both composite and component) should be defined as comparable. Comparable attributes are used for CI comparisons in Configuration Manager. Set these definitions by selecting the **Comparable** qualifier for the selected attributes in the CI Type Manager in UCMDB.

   For composite CITs, it is recommended that the key attributes not be defined as comparable. For component CITs, it is recommended that the key attributes be defined as comparable if they contain meaningful values for users.

6. **Define Comparison Matching Rules**

   You can define matching rules for the comparable attributes of certain CITs, which provide guidelines for the comparison between component CIs. A matching rule tells Configuration Manager which attribute to use in identifying parallel CIs for comparison.

   You can define multiple attributes in a CIT matching rule, with a different priority for each attribute (the primary attribute is used first, the secondary one next, and so on). The matching rules are defined in the CI Type Manager in HP Universal CMDB. You can access HP Universal CMDB from Configuration Manager.

   a. Select **Administration** > **UCMDB Foundation** to open HP Universal CMDB.

   b. Go to **Managers** > **Modeling** > **CI Type Manager**.

   c. Select **CI Types** from the list box in the CI Types pane.

   d. In the right pane, click the **Matching Rules** tab.

   e. Define matching rules for attributes to determine which CIs should be compared. For details, see the HP Universal CMDB documentation.

   > **Note:**
   > ○ Matching rules are not relevant for composite CITs.
   > ○ Matching rules can only be defined for attributes defined as comparable.

Manage Configuration Manager Content - Use Case

This use-case describes the Configuration Manager content workflow for an IIS Web Server view.

> **Note:** For a task related to this scenario, see "Configuration Manager Content Workflow" (on page 23).

This scenario includes the following steps:

1. **Background**

   Consider a view in UCMDB that includes CIs of the following types:

   - **IIS Web Server**

   - **Node**

   - **Oracle**

   To prepare the view for working in Configuration Manager, you can define various settings, as described in the following steps.

2. **Set the CI Composition in HP Universal CMDB**

   Go to **Administration > UCMDB Foundation** to open HP Universal CMDB. In HP Universal CMDB, select **Managers > Modeling > CI Type Manager**. Select **Calculated Relationships** from the list box in the CI Types pane. Under **Calculated Links**, select **Folding Rules (Configuration Manager)**. Locate the following folding rules of IIS Web Server.

   - **IIS Application Pool**

   - **IIS Web Service**

   - **IIS Web Site**

     The rules further define **IIS Web Dir** to be a component CI of IIS Web Site, and **Configuration File** to be a component CI of IIS Web Dir.

   If you want to modify any of these folding rules, make the required change in HP Universal CMDB. For details, see "Set Folding Rules for Composite CIs" (on page 137).

3. **Set Layer Definitions**

Go to the CI Type Manager in UCMDB. Note that the **layer** attribute of the CI types in our view is defined as follows:

- IIS Web Server - Software

- Node - Infrastructure

- Oracle - Software

If you want to modify any of these definitions, make the required change in the layer attribute of the relevant CIT.

4. **Set Classification Definitions**

Go to the CI Type Manager in UCMDB. Note that the **classification** attribute of the CI types in our view is defined as follows:

- IIS Web Server - Web server

- Node - Infrastructure

- Oracle - Database

If you want to modify any of these definitions, make the required change in the classification attribute of the relevant CIT.

5. **Set Managed Attributes**

Select the CIT attributes to be defined as managed attributes. For example, for IIS Web Server the attributes **Version** and **Name** are defined as managed by default. The attribute **StartupTime** is not defined as managed by default, because it is not considered part of the configuration. You can change the default definition of an attribute to fit the needs of your system.

To define an attribute as managed:

a. Go to the Attributes tab of the CI Type Manager in UCMDB.

b. Select the required attribute and click the **Edit** button 🖉 . The Edit Attribute dialog box opens.

c. Select the Advanced tab and select the check box for the **Change Monitored** qualifier. Click **OK**.

d. Save your changes.

> **Note:** Only managed attributes are visible in Configuration Manager and are copied to the authorized state of the view during authorization.

6. **Set Comparable Attributes**

Decide which managed attributes should be defined as comparable. Comparable attributes are used for CI comparisons in Configuration Manager.

For example, for IIS Web Server, the **Version** attribute is appropriate for comparison (comparing the version of two web servers). However, the **Name** attribute would not be appropriate for a CI comparison, as web servers generally have different names.

To define an attribute as comparable:

a. Select **Administration** > **UCMDB Foundation** to open HP Universal CMDB.

b. Go to the Attributes tab in **Managers** > **Modeling** > **CI Type Manager**.

c. Select the required attribute and click the **Edit** button 🖊. The Edit Attribute dialog box opens.

d. Select the Advanced tab and select the check box for the **Comparable** qualifier. Click **OK**.

e. Save your changes.

7. **Define Matching Rules**

For component CITs, you can define matching rules for attributes to determine which CIs should be compared. For the component CITs **IIS Application Pool** and **IIS Web Service**, define the **Name** attribute as a matching rule in the CI Type Manager in HP Universal CMDB.

To define matching rules:

a. Select **Administration** > **UCMDB Foundation** to open HP Universal CMDB.

b. Go to **Managers** > **Modeling** > **CI Type Manager**.

c. Select **CI Types** from the list box in the CI Types pane.

d. In the right pane, click the **Matching Rules** tab. When selecting IIS Web Service/IIS Application Pool, you can see that the **Name** attribute appears in the Matching Rules pane.

As a result, when composite CIs of type IIS Web Server are compared, the IIS Application Pool and IIS Web Service CIs are matched by their names.

Troubleshooting and Limitations

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

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

- Wait a few minutes. The default interval between analysis process executions is 10 minutes. This value is configurable in under **System > Settings**.

- Execute a JMX call to run the offline analysis calculation on the relevant view.

- Go to **Administration > Policies > Configuration Policies**. Click the **Recalculate Policy Analysis** button. This invokes the offline analysis process for all views (which may take some time). You may also need to make an artificial change to one policy and save it.

Problem. When you click **Administration > UCMDB Foundation**, the UCMDB login page appears.

Solution. In order to access UCMDB without logging in again, you need to enable single sign-on. For details, see Enable LW-SSO between Configuration Manager and UCMDB in the *HP Universal CMDB Deployment Guide*. Additionally, ensure that the Configuration Manager user logged on is defined in the UCMDB user management system.

Problem. The **Matching Rules** tab does not appear in HP Universal CMDB when you go to **Managers > Modeling > CI Type Manager**, and select **CI Types** from the list box in the CI Types pane.

Solution. Go to **Managers > Administration > Infrastructure Settings** in HP Universal CMDB
and set **Enable** Configuration Manager **Matching Rules** as `True`. After you log out and then log in
again, the Matching Rules tab appears in the CI Type Manager.

Chapter 3

Federating Data to UCMDB

This chapter includes:

Federated Data Overview

> **Note:** To federate data from Configuration Manager, you must have:
>
> - UCMDB 9.04 with CUP3 or later
>
> - Content Pack 10.

The federation mechanism that is built into HP Universal CMDB enables UCMDB to be used as a contact repository for sharing data among external applications, without duplicating it. By federating data from Configuration Manager to UCMDB, external applications can consume its analysis information in various ways:

- Use UCMDB's reporting functionality to generate and schedule reports on top of Configuration Manager's data.

- Consume Configuration Manager's data in other HP applications, such as HP Business Service Management.

- Use Configuration Manager's analysis data as a basis for making decisions in other applications.

Configuration Manager exposes the following data for federation:

- **Policy compliance status** data includes information about current policy result data for managed CIs and the associated policies.

- **Authorization status** data includes information about the authorization status of managed CIs.

UCMDB provides the class model for the schema for the model to be shared, and uses a federation TQL query as the way to consume data in UCMDB on the fly. For details, see "Federating Policy Compliance Data" (on page 30).

UCMDB provides two adapters to federate data from Configuration Manager to UCMDB. The adapters sit on top of CMDB and carries out the operation to bring the federated data from Configuration Manager. For details about these adapters, see "Federation Workflow with UCMDB" (on page 36).

For details, see "Federating Policy Compliance Data" (on page 30) and "Federating KPIs" (on page 33).

Federating Policy Compliance Data

To enable the federation of data between Configuration Manager and UCMDB, the Policy and PolicyResult CI types were added to the UCMDB class model.

Configuration Manager federates its policy data into these models:

Model	Description
Policy	• Name—the name of the policy as it appears in Configuration Manager. • Description—the description of the policy as it appears in Configuration Manager. • PolicyDefinedBy—the application in which the policy was defined. (UCMDB-CM)
PolicyResult	• Compliance result—the latest status of the policy (0% if the policy is in breach, 100% if the policy is compliant). • Compliance status—the latest result of the policy (either in breach or compliant).

The following sections contain additional information about federating KPIs:

- Supported TQL Queries

- Creating Reports

Supported TQL Queries

The basic way to consume data in UCMDB is by creating TQL queries that retrieve the information that you want from the CMDB. The TQL queries that support federated data from UCMDB are:

- Get policies

Create a TQL query that filters for the **Policy** CI type. This will retrieve all configuration properties.

- Get policy results for CIs
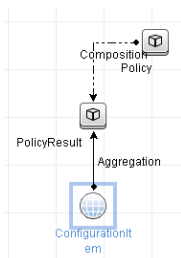
This will retrieve all attached policy results and their associations to a policy.

You can filter policies by name, description, and PolicyDefinedBy query node properties, and policy results by the compliance results and status as well.
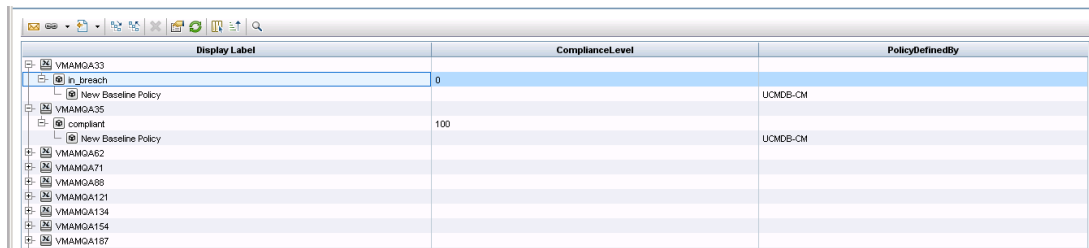
For details about creating TQL queries, see the *HP Universal CMDB Modeling Guide*.

Creating Reports

You can generate reports in UCMDB with the federated data, using UCMDB's topology reporting capabilities. The types of reports that can be created with the federated data are:

- **Policy compliance report**

  A policy compliance report displays the raw data about policy results of CIs, per policy.
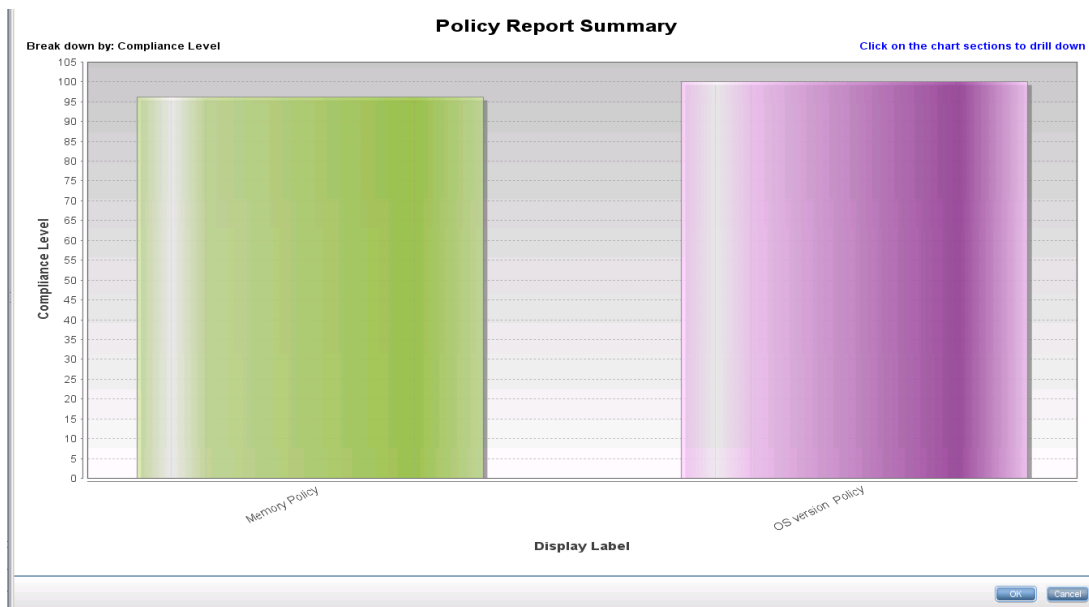

  The following out-of-the-box policy reports are provided:

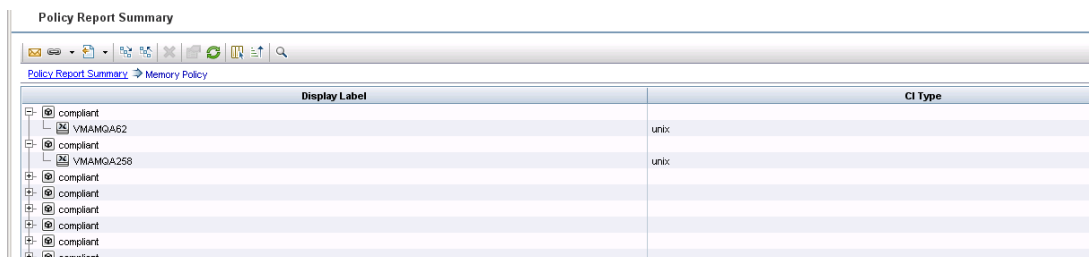 - Unix Policy Compliance

  - Unix with Oracle Policy Compliance

  - Windows Policy Compliance

- **Policy compliance summary report**

  A policy compliance summary report displays the compliance level of the policies over the CIs in the view.

  You can click on a policy and drill down to the CI list:

For details about creating reports, see "Federation Workflow with UCMDB" (on page 36).

Federating KPIs

KPIs (Key Performance Indicators) measure the health of a system according to predefined performance indicators. In the case of Configuration Manager, the KPIs that are supplied are **policy compliance** and **authorization level**. Configuration Manager federates two KPIs: policy compliance and authorization status. Note that the policy information that is federated by the policy adapter is raw data, and for policy KPIs, the information is modeled as a measurement of policy compliance for KPIs.

These KPIs are measured at two levels:

- Composite CI (for example, host).

- Business Service (aggregated on the configuration related to the Business Service). For details, see "Identifying Business Service Views" (on page 34).

Configuration Manager federates its KPI data into these models:

Model	Description
Policy compliance KPI for composite CI	- data_origin—the source of the KPI (Configuration Manager) - description—a system-generated description that provides additional information about the KPI value - kpi_name—the name of the KPI (**policy_compliance**) - kpi_status—the status of this KPI (**OK**, if the policy compliance for the composite CI is 100%; otherwise, **Warning**) - kpi_unit_of_measure—unit of measurement (%) - kpi_value—the percentage of policy compliance (for example, if a CI has three satisfied policies out of five, it is 60% compliant)
Policy compliance KPI for business service	- data_origin—the source of the KPI (Configuration Manager) - description—a system-generated description that provides additional information about the KPI value - kpi_status—the status of this KPI (**OK**, if the policy compliance for the all the composite CIs in the business service is 100%; otherwise, **Warning**) - kpi_unit_of_measure—unit of measurement (%) - kpi_value—the percentage of policy compliance for CIs in the scope of the business service level (for example, if a business service has three compliant CIs out of five, it is 60% compliant)
Authorization status KPI for composite CI	- data_origin—the source of the KPI (Configuration Manager) - description—a system-generated description that provides additional information about the KPI value - kpi_name—the name of the KPI (**authorization_status**) - kpi_status—the status of this KPI (**OK**, if the authorization status of the states for the composite CI is identical; otherwise, **Warning**)

Model	Description
	• kpi_value—the value of this KPI, as a percentage (0-not authorized; 100-authorized))
Authorization status KPI for business service	• data_origin—the source of the KPI (Configuration Manager)
• description—a system-generated description that provides additional information about the KPI value
• kpi_status—the status of this KPI (**OK**, if the authorization status of the states for the all the composite CIs in the business service is identical; otherwise, **Warning**)
• kpi_value—the value of this KPI, as a percentage (0-100)

If a CI is in the scope of multiple views, the most updated result of the policy compliance or authorization status is taken

The following sections contain additional information about federating KPIs:

Identifying Business Service Views

Business services are modeled in UCMDB as CI types. The goal is to identify business services with views that contain the entire (or any portion of it) configuration that is related to the business service, and to supply aggregative policy compliance and authorization information.

The standard way to do this in UCMDB is to create a Business Service CI, and to connect it to its business applications in such a way that each business application points to some "anchor" configuration that is identified by the application (usually software, such as a web service or DB schema), and connected to a resource that is solely dedicated to the business application. Once this anchor exists, perspectives (for example, hardware, virtualization, software, and so on) can be applied, and the configuration that is related to the business service can be viewed.

While it is most common to identify a business service according to this structure, a more general approach can be used:

1. Locate all views that contain the required CI.

   Include any views that were created the standard way for a business service, but can match additional cases.

2. Check if these views contain more than one business service. If so, these views are not identified with the business service.

   Narrow the possible cases, since multiple business services in the same view cannot describe a configuration that is solely related to one business service.

3. If there are multiple conditions identified with the business service, merge their configurations as follows:

   Because multiple views each may give some perspective about the configuration of the business service, merging these configurations can give complete information about the KPI for the service.

Two types of KPIs can be created for business services:

- The policy compliance KPI is calculated as the aggregation of the policy result on the entire configuration in the scope of the views that are identified with the business service. The policy aggregation is performed on the aggregated policy status of each CI of the business service.

- The authorization status KPI is calculated as the aggregation of the authorization status on the entire configuration in the scope of the views that are identified with the business service.

Supported TQL Queries

The following diagram displays how KPIs are modeled in UCMDB:
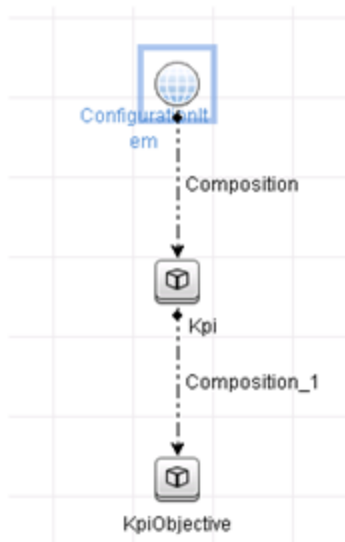
Creating Reports

The following out-of-the-box KPI reports are provided:

- Business Service KPI

- Unix KPI

- Unix with Oracle KPI

- Windows KPI

For details about creating reports, see .

Consuming KPIs in BSM

Using the federation functionality in UCMDB, the data that is federated by Configuration Manager can be optionally consumed by other applications. BSM version 9.10 or later provides such integration capabilities, and the KPIs that are federated by Configuration Manager can be viewed in

BSM. For details about how to setup the integration, see "Consume the KPIs in HP Business Service Management" (on page 42).

Once the integration is set up appropriately, you can consume KPIs for CIs in MyBSM. KPIs that enter BSM via federation are displayed in the External KPIs area of the KPIs component. For details, see the section about the KPIs Component User Interface in *Using Service Health*. For general information on how to display components in BSM, see " How to Open Pages and Components in Service Health" in *Using Service Health*.

Federation Workflow with UCMDB

This workflow provides a brief overview of the steps to be performed in UCMDB, in order to consume federated data from Configuration Manager.

This task includes the following steps:

- "Prerequisites" (on page 36)
- "Create an integration point to federate policy compliance data" (on page 36)
- "Create an integration point to federate KPI data" (on page 37)
- "Create policy reports based on the CIs in a view or a custom TQL query" (on page 38)
- "Create summary policy reports based on the CIs in a view or a custom TQL query" (on page 39)
- "Create KPI reports" (on page 41)
- "Consume the KPIs in HP Business Service Management" (on page 42)

Prerequisites

Make sure that you have installed UCMDB with HP Discovery and Integration Content Pack 10.00.

Create an integration point to federate policy compliance data

1. In UCMDB, enter the Data Flow Management module.

2. Click ![icon] to create a new integration point.

3. Set the following adapter properties:

Field	Description
Adapter	Click ![icon] and select **CMPolicyAdapter**.
Credentials ID	Do the following: a. Click ![icon]. b. Select **Generic DB Protocol (SQL)** and click **OK**. c. Click ![icon] to add the credentials to connect to the Configuration Manager database. These should be the same credentials that were provided during the installation of Configuration Manager. d. When finished, click **OK**

Field	Description
DB Name/SID	The database name or schema ID.
DB Type	Specify Oracle or MSSQL, as required.
Hostname/IP	Provide the host name or IP address of the Configuration Manager database.
Integration Name	Enter a name for the new integration point.
Port	Enter the port number that is used for communication with the Configuration Manager database.

4. Click **Test Connection** to make sure that you have configured the integration point correctly. If the test fails, see "Troubleshooting and Limitations" (on page 43)

5. Click **OK** to save the integration point.

6. Select the Policy and PolicyResults CI types in the Supported and Selected CI Types tree.

7. Click 🖫 to save the integration point.

For further details about creating integration points, see the section about the Integration Studio in the *HP Universal CMDB Data Flow Management Guide*.

Create an integration point to federate KPI data

1. In UCMDB, enter the Data Flow Management module.

2. Click 🟡 to create a new integration point.

3. Set the following adapter properties:

Field	Description
Adapter	Click 🔲 and select **CMKpiAdapter**.
Credentials ID	Do the following: a. Click 🔲. b. Select **Generic Protocol** and click **OK**. c. Click 🟢 to add the credentials to connect to Configuration Manager. Enter credentials for the user who has Views Administration and Login permissions. d. When finished, click **OK**
Hostname/IP	Provide the host name or IP address of the Configuration Manager server.
Integration Name	Enter a name for the new integration point.
Port	Enter the port number that is used for communication with the

Field	Description
	Configuration Manager application.
Use SSL	Select **False**. You cannot use secured communication to federate data from Configuration Manager.

4. Click **Test Connection** to make sure that you have configured the integration point correctly.

5. Click **OK** to save the integration point.

6. Select the KPI and KPIObjective CI types in the Supported and Selected CI Types tree.
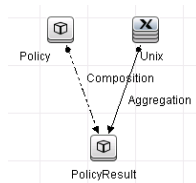
7. Click 💾 to save the integration point.

For further details about creating integration points, see the section about the Integration Studio in the *HP Universal CMDB Data Flow Management Guide*.

Create policy reports based on the CIs in a view or a custom TQL query

1. Create an integration point as described in "Create an integration point to federate policy compliance data" (on page 36), if one does not already exist.

2. In UCMDB, create a new view with a custom TQL query, or copy an existing view.
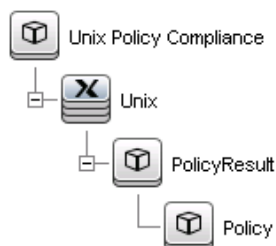
> **Note:** When using a custom TQL query, make sure you take into account the limitations of the data capacity when using federation. You should filter the CIs in the TQL query to take this limitation into account. For details, see "Troubleshooting and Limitations" (on page 43)

3. For each configuration item that you want to associate with a policy, attach the Policy CI type and the selected CI to the PolicyResult CI type, using composition and aggregation links accordingly. The cardinality should be 0..* if you also want to obtain results for CIs that do not have associated policy information. An example is shown below.
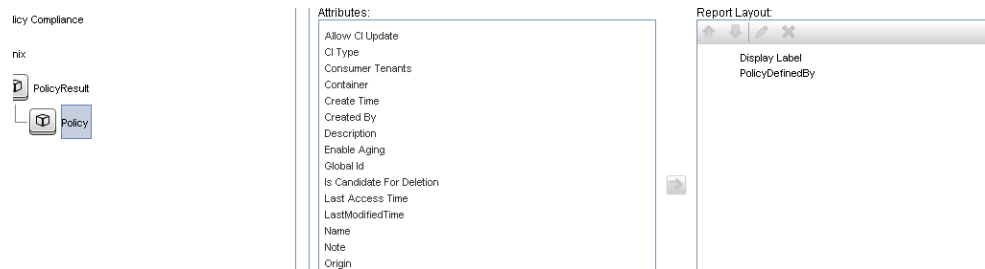

4. Specify the Configuration Manager integration point that you defined to be the data source that provides the policy and policy result data.

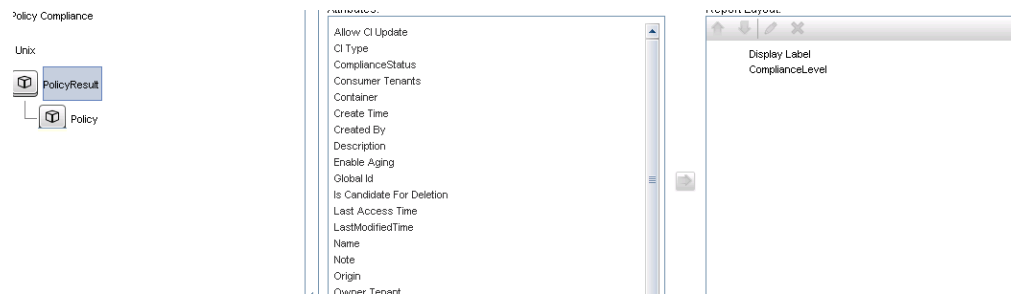5. Set the hierarchy. An example is shown below.

6. Add properties for the Policy CI type to the report layout: An example is shown below.

7. Add properties for the PolicyResult CI type to the report layout. An example is shown below.

8. If desired, you can schedule these reports to be created periodically. For details, see the *HP Universal CMDB Data Flow Management Guide*.
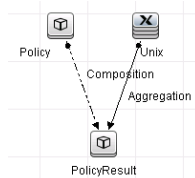
For details about creating reports, see the section about reports in the *HP Universal CMDB Modeling Guide*.

Create summary policy reports based on the CIs in a view or a custom TQL query

1. Create an integration point as described in "Create an integration point to federate policy compliance data" (on page 36), if one does not already exist.

2. In UCMDB, create a new view or copy an existing view.

   Note: When using a custom TQL query, make sure you take into account the limitations of the data capacity when using federation. You should filter the CIs in the TQL query to take this limitation into account. For details, see "Troubleshooting and Limitations" (on page 43).

3. For each configuration item that you want to associate with a policy, attach the Policy CI type and the selected CI to the PolicyResult CI type, using composition and aggregation links accordingly. The cardinality should be 0..* if you also want to obtain results for CIs that do not have associated policy information. An example is shown below.

4. Specify the Configuration Manager integration point that you defined to be the data source that

provides the policy and policy result data.

5. Set the hierarchy. An example is shown below.

6. Create an aggregation function for the Policy CI type. An example is shown below.

7. Add properties for the Policy CI type to the report layout. An example is shown below.

8. Add properties for the ConfigurationItem CI type to the report layout. An example is shown below.
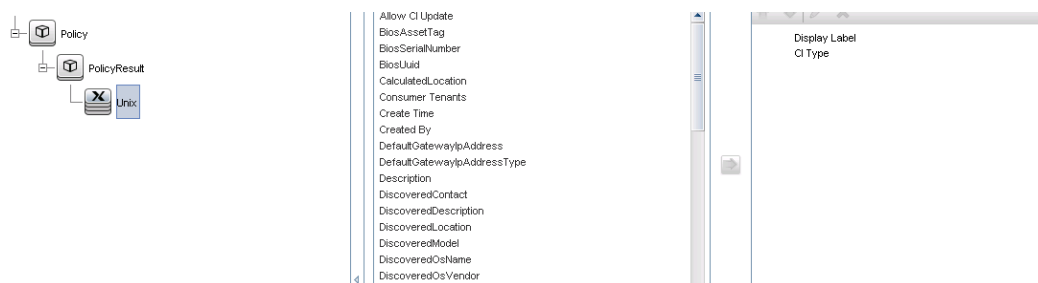
9. Change the report format to a bar chart. An example is shown below.

10. If desired, you can schedule these reports to be created periodically. For details, see *HP Universal CMDB Data Flow Management Guide*.

For details about creating reports, see the section about reports in the *HP Universal CMDB Modeling Guide*.

Create KPI reports

You can create KPI reports based on the CIs in a view, a custom TQL query, or business services.

1. Create an integration point as described in "Create an integration point to federate policy compliance data" (on page 36), if one does not already exist.

2. In UCMDB, create a new view based on a custom TQL or copy an existing view.

   Note: When using a custom TQL query, make sure you take into account the limitations of the data capacity when using federation. You should filter the CIs in the TQL query to take this limitation into account. For details, see Troubleshooting and Limitations.

3. For each configuration item that you want to associate with a policy, attach the selected CI to the Kpi CI type and the Kpi CI type to the KpiObjective CI type, using composition links. The cardinality should be 0..* if you also want to obtain results for CIs that do not have associated KPI information.

   Note: If you want to create a business services report, select the BusinessService CI type when creating the TQL query.
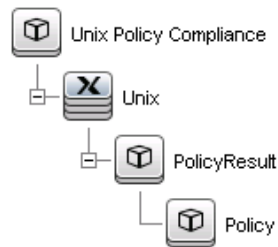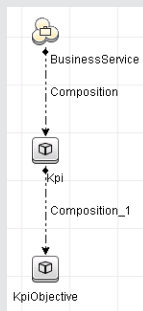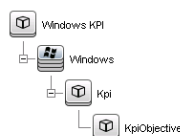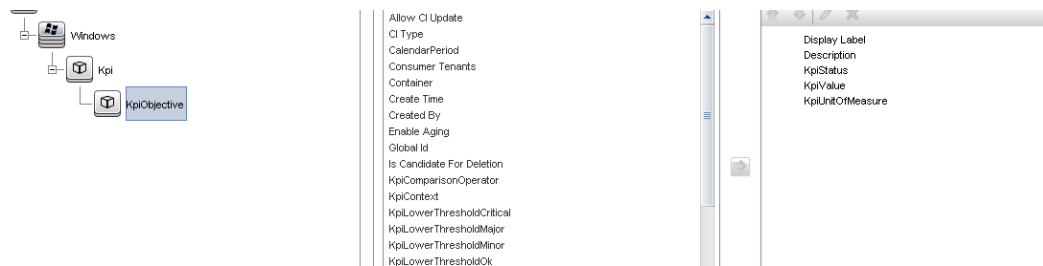

4. Specify the Configuration Manager integration point that you defined to be the data source that provides the policy and policy result data.

5. Set the hierarchy. An example is shown below.

6. Add properties for the KpiObjective CI type to the report layout: An example is shown below.


7. If desired, you can schedule these reports to be created periodically. For details, see the *HP Universal CMDB Data Flow Management Guide*.

For details about creating reports, see the section about reports in the *HP Universal CMDB Modeling Guide*.

Consume the KPIs in HP Business Service Management

1. Ensure that you have done the following:

   - The CM KPI integration point has been configured in UCMDB and is working properly.

   - BSM version 9.10 or later is installed, and DDM is activated and configured to work with BSM.

2. In BSM, navigate to **Administration > RTSM administration > Data Flow Management > Integration Studio**.

3. Edit the **CMS to RTSM** integration point. Set the required UCMDB settings (host, IP address, credentials, and probe settings).

4. Click **Test connection** and then click **Apply**.

5. In the Population tab, activate all the relevant integration jobs.

6. In the Federation tab, select **KPI** and **KPI Objective**, and click 🖫 to save the changes.

7. To verify that KPI data from Configuration Manager is retrieved by BSM, create and run a TQL query in RTSM. An example is shown below.
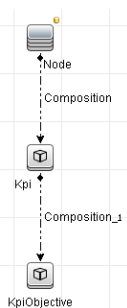
You must select a CI type that is synced and set the data source of the Kpi and KpiObjective CI types to **CMS to RTSM**.

Troubleshooting and Limitations

- Federation only works with CIs in the actual state. Therefore:

    - Policy compliance is federated only for CIs in the actual state.

    - The authorization status for CIs that were deleted from the actual state is not shown.

- SSL communication for KPI data federation is not supported.

- The maximum number of CIs that can be federated is configurable. For details about changing this number, edit the value of the Max Num To Federate setting in the Infrastructure Settings Manager in UCMDB. For details about changing settings, see the Infrastructure Settings Manager chapter in the *HP Universal CMDB Administration Guide*. The recommended number of CIs is no more than 20,000, if large views have been enabled in Configuration Manager. For details about enabling support for large views, see "Enable Large Views" in the *HP Universal CMDB Configuration Manager Deployment Guide*.

- If the test connection fails, click **Details** and check the first error in the stack trace for more information.

Administration

Chapter 5

View Management

This chapter includes:

View Management Overview

To begin working in Configuration Manager, you select views, which are defined in the UCMDB, to manage in your Configuration Manager environment. These are known as the managed views. Managing a view includes tracking its history, defining policies for it, and managing its different states by authorizing changes.

The View Management module controls the list of views being managed by Configuration Manager. All the views currently being managed appear in the list. You can add new views to the list and remove views that you no longer want to manage from the list. For details, see "View Refresh Rate" (on page 48).

For each managed view, you should define the managed CI types in the view. You can only authorize changes in managed CI types. The non-managed CI types appear faded in the view. A CI type can be managed in different views at one time; however, the same composite CI should not be managed in more than one view. If a CI in one managed view is also managed in a different view, a warning message indicates the other views in which the CI is managed.

Since managing large views and updating them can put a burden on the Configuration Manager and UCMDB systems, you can decide how often the information in a managed view should be updated. Specifying the view refresh rate helps to balance the workload. With a low view refresh rate, a view is updated once per day at a specified time. With a high view refresh rate (this is the default), the view is updated each time any change is detected in the managed CIs in the view, according to the Offline Analysis repeat interval.

> **Note:** You must have one of the following permissions to access the View Management module:
>
> - Views Administration permits you to add, remove, or modify all views in this module.
>
> - View Write permits you to see and modify your views.

In addition to selecting the views to manage, you can control how each view is managed by defining the following types of configuration behaviors:

- **Delete Candidates.** Enables you to remove CIs marked as candidates for deletion in UCMDB from the actual state of a view. For details, see "Delete Candidate Policy Pane" (on page 52).

- **Automatic State Transition.** Enables you to define the conditions under which a view can be automatically authorized. For details, see "Automatic State Transition" (on page 49).

These features can assist you by partially automating the management of the views.

After adding a view to the managed views list, the view appears on the View Summary page with other managed views, and you can access the view in State Management and the other modules.

For details on adding a view to the managed views list, see "Add a View to be Managed" (on page 50).

Topology Views and Inventory Views

There are two types of managed views: **topology views** and **inventory views**. Topology views are used for understanding the topology of a view and the relationships between the composite CIs. Inventory views are used for grouping similar composite CIs and are generally larger views including few relationships. You define the type of a view in the General pane of the View

Management module. An example of an inventory view could be a view containing all the Database CIs connected with a server.

The Configuration Explorer, State Management, and Historical Comparison modules have two options for displaying a view: topology mode and inventory mode. Every view is designated as either a topology view or an inventory view; however, both types of views can be displayed in either mode. Views with more than 250 composite CIs are automatically displayed in inventory mode even if they are defined as topology views. Configuration Manager supports inventory views with up to 5000 composite CIs.

View Refresh Rate

Configuration Manager can manage up to 500 views at the same time, and manage a maximum of 100 views that are frequently updated, according to the offline analysis repeat interval.

The view refresh rate is important when you manage many views. Since the offline analysis process takes some time to run, and therefore can put a burden on the Configuration Manager and UCMDB systems, you can tune the refresh rate and balance the load on the systems. The following table provides information about each of the options:

Once per day	- Notifications are not received from UCMDB regarding changes in the results of the TQL query for the managed view. - The offline analysis process runs whether or not there were changes in the view. - The calculation for a specific view may be delayed if there are multiple managed views that are updated once per day, since the calculations for multiple views are performed sequentially. - Exceptions to updating a view only once per day occur when you: - first manage the view (affecting view comparison, statistics, and snapshots). - initiate policy calculation, and the selected view is in the scope of the policy. - authorize a CI in a different view, and that CI is also managed in the selected view (affecting view comparison, statistics, and snapshots).
When view is updated	- The analysis is run according to the Offline Analysis repeat interval. - The view uses an active TQL query in UCMDB. - You receive notifications of changes from UCMDB regarding the change in TQL results from the view. - The offline analysis process will only run if there were changes in the view.

You may want to take the following issues into account when deciding on the view refresh rate:

What is the priority of the TQL query in UCMDB?	If it is low, then there may be no need to update the view in Configuration Manager more than once per day.

How often does the discovery run in UCMDB?	If the discovery process runs less often than once per day, then there is no benefit to updating the view more than once per day.
What often do you expect the view to change?	If not very often, then there is no reason to request frequent updates..
How important is it for you to get updated information?	If it is very important, then update the view more frequently than once per day.
How large is the view?	Updating large views that change frequently can put a load on Configuration Manager and UCMDB. Consider updating Configuration Manager only once per day, unless it is important to get more frequent updates for this view.

For additional details, see .

Automatic State Transition

Configuration Manager includes an automatic state transition feature that enables you to define the conditions under which changes in a view are automatically authorized. For a selected view, you define the types of changes approved, the CI types for which changes are approved, and whether or not to allow new policy breaches. You can choose to automatically authorize the changes in a view only when all changes meet the defined conditions, or to automatically authorize individual changes that meet the defined conditions (other changes will not be authorized). All CIs that breach one or more rules will not be authorized, and the CIs that are dependent on them will also not be authorized. The remainder of the CIs will be authorized.

Take the following examples of how authorization is applied: You select the CI types `computer` and `net device` as approved for changes, and you select `Added CI` as the only approved type of change, and you select not to allow any new policy breaches:

- When view level authorization is specified, the only change approved for authorization is the addition of a CI of type computer or net device. If any other type of CI is added to the view, or if any CI in the view is removed or modified, none of the changes are automatically authorized. Similarly, if new policy breaches are detected in any CI, the authorization does not proceed. If, for example one computer is added and another computer is removed, none of the changes are automatically authorized, even though the added computer CI meets the rules.

- When CI level authorization is specified, only the addition of `computer` or `net device` will be authorized. The rest of the changes will not be authorized.

  If no new policy breaches are allowed and the view contains a new topology policy breach - then none of the changes will be authorized, since there is no way to know which change caused this breach. If there are only new baseline policy breaches, then only the CIs that are in breach against their baseline policy will not be authorized.

You can define different authorization conditions for each individual view. Automatic state transition is executed for all changes that match the relevant authorization conditions in any of the views.

Add a View to be Managed

This task describes how to add a view to the managed view list.

1. In the View Management module, click the **Add views to managed views list** button 🔲 in the toolbar. The **Select view to manage** dialog box opens.

2. Select the required view and click **OK**. The view details are displayed in the Details area.

   > **Note:** If you do not see the required view in the list, try clicking **Refresh** to update the view list.

3. In the General pane, set the view type and managed CI types.

4. Optionally, select the check box in the Delete Candidate Policy pane. For details, see "Delete Candidate Policy Pane" (on page 52).

5. Optionally, set automatic state transition conditions for the view. For details, see "Set Automatic State Transition Rules for a View" (on page 50).

6. Click **Save** 🔲 in the toolbar. The view is added to the managed views list and can be accessed from the other modules.

Set Automatic State Transition Rules for a View

This task describes how to set automatic state transition rules for a view.

1. In the View Management module, select a view in the left pane and select the **Enable automatic state transition** check box in the Automatic State Transition pane. For details, see "Automatic State Transition" (on page 49).

2. Select either **View level** or **CI level** authorization.

3. In the criteria table, configure the following options:

   - Click **CI Types** to open a CI type tree. Select the required CI types approved for authorization of changes.

   - Click **Configuration Policies** and select the required option (**Allow new policy breaches in the view** or **Do not allow new policy breaches in the view**).

   - Click **Detected Change Type** and select the types of changes approved for authorization.

4. Click **Test Configuration** to determine if the view contains CIs with changes that match the conditions set for authorization.

   - If all changes satisfy all automatic state transition rules, the status of the test is **Passed**.

   - If some or all of the changes do not satisfy the automatic state transition rules, the status of the test is **Unsatisfied**.

5. Click **OK** to return to the View Management window, where you can either click **Save** 🔲 to save the conditions, or edit the authorization rules and test them again.

The automatic state transition rules are now set. When you run automatic state transition, the changes in the view matching the conditions you set are authorized. For details, see "Authorize Changes to CIs" (on page 109).

> **Note:** Automatic state transition is executed on all views for which automatic state transition is enabled.

Specify the View Refresh Rate

1. Navigate to **Administration > View Management**.

2. Select a view.

> **Note:** You can also specify the view refresh rate when you create a new view.

3. In the General pane, select the view refresh rate. You can choose to have the view updated once per day, or each time any change occurs to the managed CIs in the view.

   For views that will be refreshed once per day, you can specify the hour at which this update will begin: The default time is 12:00 AM (midnight).

> **Note:** This is the time at which the calculations begin. For views that are refreshed more than once per day, calculations are done in sequence..

   a. Navigate to **System Settings > Application Management > Offline Analysis and Authorization > Daily View Refresh Settings**.

   b. From the drop-down list, select the time at which the update will be run.

4. Click 💾.

View Management User Interface

This section includes:

## View Management Page

This page displays the list of views currently being managed.

To access	Select **Administration > View Management**.
Important information	The left pane displays the list of managed views. The General pane, Delete Candidate Policy pane, and the Automatic State Transition pane display details for the managed view selected in the left pane.
	After adding a view to the managed views list, the view data may be unavailable for a few minutes, until the system is updated.
Relevant tasks	• "Add a View to be Managed" (on page 50)
	• "Set Automatic State Transition Rules for a View" (on page 50)

User interface elements are described below:

UI Elements (A-Z)	Description
<Filter views>	Enter a string to filter the list of displayed views.
⭐	Click to toggle between displaying all views and displaying the favorite views only.
➕	Click to select a view to add to the list of managed views. The **Select view to manage** dialog box opens.
✖	Click to remove the selected view from the list of managed views.
💾	Click to save changes.
↩	Click to undo changes made to the view.
🔄	Click to trigger automatic state transition for all views.
🔄	Click to refresh the view list.
View Name	The names of the managed views.

General Pane

UI Elements (A-Z)	Description
Description	The description of the selected managed view from UCMDB.
Managed CI Types	Select the CI types to be managed in this view. Only the selected CI types are managed in this view. If some of the child CI types of a CI type are selected and others are not, the parent CI type is not managed in the view. **Note:** All CI types are selected by default.
View Name	The name of the selected managed view.
View Refresh Rate	Select either **Once per day** or **When view is updated**.
View Type	Select the view type. The available options are **Topology** and **Inventory**. For details, see "Topology Views and Inventory Views" (on page 47).

Delete Candidate Policy Pane

UI Elements (A-Z)	Description
Delete CIs marked as candidates for deletion from Actual State (override	When the check box is selected, CIs marked as candidates for deletion in UCMDB are deleted from the actual state of the view immediately. When the check box is cleared, the CIs are only deleted at the deletion time scheduled in UCMDB.

UI Elements (A-Z)	Description
UCMDB aging mechanism)	

Automatic State Transition Pane

Relevant tasks	["Set Automatic State Transition Rules for a View" (on page 50)](#)

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

UI Elements (A-Z)	Description

<Criteria List>	The following criteria are used to set the automatic state transition rules:
	
	● **CI Types.** Define the CI types for which you approve changes for authorization. When this option is highlighted, a CI type tree appears below. Select the required CI types from the tree.
	
	● **Configuration Policies.** Define whether new policy breaches in the view are approved for authorization.
	
	If you select the **Allow new configuration policy breaches in the view** check box, all breaches in Configuration Manager policies are ignored.
	
	If you do not select the check box, then any new policy breach stops the automation:
	
	  ▪ If there is a CI with a new baseline policy breach, only the change on that CI is not authorized.
	
	  ▪ If there is a CI with a new topology policy breach, no changes on CIs in the view are authorized.
	
	● **Detected Change Type.** Define which types of changes you approve for authorization. Select from the following options:
	
	  ▪ Added CI
	
	  ▪ Modified CI
	
	  ▪ Removed CI
	
	● **Related RFCs.** Specify whether or not changed CIs are required to have RFCs for automatic state transition of the view to occur. If you select only **Do not allow changes with no related RFCs**, only RFCs that are directly related to CIs will be validated. To validate RFCs that are indirectly related to the CIs, select **Allow indirect RFCs on CI**.
	
	Select the **Log changes on selected RFCs in Change Management system** check box to mark the RFCs in the change management system with the relevant change.

Enable automatic	Select this check box to activate the fields in the Automatic State

UI Elements (A-Z)	Description
state transition	Transition pane. The following options are available: • **View level** authorization (default). This option automatically authorizes all changes in the selected view, if all rules for all CIs in the view are satisfied. This means that all the changes in the view will be automatically authorized if all the rules are satisfied, while if a single change does not meet the defined rules, none of the changes in the view will be authorized. • **CI level** authorization. This option enables you to select the specific CI types and change types for which you want automatic state transition to be performed. In this case, not all CIs in the view must be satisfied for all rules.
Test Configuration	After selecting automatic state transition settings, click **Test Configuration** to check if the view contains changes matching the conditions set for authorization.

Troubleshooting and Limitations

The following limitation is applicable when working with managed views in Configuration Manager:

The following types of views cannot be selected to be added to the managed views list:

- views containing calculated links

- views containing federated data

- views containing compound links (compound links are allowed if they are set to return the full path)

If you try to select one of the above types of views to manage, an error message appears.

Chapter 6

Automation Management

This chapter includes:

Automation Management Overview

Configuration Manager provides the ability to use predefined flows from HP Operations Orchestration to automate standard system operations.

Automations contain the following information:

- General details, such as the name and description.

- The CI type on which the automation will run.

- Whether the automation is controlled or not controlled.

- Parameters that assist in calculating the automation's risk.

- Parameter mappings that can be specified during automation setup:

  - a selection list populated from the OO flow

  - a default value populated from the OO flow

    > **Note:** When you import flows from HP Operations Orchestration version 9.0, default values do not appear in Configuration Manager. You must enter these values manually, either during setup or during execution.

  - free text

  - values from the CI that is selected during execution

    The following CI types can be mapped:

    - **Node**: Domain name, Host name, IP address

    - **Running Software**: Domain Name, Host Name, IP Address, Installation Path, Software Name

Set Up an Automation

This task describes how to create an automation from an HP Operations Orchestration flow and how to configure it.

	The Automation Setup movie (to see a demonstration of how to set up and configure an automation) can be accessed by clicking the .htm file in the following location: **<Configuration Manager installation directory>\servers\server-0\webapps\docs\en_US\movies\Automations_Setup\.**

This task includes the following steps:

- "Configure HP Operations Orchestration connection settings" (on page 56)

- "Import a flow from HP Operations Orchestration" (on page 57)

- "Specify automation properties" (on page 57)

1. **Configure HP Operations Orchestration connection settings**

   a. Navigate to **System > Settings > Integrations > Operations Orchestration (OO) > OO**

Server Location.

b. Enter the following details:

UI Elements (A-Z)	Description
Cyclic Interval	Defines the interval (measured in minutes) which determines how often the HP Operations Orchestration server is checked for automation flow results. **Default:** 60 seconds
Host	The host name of the machine on which the HP Operations Orchestration server is installed.
Password	The password required to connect to the HP Operations Orchestration server.
Port	The port used by the HP Operations Orchestration server.
User Name	The user name required to connect to the HP Operations Orchestration server.
Version	The HP Operations Orchestration version.

2. **Import a flow from HP Operations Orchestration**

   When you import a flow from HP Operations Orchestration, you create an automation in Configuration Manager.

   a. Select **Administration > Automation Management.**

   b. Click ![plus icon] to open the **Select Flow** window.

   c. In the left pane, click to expand the Flow Tree and select the HP Operations Orchestration flow that you want to run as an automation in Configuration Manager.

   d. Click **OK** to return to the Automation Management window.

3. **Specify automation properties**

   a. In the left pane of the Automations window, select the automation that you want to configure**.**

   b. Fill in the required details for the automation.

      ○ The name of the automation is automatically taken from the OO flow, but can be changed.

      ○ You must specify the CI type to be automated.

   c. Click **Save** ![save icon].

Automation Management User Interface

This section includes:

Automation Management Page

This page displays the list of automations currently being managed. On this page, you can import flows from HP Operations Orchestration and change their configurations.

To access	Select **Administration > Automation Management**.
Important information	The left pane displays the list of automations. The right pane display details for the automation selected in the left pane.
Relevant tasks	"Run a Controlled or Non-Controlled Automation" (on page 134)

Left Pane

UI Elements (A-Z)	Description
	Click to refresh the list of automations.
	Click to save changes made to the selected automation.
	Click to save changes made to all edited automations.
	Click to add a flow to the automations list.
	Click to remove the selected automation from the list of automations.

<Automation> Pane - Automation Details Area

User interface elements are described below:

UI Elements (A-Z)	Description
Associated CI Type	Enables you to select the specific CI type to which this automation will be assigned. Click to open the CI Selector window. During execution, you will see only the automations that were assigned to the selected CI type. For example, if you select Windows CI type, when you run the execution you will see automations that relate to Windows CI type and other branches that are above it in the hierarchy.
Description	A description of the automation. By default, the description from the imported flow is used as the automation's description, but this may be changed.
Flow Path	Displays the original full path and name of the imported flow in the HP Operations Orchestration tree (for information purposes only).
Flow UUID	Displays the unique identifier of the imported flow (for information purposes only).
Name	The name of the automation. By default, the name of the imported flow is used as the automation's name, but this may be changed.

<Automation> Pane - Execution Details Area

User interface elements are described below:

UI Elements (A-Z)	Description
Causes Configuration Change	Specifies whether the automation causes a change to the CI in UCMDB. Select **Yes** or **No**. Relevant when defining policies and during automation analysis.
Causes Downtime	Specifies whether or not the automation causes the CI to become unavailable during the execution. Select **Yes** or **No**. Relevant when defining policies and during automation analysis.
Controlled Execution	Select this check box to indicate that the selected flow will be run as a controlled automation.
	Clear this check box to indicate that the selected flow will be run as a non-controlled automation.
	• In a controlled automation, you review the policies and analysis before running the automation.
	• In a non-controlled automation, the automation runs without any additional information.
	For details on running an automation, see "Run a Controlled or Non-Controlled Automation" (on page 134).
Estimated level of risk	A subjective evaluation of the level of risk in the automation. Valid values are:
	• Unknown
	• None
	• Low
	• Medium
	• High
	Relevant when defining policies and during automation analysis.

<Automation> Pane - Execution Parameters Area

User interface elements are described below:

UI Elements (A-Z)	Description
<Flow execution parameters>	Specify the parameters that you want to use when the automation is executed. The parameters displayed in this list vary according to the selected flow.
	Note: A gray asterisk indicates a required field in the HP Operations Orchestration flow. If you do not fill in the required value, you cannot run the automation in Configuration Explorer. For information on how to run an automation, see "Run a Controlled or Non-Controlled Automation"

UI Elements (A-Z)	Description
	(on page 134).

Chapter 7

Configuration Policy Management

This chapter includes:

Configuration Policies Overview

A configuration policy enables you to define the expected configuration of a view. By applying policies to your managed views, you set standards for the views. The policies help to ensure that the views adhere to the standards and make your IT environment more predictable.

The Configuration Policies module controls the policy groups and policies you define for the managed views. There are two types of configuration policies you can define:

- **Baseline policies**

  In a **baseline policy**, you define a baseline for a composite CI with selected attributes to be compared to the CIs of the relevant views. For instance, you could define a baseline policy stating that every production server in the view must contain at least two CPUs. All server CIs in the view are compared to the baseline CI. If any one does not satisfy the policy, the view is said to be in breach of the policy.

  Note: If you identify an existing CI in your environment with the desired configuration, you can select that CI to serve as the baseline.

- **Topology policies**

  In a **topology policy**, you define a condition TQL query that determines the configuration of the view. For instance, the condition TQL could stipulate that every cluster of a production J2EE include at least two servers. If the view satisfies this condition, it satisfies the topology policy. If it does not, it is said to be in breach of the policy.

  In some cases, it is easier to define a TQL query representing a problematic topology rather than the desired configuration. In that event, there is an option to set the condition of the topology policy as negative, which inverts the satisfaction of the policy (in the above example, only clusters with less than two servers would satisfy the condition).

In both types of policies, you can also define the following settings:

- **Validation.** Set the time period for which the policy is valid

- **Advanced Filter.** Select a TQL query that limits the policy to a subset of CIs in the view. For example, if the baseline CI is of type Oracle, the filter could limit it to Oracle version 9.

Both types of policies can be applied to all of the managed views in Configuration Manager.

For details on defining policies, see "Configuration Policies Page" (on page 65).

Note:

- You must have Configuration Policies Administration permission to work with this module.

- You must also have one of the following permissions:

  - View Write permits you to assign or remove views.

  - View Read permits you to preview a policy or create a baseline policy from a managed CI (included in View Write).

Baselining

A configuration baseline is the configuration of a service, product, or infrastructure that has been formally reviewed and accepted as the basis for further activities. It captures the structure, contents, and details of a configuration and represents a set of configuration items that are related to each other.

Establishing a baseline provides the ability to:

- Mark a milestone in the development of a service

- Build a service component from a defined set of inputs

- Change or rebuild a specific version at a later date

- Assemble all relevant components in preparation for a change or release

- Provide the basis for a configuration audit and back out (for example after a change)

Policy Groups

You can define policy groups to group policies together logically. A policy group can contain both baseline and topology policies. Assigning a policy group, rather than individual policies, to a view, can make it easier to manage the policies. You can also define subgroups within the policy groups.

You can copy a policy from one group and paste it into another group or the root of the tree. This can provide a shorter way of adding policies to your policy groups. If you want to define a similar policy to an existing one, you can copy it to the required location and modify it. Changes made to the copied policy do not affect the original policy. You can also cut a policy from a group and paste it into another group. In this case, the policy is deleted from the original group.

You can also cut or copy a policy group and paste it into the root of the policy tree or into another group. It is only possible to cut or copy a single policy or group at one time.

When cutting or copying policies and groups and pasting them elsewhere, the policies still apply to the views to which they were assigned. However, when a policy group is applied to a view and one of the group's policies is copied to a different group, the copied policy does not apply to the views of its previous group; rather, it now applies to the views of the new group.

For details on defining policy groups, see "Configuration Policies Page" (on page 65).

Define a Configuration Policy

This task describes how to define a new policy and apply it to managed views.

1. Click the **Add Policy** button in the Configuration Policies toolbar and select Add Baseline Policy or Add Topology Policy.

2. Enter the policy name and description in the General area of the Details pane.

3. In the Views area of the Details pane, select the views to which the new policy applies.

4. In the Validity area of the Details pane, select the period of policy validation.

5. In the Filter area of the Details pane, select the CI type of the CIs to be tested against the policy. Optionally, select a TQL to serve as an advanced filter of the CIs to be tested against the policy.

6. For topology policies, set the condition type and condition TQL in the Condition area of the Details pane.

   For baseline policies, define a baseline CI and its attributes in the Baseline area of the Details pane.

7. When you are finished, click the **Save** button ![save icon] in the Configuration Policies toolbar to save your policy.

Configuration Policies User Interface

This section includes (in alphabetical order):

Attribute Operators

This following table contains a list of operators used to define attribute conditions.

Operator	Description
Contain	Checks whether the attribute values contain the specified list of values.
Contain ignore case	Checks whether the attribute values contain the specified list of values regardless of the case.
Equal	Checks whether the attribute value is equal to the specified value.
Equal ignore case	Checks whether the attribute value is equal to the specified value regardless of the case.
Greater than	Checks whether the attribute value is greater than the specified value.
Greater than or equal	Checks whether the attribute value is greater than or equal to the specified value.
In	Checks whether the attribute value is in a list of defined values. Click the **Edit Values** button ![edit icon] to edit the list of values.
In ignore case	Checks whether the attribute value is in a list of defined values regardless of the case. Click the **Edit Values** button ![edit icon] to edit the list of values.
Less than	Checks whether the attribute value is less than the specified value.
Less than or equal	Checks whether the attribute value is less than or equal to the specified value.
Like	Uses a wildcard (%). Use **Like** to search for a fragment of a name. You can insert the wildcard character at any point in the name.

Operator	Description
Like ignore case	Uses a wildcard (%). Use **Like ignore case** to search for a fragment of a name. The case of the string is ignored.
Not equal	Checks whether the attribute value is not equal to the specified value.
Not null	Checks whether the attribute value is not null.

Configuration Policies Page

This page enables you to define and edit configuration policies.

To access	Select **Administration > Policies > Configuration Policies**.
Important information	The left pane contains an expandable list of the policies. The details pane displays details for the policy selected in the left pane.

User interface elements are described below:

UI Elements (A-Z)	Description
	Click **Add Policy Group** to define a new policy group.
	Click **Add Policy** to define a new policy. Select one of the following options: • Add Baseline Policy • Add Topology Policy
	Click **Delete** to delete the selected policy.
	Click **Cut** to remove the selected policy or group from its current location and save it to the clipboard.
	Click **Copy** to copy the selected policy or group to the clipboard.
	Click **Paste** to add the copied policy or group to the selected location.
	Click **Undo** to undo the last action.
	Click **Save** to save the changes made to the current policy.
	Click **Preview** to open the Policy Preview dialog box which provides a preview of the satisfaction level of the selected policy over the managed views. **Note**: Only views for which the user has View Read permission are sent to the server and are displayed in the preview results. If a user does not have View Read permission for a particular view and attempts to preview it, an error message is displayed.

UI Elements (A-Z)	Description
	Click **Recalculate Policy Analysis** to recalculate the policy analysis for the selected policy.
	Click **Export Report** to choose the export format for the Configuration Policies Report 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. • **CSV.** The table data is formatted as a comma-separated values (CSV) text file that can be displayed in a spreadsheet.
	Click **Refresh** to refresh the policy list.

Left Pane

Important information	Click the arrow next to **Policies** (the root of the policies tree) to expand the tree. Click the arrow next to a policy group to expand the list of policies in the group.

Details Pane

Important information	When you select a policy group in the left pane, the group details appear in the Details pane. When you select a policy in the left pane, the policy details appear in the Details pane.

Details: <Policy> Section

User interface elements are described below:

UI Elements (A-Z)	Description
Filter	This section is used to filter the CIs that are tested against the policy. This section includes: • The main CI type to be filtered for testing against the policy. Click the button to open the **Select CI Type** dialog box, which enables you to select the required CI type. • Properties selector for the main CI type. Click the button to open the **Specify baseline for filter** dialog box. For details about selecting properties, see "Baseline CI Section" (on page 67) • An additional CI type that is related to the main CI type. Click the button to open the **Select CI Type** dialog box, which enables you to select an additional CI type. • An additional TQL query that further refines the selection. Click the button to open the **Select TQL** dialog box, which enables you to

UI Elements (A-Z)	Description
	select the required filter TQL query.
General	This section includes: • **Description.** Enter the policy description. • **Policy Name.** Enter the policy name.
Validity	Specify the scope of the policy's validity. Click the calendar buttons to select the dates and times for the beginning and end of the period.
Views	The **Assign policies to views** field lists the views to which this policy applies. Click the button to open the Select Views dialog box, which enables you to select the views to which the policy applies.

Baseline CI Section

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

UI Elements (A-Z)	Description
	Select one of the following options: • **Create baseline from a managed CI.** Select an existing CI from the view to serve as a baseline CI. • **Create baseline from existing configuration model.** Select a model from the Configuration Analysis module to serve as a baseline CI.
	Click **Add CI class type to baseline** to select a CI type to add to the baseline definition. (When no baseline is defined, this is called **Create Baseline**.) You can add multiple CIs of the same type using the CI count feature.
	Click **Remove Selected Item from Baseline** to delete the selected CIs from the baseline definition.
<Check box column>	Select the check boxes next to the attributes you to include in the baseline definition. You can select all of the attributes by selecting the check box in the column header.
<Comparable column>	If the comparable column is blank for a selected attribute, the attribute is not relevant for comparison. If a icon appears in the column for a selected attribute, the attribute is relevant for comparison. If a icon appears in the column for a selected attribute, the attribute is relevant for comparison and is assigned a rank in the system's matching algorithm.

UI Elements (A-Z)	Description
Attribute Name column	The names of the attributes for the selected CI.
Attribute Value column	The values of the attributes for the selected CI. • If the attribute is of the type **Enum**, select a value from the drop-down list or use free text for a new value. • If the attribute is of the type **string_list**, you can add multiple values by clicking the 🖉 button and using the Attribute Name dialog box.
CI Type	Select a CI type from the baseline. The attributes for this CI type are displayed in the table. **Note:** It is possible to select more than one CIT of the same type in the baseline. This is known as **Common Definition mode**. In this mode, any changes you make to one of the selected CITs apply to all of them.
Consider additional internal CIs as breach	When you select **Consider additional internal CIs as breach**, the CI being compared to this baseline is considered in breach of the policy if it has additional internal CIs.
Operator column	Select an operator defining the relationship between the attribute and its value. For details, see "Attribute Operators" (on page 64).

Policy Preview Dialog Box

This page enables you to preview the satisfaction level of a policy over the managed views.

To access	Click **Preview** 🔍 in the Configuration Policies toolbar.

User interface elements are described below:

UI Elements (A-Z)	Description
▷	Click **Continue Calculation** to continue the calculation of the policy satisfaction level after it was paused.
▮▮	Click **Pause Calculation** to pause the calculation of the policy satisfaction level.
🗐	Click **Show Policy Details** to display details for the CIs of the selected view.
CI Name	The names of the CIs in the selected view.
Policy Satisfaction	The policy satisfaction level for the view (by percentage).
Policy Status	The policy status for each CI in the selected view.
State	Select the state of the view.

UI Elements (A-Z)	Description
View Name	The name of the view.

Select Composite CI Dialog Box

This dialog box enables you select a specific CI for a baseline definition.

To access	Click **Select predefined configuration** and select **Create baseline from a managed CI** from the Baseline CI section in the Details Pane.
Important information	When you select a specific CI for a baseline definition, the CI types previously included in that definition are removed.

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

UI Elements (A-Z)	Description
<List of CIs>	A list of the CI names and types in the selected view. Select one to serve as the model CI.
Filter	Enter a string to filter the CIs in the list.
State	Select **Actual** or **Authorized**.
View	Select a view from the drop-down list.

Troubleshooting and Limitations

The following limitation is applicable when working with configuration policies:

Condition TQL queries must not include attribute conditions on unmanaged attributes.

Chapter 8

Automation Policy Management

This chapter includes:

Automation Policy Management Overview

Automation policies are business rules that determine when there is a high risk in running an automation. The automation policy assessment provides you with an awareness of those risks.

All automation policies are managed from the Automation Policy Management module. They enable you to define restrictions based on the automation execution information and assessment.

Configuration Manager pre-evaluates the organization's policies and determines whether the automation complies with the business rules.

A condition can be based on CI analysis information, such as severity and importance impact, or flow statistics, such as success ratio or collision conditions. It states what the acceptable threshold is for that condition. Each policy evaluation can result in being breached or satisfied.

For example, you can define a rule which states that a policy is breached when the **My_CI** application has an impact severity level of **Critical** or **High**. If the automation fulfills all the conditions, the policy is considered to be in breach.

For information on how to run an automation, see "Automation Execution Dialog Box" (on page 139).

For details on defining automation policies, see "Automation Policies Page" (on page 73).

> **Note:** Users with Automation Policies Administration permission are able to see and modify all policies.

Define an Automation Policy

This task describes how to define a new automation policy.

1. Click **Add New Policy** ⊞ in the **Administration > Policies > Automation Policies** toolbar.

2. In the **General** area, enter the following:

   - The policy name

   - The policy description

   - The frequency of policy validation

3. In the **Scope** area, select the views to which the new automation policy applies. You can either select a specific view or apply the policy to all views.

4. (Optional) Select the CI type of the CIs to be tested against the policy.

5. In the **Restrictions** area, define the required automation/CI conditions.

6. Click **Save** in the Automation Policies toolbar to save your policy.

Configuration Manager Automation Policy - Use Case

This section describes a use-case for defining an automation policy in Configuration Manager.

This scenario includes the following steps:

1. **Background**

   The owner of the **HP Portal** application needs to continually monitor the high-availability of his application. As a result, it is important to guarantee that when changes occur, the application will continue to function in accordance with its agreed to requirements.

   Toward this end, the application owner wants to define an automation policy that gives an indication in the event that:

   - An automation which implements a change causes application downtime

   - The CI is directly affected by more than one automation.

2. **Prerequisite - Import the Managed View from HP Universal CMDB**

   The application topology is modeled in a view in HP Universal CMDB. Once you import the required view, there is a corresponding managed view in Configuration Manager. The following image displays the **HP Portal** application topology in Configuration Manager:
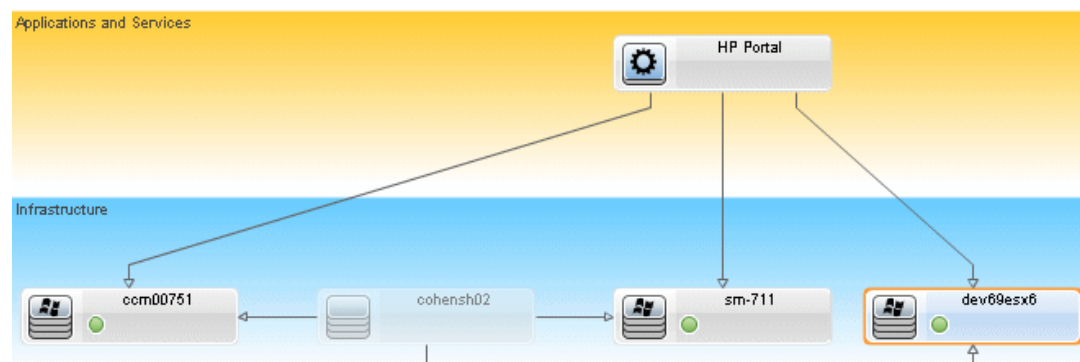
   For details on how to import a managed view, see "Add a View to be Managed" (on page 50).

3. **Define the Automation Policy in Configuration Manager**

   a. Go to **Administration > Policies > Automation Policies** to create a new automation policy.

   b. In the **General** area, do the following:

      ○ In the **Name** box enter: `Causes downtime and a CI collision on the HP Portal application.`

- ○ (Optional) In the **Description** box, enter the required description.

- ○ Use the **Perform Validation** check boxes to define the frequency of policy validation.

c. In the **Scope** area do the following:

- ○ Select **Selected Views** and click the 🗒 button to select the managed view to which to apply the policy.

- ○ In the **Assign CI Type** box, click the 🗒 button to select **BussinessApplication** as the CI type to be tested against the policy.

d. In the **Restrictions** area, do the following:

- ○ Under **Automation Restrictions**, select **Causes Downtime**.

- ○ Under **CI Restrictions**, select **Direct Collision**.

e. Save the new automation policy.

4. **View Policy Evaluation Results**

You can view the policy evaluation results within the context of running a controlled automation. For details, see "Run a Controlled or Non-Controlled Automation" (on page 134).

Automation Policies User Interface

This section includes:

Automation Policies Page

Configuration Manager provides out-of-the-box automation policies. To see a description of each policy, select the required policy in the Policies pane. The description of the policy appears in the **Description** box in the General pane.

This page enables you to define and edit automation policies.

To access	Select **Administration > Policies > Automation Policies**.
Important information	You must have Automation Policies Administration permission to work with this module.
Relevant tasks	• "Run a Controlled or Non-Controlled Automation" (on page 134) • "Define an Automation Policy" (on page 71) • "Configuration Manager Automation Policy - Use Case" (on page 72)
See also	"Automation Execution Dialog Box" (on page 139)

User interface elements are described below:

UI Element (A-Z)	Description
🗒	**Add New Policy.** Create a new policy.

UI Element (A-Z)	Description
🗑	**Delete Policy.** Delete the selected policy.
📋	**Save All.** Save all the changes made to the current policy.
🔄	Click **Refresh** to update the information on the Policy Management page.

Policies Pane

User interface elements are described below:

UI Element (A-Z)	Description
<List of policies>	Displays the list of out-of-the-box and user-defined automation policies.

General Pane

User interface elements are described below:

UI Element (A-Z)	Description
Description	Enter the policy description.
Perform validation	Select the scope of the policy's validity. The available options are: • **Valid From.** If only this check box is selected, the policy's validity begins from the date selected in the calendar and is always valid. Click the calendar buttons 📅 to select the date and time for the beginning of the period. • **Valid Until.** Select a fixed period for which the policy is valid. To select a fixed period, you must select the check boxes of both **Valid From** and **Valid Until**. Click the calendar buttons 📅 to select the date and time for the end of the period. **Note:** If neither of the check boxes are selected, the policy validation is never calculated.
Policy Name	Enter a unique policy name.

Scope Pane

User interface elements are described below:

UI Element (A-Z)	Description
Assign CI Type	The CI type of the CIs to be tested against the policy. Click the 📋 button to open the select CI Type dialog box, which enables you to select the required CI type.

UI Element (A-Z)	Description
	At least one CI of the CI type selected must appear in the impact topology map for policy validation to be calculated.
	For example, if there is a collision on a **Unix** type CI in your view, but in the **Assign CI Type** box, you selected **Windows**, the policy is not evaluated for the **Unix** type CI.
	If there is no CI of the type **Windows** in your topology map, the policy is not evaluated.
	Note: If no CI type is specified, then the policy applies to all CIs.
Assign policy to views	Enables you to select the views to which the policy applies.
	• **All Views.** Apply the policy to all managed views.
	Note: You need Automation Policies All Views permission to apply a policy to all views, including the views you are not managing. If you do not have Automation Policies All Views permission, you can only apply the policy to the view you are managing.
	• **Selected Views.** Select a view to which to apply the policy. Click the ▤ button to open the Select Views dialog box.
	Note: If you do not select either **All Views** or select a view from the **Selected Views** option, the policy validity is not calculated.

Restrictions Pane

User interface elements are described below:

UI Element (A-Z)	Description
Automation Restriction Conditions	Describes the automation restriction conditions for this policy.
	For example, you can define a policy which stipulates that running your automation for the first time causes a policy breach.
	Note: The AND operator connects all the conditions defined. Therefore, the policy is breached only if the automation complies with all of the conditions defined for this policy.
	For a list of the operators used to define attribute conditions, see "Attribute Operators" (on page 64).
	For a description of the conditions you can define, see "Automation Execution Dialog Box" (on page 139).
CI Restriction Conditions	Describes the CI restriction conditions for this policy.
	The AND operator connects all the conditions defined. Therefore, the policy is breached only if the automation complies with all of the conditions defined for this policy.

UI Element (A-Z)	Description
	There must be at least one CI in your impact map that complies with all the conditions defined for the policy to be breached. ● The breached CI must comply with all conditions in the CI Restriction pane. ● The CI must be in the view selected in the Scope pane. ● The CI must be of the CI type, or sub-type of it, selected in the Assigned CI Type box. For a list of the operators used to define attribute conditions, see "Attribute Operators" (on page 64). The CI Restriction conditions are: ● **Collision exists.** Checks whether a collision (direct or indirect) exists. ● **Direct Collision exists.** Checks whether a direct collision exists. ● **Impact importance.** Checks the impact importance level. ● **Impact severity.** Checks the impact severity level. ● **Indirect collision exists.** Checks whether an indirect collision exists. For more information about collision, see the "Automation Execution Dialog Box" (on page 139) For more information on impact importance and impact severity, see the "Automation Analysis > Impact - <State> Pane" (on page 142).

Application

Chapter 10

Home Page

This chapter includes:

Home Page Overview

The Home Page provides a dashboard view of the key metrics being monitored by http://www.cruisecritic.com/ports/newport.cfm?ID=87. The page includes graphical displays of data over time, including the number of managed CIs by authorization status, the number of CIs by policy status, the number of authorized changes, and the number of non-compliant CIs.

Note: You can view only CIs in views for which you have View Read permission.

Home Page User Interface

This section includes (in alphabetical order):

Home Page

This page provides an overview of data relating to your managed views.

Note: In all panes, only CIs in the views for which the user has View Read permission are displayed.

To access	Select **Application > Home**
Important information	The **Managed CIs** pane displays the number of authorized and unauthorized CIs over the selected period.
	The **Policy Summary** pane displays the number of satisfied and breaching CIs in each state for each of the policies under administration.
	The **Authorized Changes** pane displays the number of authorized changes over the selected period.
	The **Non-Compliant CIs** pane displays the total number of CIs satisfying or in breach of baseline policies.
	Note: You can rearrange the layout of the Home Page panes by dragging them to the desired position.

Left Pane

User interface elements are described below:

UI Elements (A-Z)	Description
⭐	Click **Show favorite views only** to toggle between displaying data for all views and displaying data for favorite views only.
🔄	Click to refresh the displayed data.
New Policy Breaches	Displays a list of the managed views with the number of policy breaches on the total number of CIs for each view.

UI Elements (A-Z)	Description
Pending Authorizations	Displays a list of the managed views with the number of unauthorized CIs out of the total CIs for each view.

Authorized Changes Pane

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

UI Elements (A-Z)	Description
Week ▼	Select the time period for the data displayed in the graph. The options are: - Week - Month - Three Months - Year
▤	Click to display a legend of the graph.
▦	Click to change the display to table format.
▥	Click to change the display to graph format.
My Views ▼	Select the view(s) reflected in the graph.
<Graph>	The graph displays the number of changes authorized over the selected time period.

Managed CIs Pane

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

UI Elements (A-Z)	Description
Week ▼	Select the time period for the data displayed in the graph. The options are: - Week - Month - Three Months - Year
▤	Click to display the graph's legend.
▦	Click to change the display to table format.

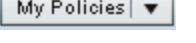| UI Elements (A-Z)	Description
📊	Click to change the display to graph format.
<Graph>	The graph displays the number of authorized and unauthorized CIs over the selected time period. The green area represents the authorized CIs and the blue area represents the unauthorized CIs.

Non-Compliant CIs Pane

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

UI Elements (A-Z)	Description
Week ▼	Select the time period for the data displayed in the graph. The options are: • Week • Month • Three Months • Year
☰	Click to display a legend of the graph.
▦	Click to change the display to table format.
📊	Click to change the display to graph format.
My Views ▼	Select the view(s) reflected in the graph.
My Policies ▼	Select the policies reflected in the graph.
<Graph>	The graph displays the number of CIs satisfying all their baseline policies (compliant CIs) with the green bar and the number in breach of a baseline policy (non-compliant CIs) with the red bar.

Policy Summary Pane

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

UI Elements (A-Z)	Description
Policy Name	The policy name. Hold the pointer over the policy name to display a tooltip showing the policy details, including a description and the rule validity.
Policy Status	Bar graphs display the policy satisfaction status for the actual and authorized states. Hold the pointer over a graph to display a tooltip that summarizes the data by percentage and number of CIs.

UI Elements (A-Z)	Description
	Note: The status bar does not display policy satisfaction status for federated policies that contain CIs in the authorized state.

Chapter 11

View Summary

This chapter includes:

View Summary Overview

The View Summary provides a general summary of all of the managed views, displaying authorization level, policy status, the date and time of the last authorization, and the automatic state transition status. It serves as a portal for accessing the managed views by drilling down to the State Management module. You can also export the View Summary data in a report format.

The policy status information enables you to track the views' levels of adherence to policies, both in the actual and in the authorized state. For views with policy breaches, you can drill into the view to see the details (the breaching CIs and policies).

The automatic state transition information enables you to track the views' levels of authorization. It indicates whether a view is state-managed manually or automatically. You can quickly identify the views that require authorization and drill into those views to take the appropriate action.

Additionally, the View Summary enables you to track when the view was last authorized, by whom, and how many changes where authorized. You can drill down to view the last authorization in detail.

Note: The View Summary displays only views for which you have View Read or View Write permission.

Review Automatic State Transition Status

Click 🎗 in the Automatic State Transition Status column for a specific view to display the status of that execution.

For each execution, the date and number of changes are displayed. If there are rules that were not satisfied, those are also displayed.

- If all execution rules are satisfied and all changes are authorized, clicking the **See Details** link takes you to the Historical Comparison (Authorized State) module, where you can see the details of the most recent authorization.

- If all changes did not satisfy the authorization rules, or if the attempt to authorize the changes failed, clicking the **See Details** link takes you to the State Management module, where you can review the changes and manually authorize them.

- If some of the changes were authorized and other changes did not satisfy all authorization rules, clicking the **See Details** link next to the authorized changes takes you to the Historical Comparison (Authorized State) module, and clicking the **See Details** link next to the changes that were not authorized takes you to the State Management module.

View Summary User Interface

This section includes:

View Summary Page

This page displays a summary of the authorization and policy satisfaction statuses for all of the managed views.

To access	Select **Application > View Summary**.

Important information	Click a column header to sort the view summary by that column. When you click a column header, a small black triangle appears. An upward triangle indicates an ascending sort and a downward triangle indicates a descending sort. Click the column header again to toggle between an ascending and a descending sort.

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

UI Elements (A-Z)	Description
⭐	Click **Show favorite views only** to toggle between displaying all views and displaying the favorite views only.
<img>	Click **Export Report** to choose the export format for the View Summary report 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. • **CSV.** The table data is formatted as a comma-separated values (CSV) text file that can be displayed in a spreadsheet.
🔄	Click **Refresh** to refresh the policy list.
⚠	If a warning icon appears next to the view name, hold the pointer over it to display the warning in a tooltip or click it to open the warning in a dialog box.
ⓘ	If an information icon appears next to the view name, hold the pointer over it to display the message in a tooltip or click it to open the message in a dialog box.
<img>	Displays the automatic state transition status of the view.
<Filter views box>	Enter a string in the box to filter the views displayed. Only views with names including the entered string are displayed.
Authorization Level	Displays the authorization level of the view in graphical format as well as numerically (the number of authorized CIs out of total CIs). Hold the pointer over the graph to display a tooltip with percentages for the data.
Authorization Level Legend	The legend for the authorization level graph. The following categories are included: • Authorized CIs • Unauthorized CIs
Last Authorized On	The date and time when the view was last authorized. Click on the date to go to the snapshot of the view at that time in the Authorization History.

UI Elements (A-Z)	Description
Last Data Update	The date and time when the view was last updated.
Policy Status	Displays the status of view's policies in the actual and authorized states using bar graphs. Hold the pointer over the graph to display a tooltip with percentages for the data.
Policy Status Legend	The legend for the policy status graph. The following categories are included: • Satisfied • In-breach
View Name	Click on the view name to go to the State Management page for the selected view.

Chapter 12

Policy Summary

This chapter includes:

Policy Summary Overview

The Policy Summary module provides a general summary of all policies defined in Configuration Manager. The display enables you to view the policy status of all the CIs for which a given policy is defined. You can also export the Policy Summary data in a report format.

> **Note:** Policy statistics are calculated only on views for which you have View Read permission.

Policy Summary User Interface

This section includes:

Policy Summary Page

This page displays a summary of policy satisfaction levels broken down by policy.

To access	Select **Application > Policy Summary**.
Important information	For each policy, the number of CIs in all views at each satisfaction status is displayed. The available states are indicated in the Policy Status Legend: • ☐ Satisfied • ☐ In-breach Click a column header to sort the policy summary by that column. When you click a column header, a small black triangle appears. An upward triangle indicates an ascending sort and a downward triangle indicates a descending sort. Click the column header again to toggle between an ascending and a descending sort.

User interface elements are described below:

UI Elements (A-Z)	Description
⭐	Click **Show only policies which are relevant to favorite views only** to toggle between displaying all policies and displaying policies relevant to favorite views only.
🔁	Click **Export Report** to choose the export format for the Policy Summary Report data. The available options are: • **Export "Policy Summary" Report to Excel.** The table data is formatted as an .XLS (Excel) file that can be displayed in a spreadsheet. • **Export "Policy Summary" Report to PDF.** The table data is exported in PDF format. • **Export "Policy Summary" Report to CSV.** The table data is

UI Elements (A-Z)	Description
	formatted as a comma-separated values (CSV) text file that can be displayed in a spreadsheet.
	Click **Refresh** to refresh the policy list.

Left Pane

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

UI Elements (A-Z)	Description
Policy Name	The policy name. Hold the pointer over the policy name to display a tooltip showing the policy details, including a description and the rule validity.
Policy Status	Bar graphs display the policy satisfaction status for the actual and authorized states. Hold the pointer over a graph to display a tooltip that summarizes the data by percentage and number of CIs. **Note:** The status bar does not display policy satisfaction status for federated policies that contain CIs in the authorized state.

Right Pane

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

UI Elements (A-Z)	Description
<Breakdown by View Table>	A table displaying the policy satisfaction data broken down by view for the policy selected in the left pane. The number of CIs in each view at each status is indicated.

Chapter 13

Configuration Modeling

This chapter includes:

Configuration Modeling Overview

The Configuration Modeling module provides an environment for comparing composite CIs in your managed views with a configuration model. A configuration model is a description of a composite CI, and includes its topology/hierarchy and the attributes of its component CIs. The configuration model can be:

- arbitrary (that is, modeled at will completely by the user)

- created from a composite CI (whether or not that composite CI is actually a candidate for comparison with the model)

- imported from a baseline policy

- based on a group of similar composite CIs

After you run the comparison, the pane displays a bar graph for each composite CI in the comparison, showing the degree to which it matches the model. The closeness of the match is determined by comparing the composite CIs to the model with regard to the topology and to the attributes of each component CI. If no attributes are selected for comparison in a particular CI of the model, the comparison for that CI is based purely on the topology of the model.

A composite CI is considered to be in breach of the model if any of the attributes in its CI hierarchy do not match the model's requirements. In addition, you can choose between two options as to what topology will be considered as satisfying a model:

- If the topology of the composite CI is identical to the topology of the model

- If the topology of the composite CI contains the model topology

For details on the Configuration Modeling module, see <u>"Configuration Modeling Page" (on page 95)</u>.

> **Note:**
>
> - You must have Configuration Analysis permission to work with this module.
>
> - Only views for which you have View Read permission are displayed.
>
> - If you have exceeded your licensed capacity of composite CIs that can be analyzed, a warning notification is displayed. Contact your HP sales representative to purchase a license.

Define a Configuration Model for Comparison

This task describes how to define a configuration model for comparison with selected composite CIs.

	The Configuration Modeling and Analysis movie (to see a demonstration of defining a configuration model for comparison and analysis) can be accessed by clicking the .htm file in the following location: **<Configuration Manager installation directory>\servers\server-0\webapps\docs\en_US\movies\Configuration_ Modeling_and_Analysis\.**

1. Navigate to **Application > Configuration Analysis > Configuration Modeling**. You can create a model in one of the following ways:

   ■ To create a model based on a specific group of similar CIs:

      ○ Select the state of the view from which you want to select composite CIs. The available options are Actual or Authorized.

      ○ Click **Add composite CIs** to open the Add composite CIs dialog box. Select the view containing the CIs you want to compare, then move the CIs to the Selected CIs column using the arrow buttons. Repeat to add additional CIs, if desired, and when you are finished, click **OK**. If the selected view contains more than 1,000 CIs, the top arrow button enables you to randomly select CIs (to a maximum of 1,000).

      > **Note:** If you select CIs in the Analysis Scope pane first and then build a model, Configuration Manager automatically removes any selected CIs whose types do not match the model's type.

      ○ Click in the main Configuration Modeling toolbar. The model that is created tries to satisfy all composite CIs in the scope.

      > **Note:** If you have not selected enough CIs or their attributes or hierarchies are too different from each other, you will be prompted to change your selections.

   ■ To create a model based on a specific CI type, select the CI type by clicking in the Configuration Model toolbar (which creates an empty baseline) or by selecting the CI in the Analysis Scope pane and dragging it to the Configuration Model pane (which creates a fully specified baseline).

   ■ To create a model based on any managed CI (not necessarily a CI in the Analysis Scope), click **Select predefined configuration** in the Configuration Model pane and select **Create a model from a composite CI**.

   ■ To create a model based on a policy that you created in the Configuration Policies module, click **Select predefined configuration** in the Configuration Model pane and select **Create model from existing baseline policy**.

2. Select the attributes to participate in the comparison by selecting the check boxes next to the required attributes. Enter values for the selected attributes in the Attribute Value column and operators in the Operator column.

3. Click **Analyze** in the main toolbar to run the comparison.

Configuration Analysis User Interface

This section includes (in alphabetical order):

Add Composite CIs Dialog Box

This dialog box enables you select a specific CI for a model definition.

To access	Click **Add composite CIs** ➕ in the Analysis Scope pane.
Important information	Only views for which the user has View Read permission are displayed.

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

UI Element	Description
<List of CIs>	The left pane displays the CI name. For composite CIs, you can expand a CI entry to display the individual component CIs. The right pane displays the attribute names and values for this CI.
Filter	Enter a string to filter the CIs in the list.
State	The state of the CIs that was selected in the Analysis Scope pane is displayed.
View	Select a view from the drop-down list.

Comparison Details Dialog Box

This dialog box enables you to display comparison details for the selected CI.

To access	Click **Show comparison details** 🔲 in the Analysis Scope pane.

User interface elements are described below:

UI Elements (A-Z)	Description
🔍	Toggles between displaying all CIs and all attributes, and displaying only attributes and CIs with breaches for the selected composite CI.
🔍	Jumps to the next breach in the current composite CI.
<Left pane>	Displays the CI names and their respective models. For composite CIs, click the arrow to expand it and display the component CIs. For each CI for which there is a model value, an icon indicates whether it is in breach of the policy or not. **Note:** A CI is considered in breach of a policy if at least one of its attributes breaches the policy or if it does not match a CI in the model.
<Right pane>	Displays the attribute names and values, as well as the baseline values, for the CI selected in the left pane. For attributes with baseline values,

UI Elements (A-Z)	Description
	an icon indicates whether or not the selected CI is in breach of the policy with reference to that attribute.

Configuration Modeling Page

This page enables you to build a configuration model to compare to composite CIs from managed views.

To access	Select **Application > Configuration Analysis > Configuration Modeling**.
Important information	The Configuration Modeling page includes the following panes: • Analysis Results • Analysis Scope • Configuration Model Define the model in the Configuration Model pane. Select the composite CIs for comparison in the Analysis Scope pane. When you are finished, click **Analyze** to run the comparison. The results are not updated dynamically in response to changes. Every time you make a change in either the model or the composite CI selection, you need to click **Analyze** again to re-run the comparison.

User interface elements are described below:

UI Elements (A-Z)	Description
	Click **Create New Model** to build a new configuration model.
	Click **Open Model** to select an existing model to open.
	Click **Save Model** to save the current model.
	Click **Save Model As** to save the current model under a new name.
Detail Level ▾	Click **Detail Level** to specify how strictly you want your model to conform to the selected CIs. The following scale is displayed: Less Detailed Model 10% 100% More Detailed Model
品 Analyze Model	Click **Analyze Model** to create a model from the selected CIs, based on the selected level of detail.
↻ Analyze	Click **Analyze** to run the comparison.
◁	Click **Back to Environment Segmentation Analysis** to return to the

UI Elements (A-Z)	Description
	Environment Segmentation Analysis module.

Analysis Results Pane

Important information	After the analysis is run, this pane displays a pie chart showing the percentage of satisfied CIs, as well as a breakdown of how close the in-breach CIs are to being satisfied.

Analysis Scope Pane

Important information	In this pane, you select the composite CIs to compare to the configuration model.

User interface elements are described below:

UI Elements (A-Z)	Description
	Click **Add composite CI**s to select composite CIs to add to the Analysis Scope using the Add Composite CIs dialog box.
	Click **Remove composite CI from list** to delete the selected composite CI from the Analysis Scope.
	Click **Remove all composite CIs** to delete all composite CIs from the Analysis Scope.
	Click **Show Comparison Details** to open the Comparison Details dialog box, which displays the attributes of a CI that is in breach of a policy.
<Composite CI Name>	The names of the managed CIs in the Analysis Scope.
Similarity Results	Displays a bar graph indicating the degree to which the CI matches the model.
State	Select the state of the view from which you are selecting composite CIs.
	You can select CIs from both the actual and authorized state of any view, but the comparison is only done in the selected state. If any of your selected CIs do not exist in that state of the view, they appear in faded text and do not participate in the analysis.

Configuration Model Pane

Important information	In this pane, you build a configuration model by adding CI types to the model and selecting the attributes by which to compare it to the selected composite CIs.

User interface elements are described below:

UI Elements (A-Z)	Description
	Click to select a predefined configuration: • **Create model from a managed CI.** Select an existing CI to serve as a configuration model. • **Create model from existing baseline policy.** Select a configuration model already defined in a policy.
	Click to select a CI type to add to the configuration model. You can add multiple CIs of the same type using the CI count feature. **Note:** CIs are added hierarchically under the currently selected CI.
	Click to delete the selected CIs from the configuration model.
	Click **Matching CI Results** to view a breakdown of the compared CIs into satisfied and in-breach categories.
	Indicates that the attribute is relevant for comparison.
	Indicates that the attribute is relevant for comparison and is assigned a rank in the system's matching algorithm.
Attribute Name column	The names of the attributes of the selected CI type.
Attribute Value column	The values of the attributes of the selected CI type. Select or enter a value for each attribute. To display suggested values, begin typing or press the Down arrow key.
CI Type	The selected CI types. It is possible to select more than one CIT of the same type in the model. This is known as **Common Definition mode**. In this mode, any changes you make to one of the selected CITs apply to all of them.
Consider additional internal CIs as breach	When you select **Consider additional internal CIs as breach**, the CI being compared to this configuration model is considered in breach of the policy if it has additional internal CIs.
Matching CI Results column	A bar graph displays the number of satisfied, in-breach, and missing CIs for each CI type. Hold the pointer over the graph to display a tool tip with percentages.
Matching Results column	For each selected attribute, the percentage indicates the number of composite CIs matching the values specified for that attribute in the model.
Operator column	Select an operator defining the required relationship between the attribute's baseline value and the actual value. For details, see "Attribute Operators" (on page 64).

Select Baseline Policy Dialog Box

This dialog box enables you to select an existing baseline policy, whose baseline will be used as a model definition.

To access	In the Configuration Model pane, click [icon] and select **Create model definition from existing baseline policy**.

User interface elements are described below:

UI Elements (A-Z)	Description
Policy Name	Displays a list of defined baseline policies that you can use as a baseline for the model.
Policy Status	For each policy in the list, displays the percentage of CIs on which the policy is satisfied or breached.

Select Composite CI Dialog Box

This dialog box enables you select a specific CI for a model definition.

To access	In the Configuration Model pane, click [icon] and select **Create model from a managed CI**.
Important information	When you select a specific CI for a model definition, CIs in the scope are removed if their type does not match the selected CI's type. Only views for which the user has View Read permission are displayed.

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

UI Elements (A-Z)	Description
<List of CIs>	A list of the CI names and types in the selected view. Select one to serve as the model CI.
Filter	Enter a string to filter the CIs in the list.
State	Select **Actual** or **Authorized**.
View	Select a view from the drop-down list.

Chapter 14

Environment Segmentation Analysis

This chapter includes:

Environment Segmentation Analysis Overview

The Environment Segmentation Analysis module can create CI segments (a group of CIs with similar configuration).

You select CIs as input and specify the desired level of similarity between the CIs in each segment that is created. When selecting CIs as input, there does not need to be any specific similarity between them. Configuration Manager generates a list of segments and creates a configuration model for each segment. Every CI that you selected as input becomes part of one of the created segments.

You can select a segment and then analyze it in the Configuration Modeling module, or use the CIs that it contains as the basis for a different model.

For details on the Environment Segmentation Analysis module, see "Environment Segmentation Analysis Page" (on page 103).

> **Note:**
>
> - You must have Configuration Analysis permission to work with this module.
>
> - Only views for which you have View Read permission are displayed.
>
> - If you have exceeded your licensed capacity of controlled automations that can be run, a warning notification is displayed. Contact your HP sales representative to purchase a license.

Select CIs that Contain Groups of Similar CIs

This task describes how to select CIs among which you can find groups of similar CIs.

1. Navigate to **Application > Configuration Analysis > Environment Segmentation Analysis**.

2. Select the state of the view from which from which to take CIs for comparison. The available options are Actual or Authorized.

3. Click **Add composite CIs** to open the Select Composite CIs dialog box. The CIs will be chosen from the state which you selected in step 2. You can select a maximum of 1,000 composite CIs.

   > **Note:** You must select CIs of the same CI type.

4. Click to set the segment size parameter to the required value and to define the scope of the segment.

   - Selecting a low value causes more, smaller segments to be created, and the composite CIs in those segments will be more similar to each other.

   - Selecting a high value causes fewer, larger segments to be created, and the composite CIs in those segments will be more varied.

5. Click to create the segments.

6. Review the results: The Segments List displays the name of each segment, the number of composite CIs in it, and the average similarity level that the composite CIs in the segment have to the segment's model. Click a segment in the list (Segments List pane) or in the pie chart (Segments Results pane) to view the model in the Configuration Model pane.

7. To further analyze the contents of a segment, select the segment in the Segments List and click **View Configuration Modeling for selected segment** 📇. This takes you to the Configuration Modeling module, with the selected segment being used as the model.

> **Note:** If you now make changes in the Configuration Modeling module, they are not reflected in the Environment Segmentation module. For example, removing or adding CIs from the Analysis Scope in Configuration Modeling will not remove them from the segment or from the scope in the Environment Segmentation module.

Environment Segmentation Analysis User Interface

This section includes (in alphabetical order):

Add Composite CIs Dialog Box

This dialog box enables you select a specific CI for a model definition.

To access	Click **Add composite CIs** ➕ in the Analysis Scope pane.
Important information	Only views for which the user has View Read permission are displayed. You can only select CIs of the same type for the definition.

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

UI Element	Description
<List of CIs>	The left pane displays the CI name. For composite CIs, you can expand a CI entry to display the individual component CIs. The right pane displays the attribute names and values for this CI.
Filter	Enter a string to filter the CIs in the list.
State	The state of the CIs that was selected in the Analysis Scope pane is displayed.
View	Select a view from the drop-down list.

CI Details Dialog Box

This dialog box enables you to display comparison details for the selected CI.

To access	Click **Show CI details** 🔲 in the Analysis Scope pane.

User interface elements are described below:
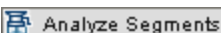
UI Element	Description
🔲	Toggles between displaying only the managed attributes and displaying all attributes for the selected CI. By default, only managed attributes are displayed.
CI Name	Displays the name of the selected CI.
Attribute Name	Lists the attributes that are being modeled for the selected CI.
Value	Displays the value that is currently assigned to the selected attribute.

Environment Segmentation Analysis Page

This page enables you to find groups of similar CIs in your environment.

To access	Select **Application > Configuration Analysis > Environment Segmentation Analysis**.
Important information	The Environment Segmentation Analysis page includes the following panes: ● Analysis Scope ● Segments List and Results (in chart format) ● Configuration Model Select the composite CIs from which to create segments in the Analysis Scope pane. When you are finished, click **Analyze Segments**. The results are not updated dynamically in response to changes. Every time you make a change to the analysis scope or to the parameters described below, you need to click **AnalyzeSegments** again to re-create the groups.

User interface elements are described below:

UI Elements (A-Z)	Description
📄	Click **Create New Model** to clear all selected values and segments.
Parameters	Click Parameters to open the Segmentation Parameters dialog box. For details, see "Configuration Explorer Page" (on page 148)
Analyze Segments	Click **Analyze Segments** to create segments based on the selected

UI Elements (A-Z)	Description
	CIs.

Analysis Scope Pane

Important information	In this pane, you select the composite CIs to be used for creating the segments.

User interface elements are described below:

UI Elements (A-Z)	Description
➕	Click **Add composite CI** to select composite CIs to add to the Analysis Scope. For details, see "CI Details Dialog Box" (on page 103).
✖	Click **Remove composite CI from list** to delete the selected composite CI from the Analysis Scope.
✖	Click **Remove all composite CIs** to delete all managed CIs from the Analysis Scope.
🗐	Click **Show CI details** to open the CI Details dialog box. For details, see "CI Details Dialog Box" (on page 103).
<Composite CI Name>	The names of the composite CIs in the Analysis Scope.
Segment ID	Displays the name of the segment to which the composite CI was assigned.
State	Select the state of the view from which you are selecting composite CIs. You can select CIs from both the actual and authorized state of any view, but the segmentation is only done in the selected state. If any of your selected CIs do not exist in that state of the view, they appear in faded text and do not participate in the segmentation.

Configuration Model Pane

Important information	This pane displays the configuration model generated for the selected segment. Select a CI in the model to see the attributes defined for it. The attributes that are greyed out are not selected for the model.

User interface elements are described below:

UI Elements (A-Z)	Description
Attribute Name	The names of the attributes of the selected CI type.
Attribute Value	The values of the attributes of the selected CI type.

UI Elements (A-Z)	Description
CI Type	The selected CI types.
Operator	The required relationship between the attribute in the model and the attribute in the compared CI. For details, see "Attribute Operators" (on page 64).

Segments List Pane

Important information	After the segments are created, this pane displays a list of the segments that were created.

User interface elements are described below:

UI Elements (A-Z)	Description
🖼	Click **View Configuration Modeling for selected segment** to open the Configuration Modeling page, where you can edit the model and save it.
Average Similarity	The average percentage of similarity between the CIs in the segment and the segment's configuration model.
Number of CIs	The number of CIs in each segment.
Operator column	The attribute that defines the relationship between the attribute and its value. For details, see "Attribute Operators" (on page 64).

Segments Results Pane

Important information	After the segments are created, this pane displays a pie chart showing the groups of CIs that were created, based on the selected segment size.

Segmentation Parameters Dialog Box

This dialog box enables you to specify the detail level and scope for the selected CIs that are part of the suggested segment.

To access	Click **Parameters** on the Environment Segmentation Analysis page.

UI Element	Description
Similarity Level	The Similarity Level setting specifies the similarity level of the CIs in the segment. The following scale is displayed: Lower Similarity Level 1% 100% Higher Similarity Level A small value means that a segment contains CIs that may be varied; a

UI Element	Description
	large value means that each segment contains CIs that are very similar to each other.
Define Configuration Model Scope	Specify the CI type and attributes that should appear in the model. By default, all components and attributes in the selected CIs are part of the model. If you do not want a specific component to be part of the model, clear the check box next to that component. When you remove a component from the model, all of its attributes are automatically removed from the model as well. You can include a component in the model but remove all of its attributes from the scope by clearing the check box in the title bar next to Attribute Name, or you can remove selected attributes by clearing those check boxes.

Chapter 15

State Management

This chapter includes:

State Management Overview

The State Management module enables you to review and authorize changes in a view. State Management displays all the CIs currently contained in the view in either the actual or authorized state. For example, an application owner might want to track and acknowledge changes that occur in their application service tree. CIs that were added to the view, removed from the view, or updated between the two states are indicated by the appropriate indicator icon in the Composite CIs pane and the Topology pane. For details on the indicator icons, see "Composite CIs Pane" (on page 116).

You begin the authorization process by analyzing (or reviewing) the changes you want to authorize: check the type and nature of the change, whether there are new policy breaches and whether there are related RFCs. Select the changes you want to authorize from among the CIs marked as changed. When you click **Authorize**, all of the selected changes are submitted for authorization. After the authorization finishes, the authorized state is updated with the selected changes, and a snapshot of the view is saved. For details on manual authorization, see "Authorize Changes to CIs" (on page 109).

It is also possible to authorize views automatically using the automatic state transition feature. The automatic state transition rules are validated against all managed CIs in the view, and the CI changes are automatically authorized if they comply with these rules. For details, see "Automatic State Transition" (on page 49).

Before authorizing changes (either manually or during automatic state transition, Configuration Manager checks whether any CI that may be deleted as the result of authorizing a change has any other CIs that are dependent on it. A warning notice will be displayed during authorization for the following situations:

- If the removal of a CI in one view leads to the removal of its dependent CIs in another view.

- If the removal of a CI leads to the removal of a CI that is a component of the composite CI in another view.

- If CI to be removed has any relation in another view.

- If the authorization of a change in one view will cause a policy breach in another view.

> **Note:** You must have one of the following permissions to access the State Management module:
>
> - View Read permits you to select and review changes.
>
> - View Write permits you to review and authorize changes.

Integration with Service Manager

Configuration Manager enables you to push CIs from UCMDB to Service Manager in authorized as well as actual state. When you create a new integration point in UCMDB using the Service Manager 7.1x - 9.2x adapter, you can select from which state data should be pushed. For details, see "New Integration Point/Edit Integration Point Dialog Box" in the *HP Universal CMDB Data Flow Management Guide*. However, you can only access the Data Flow Management module in UCMDB when you are logged in to Configuration Manager in the actual state.

When setting up an integration, you must load the **cm4sm.unl** file into Service Manager. This file enables the service that allows integration between Service Manager and Configuration Manager. For details, see "Import a UNL File into Service Manager" (on page 110).

Both planned and unplanned changes are taken into consideration before they are authorized. One of the following scenarios is possible:

- Planned change—one or more related RFCs have already been opened for a discovered change. When they are authorized, the related RFCs are then validated.

- Unplanned change—no RFC had previously been opened for the change.

  - If the change does not affect the CI (for example, if the discovery pattern for this CI changed), you can authorize the change without creating an RFC.

  - If there is an actual change to the CI or its attributes, you can create an RFC through Configuration Manager.

As part of the offline analysis process, Configuration Manager checks and stores RFCs that are related to changed CIs. The following CIs are checked for RFCs:

- Changed CIs

- Containers of changed CIs

- Relations of changed CIs

For each CI in a managed view, the analysis process checks if the CI has a related RFC. If no related RFC is found for a CI, then the containing CI is queried for RFCs, and if there is no RFC on the containing CI, the connected CIs are checked.

Note that the same RFC can be related to more than one CI, and a single CI can also be related to several RFCs. For example, if an RFC is found on a host in one view, the same RFC is related to the host in other views.

There are four possible relationships between CIs in Configuration Manager and RFCs in Service Manager:

- Direct—a CI has a direct relation to an RFC.

- Container—the container of a CI has a relation to the RFC.

- Manual—an RFC is manually created for a changed CI.

- Relation—multiple CIs that are related to each other are related to the same RFC.

Authorize Changes to CIs

This task describes how to authorize changes to composite CIs.

	The Change Authorization movie (to see a demonstration of how to authorize a change) can be accessed by clicking the .htm file in the following location: **<Configuration Manager installation directory>\servers\server-0\webapps\docs\en_US\movies\Change_Authorization\.**

Changes to CIs can include:

- all attribute changes for a CI (you cannot authorize individual attribute changes)

- adding or removing a CI

- incoming relationship changes

- outgoing relationship changes

To authorize a change:

1. In the Composite CIs pane of the State Management module, expand the entries for the CIs with changes by clicking the small arrow to the left of each check box. Each change for a given CI appears on its own line.

2. After reviewing the changes, select the check boxes for the ones that you want to authorize.

   Note: If you select the check box for a CI, all the changes for that CI are automatically selected.

3. When you are finished reviewing the changes, do one of the following:

   - Click **Authorize** to authorize the selected planned changes and validate their existing RFCs.

     A message appears stating that the changes were submitted for authorization. Click **OK**.

   - Click **Create rollback RFC for the selected changes** to create an RFC incident ticket. for each selected CI.

     Enter the required information and click **Submit**. For details, see "Create RFC for Rolling Back Changes Dialog Box" (on page 112).

   Note: The authorization process may take a long time. You can continue working on other views while it proceeds.

   The updated view becomes the new authorized state of the view.

Import a UNL File into Service Manager

This task describes how to upload the **cm4sm.unl** UNL file to Service Manager, in order to activate the service that enables integration between Service Manager and Configuration Manager.

To import the UNL file:

1. In Service Manager, click **Menu Navigation > Tailoring > Database Manager**.

2. Right-click the detail button and select **Import/Load**.

3. In the HP Service Manager File Load/Import page, click **Specify File** and select **<Configuration Manager installation folder>/adapters/sm/cm4sm.unl**.

   The file is loaded via the file browser.

4. Enter the description in the **Import Description** box.

5. Select **winnt** in the **File Type** list.

6. Select a display option.

7. Click **Load FG** to start loading.

State Management User Interface

This section includes (in alphabetical order):

Authorize Selected Differences Dialog Box

This dialog box enables you to select the specific changes that you want to authorize.

To access	Click **Authorize** in the left pane of the State Management page.
Important information	By clicking **Submit**, you are authorizing the proposed changes. This transforms the actual state of the CI into its new authorized state.
	If the **Change Management integration enabled** check box in the System Settings page is enabled, validation of the selected RFCs will be logged in the change management system. If this check box is not selected, the changes will only be noted when creating reports and RFCs will not be validated in the change management system.
	Note: You cannot authorize a CI whose parent CI is not contained in the view.

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

UI Elements (A-Z)	Description
<List of CIs with proposed changes>	The list of changes that were displayed for authorization in the Composite CIs pane.
	For each CI in the list, a list of related RFCs is displayed. Select the relevant RFC check boxes for the specific changes that you want to log in the change management system.

CI Details Dialog Box

This dialog box enables you to view details of a selected CI.

To access	Click **Show Composite CI Details** 🖼 or double-click a CI in the Composite CIs pane or Topology pane.

User interface elements are described below:

UI Elements (A-Z)	Description
🔍	Click **Show Only Differences** to display only those attributes where the value differs between the two states displayed.
🔍	Click **Next Difference** to jump to the next component CI in the list.
🖼	In the Attributes tab, toggles between displaying only the managed attributes and displaying all attributes for the selected CI. By default, only managed attributes are displayed.
≠	Indicates a difference between the value in the two states displayed.
Attributes tab	The left pane displays the CI name. For composite CIs, you can expand a CI entry to display the individual component CIs. The right pane displays the attribute names and values for this CI. Both the actual values and the authorized values of the attributes are displayed.
Incoming Relationships tab	Displays all the relationships of the selected CI in the incoming direction. For composite CIs, you can expand a CI entry to display the individual component CIs. When you select one of the component CIs, the Internal Relationship Path Details pane at the bottom of the dialog box displays more detailed information about the relationship.
Outgoing Relationships tab	Displays all the relationships of the selected CI in the outgoing direction. For composite CIs, you can expand a CI entry to display the individual component CIs. When you select one of the component CIs, the Internal Relationship Path Details pane at the bottom of the dialog box displays more detailed information about the relationship.

Create RFC for Rolling Back Changes Dialog Box

This dialog box enables you to create an RFC for an unplanned and undesired change, which will be validated in Service Manager.

To access	Click **Rollback** 🔄 in the left pane of the State Management page.
Important information	Enter a title and select the relevant information for the RFC that you are creating for the unplanned change.

| | By clicking **Submit**, you are creating an RFC and manually relating it to the selected CIs. |

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

UI Elements (A-Z)	Description
Affected CIs	The list of changes that were marked for authorization in the Composite CIs pane.
Category	Select a category from the displayed list of category values (set on the System Settings page). For details, see "RFC Creation" (on page 177).
Description	The list of CIs and the required actions that should be performed for each CI. If a single CI has been selected, an automatically generated description is displayed.
Impact	Select the widest range of impact that the change will have from the displayed list of values (set on the System Settings page). For details, see "RFC Creation" (on page 177).
Requested end date	The date by which the RFC should be executed.
Risk assessment	Select the level of risk for the changed CI from the displayed list of values (set on the System Settings page). For details, see "RFC Creation" (on page 177).
Service	The list of services that are available to the CI.
Title	Enter a title for the RFC, for example, a short summary of the requested changes.
Urgency	Select the level of urgency for the change in the CI from the displayed list of values (set on the System Settings page). For details, see "RFC Creation" (on page 177).

Policy Details Dialog Box

This dialog box enables you to display detailed information on CI policy breaches for baseline policy rules.

To access	Click **Show Composite CI Details** 🔲 in the Comparison Details pane.
Important information	The Policy Details dialog box is only relevant when a CI with a baseline policy is selected. Click the small arrow next to the icon and select the dialog box displaying policy details for the actual or authorized state.

User interface elements are described below:

UI Elements (A-Z)	Description
🔍	Toggle between displaying all attributes and only those with breaches, for the selected CI.
🔍	Jump to the next breach in the list.
<Left pane>	Displays the CI names and their respective baselines. For composite CIs, click the arrow to expand it and display the component CIs. For each CI for which there is a baseline value, an icon indicates whether it is in breach of the policy or not. **Note:** A CI is considered in breach of a policy if at least one of its attributes breaches the policy or if it does not match a CI in the baseline.
<Right pane>	Displays the attribute names and values, as well as the baseline values, for the CI selected in the left pane. For attributes with baseline values, an icon indicates whether or not the selected CI is in breach of the policy with reference to that attribute.

Sort CIs Dialog Box

This dialog box enables you to sort the CI list in the Composite CIs pane.

To access	Click the **Sort Composite CIs** button 🔽 from the toolbar in the Composite CIs pane.
Important information	Save the new sort fields for the change to take effect.

User interface elements are described below:

UI Elements (A-Z)	Description
📑	Move all the fields from the Available Sort Fields pane to the Selected Sort Fields pane.
➡	Move the selected field from the Available Sort Fields pane to the Selected Sort Fields pane.
✖	Remove the selected field from the Selected Sort Fields pane.
✖	Remove all the fields from the Selected Sort Fields pane.
↑ ↓	Move a selected field up or down within the Selected Sort Fields list.
⬇ ⬆	For each selected field, select **Ascending** or **Descending** for the sort direction.
Available Sort Fields	All the available fields by which to sort the CIs.

UI Elements (A-Z)	Description
Selected Sort Fields	The selected fields by which to sort the CIs. The sort order follows the order of the list.

State Management Page

This page enables you to display a view in the actual state and select the changes that you want to authorize.

To access	Select **Application > State Management**.
Important information	The State Management page includes the following panes: ● **Composite CIs.** Displays a list of CIs in the view with icons indicating the types of changes that occurred for each CI between the actual and authorized states. ● **Topology.** Displays a topology map of the CIs in the view with icons indicating the types of changes that occurred for each CI between the actual and authorized states. Each node in the topology map displays the name, CI type, and management status, as well as the change type and current and previous policy status, where relevant. For details, see "Topology Pane" (on page 150). **Note:** In inventory mode, the Topology pane is called **Related CIs**. ● **Comparison Details.** Displays details of the changes for the selected CI. Click the relevant tab to view the change details for the selected CI. ● **Filter.** In inventory mode, the Filter pane enables you to filter the composite CI list. For details, see "Filter Pane" (on page 152). Select the changes to authorize by clicking the check boxes next to the relevant CIs in the Composite CIs pane.

User interface elements are described below:

UI Elements (A-Z)	Description
	Click **Select View** to select a different view to open on the State Management page.
	Click to change the display to inventory mode.
	Click to change the display to topology mode.
	Click **Export Report** to choose a report to export and the export format for the data. The available reports are: ● **Change Report** ● **Policy Analysis Report**

UI Elements (A-Z)	Description
	The available format 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.
	• **CSV.** The table data is formatted as a comma-separated values (CSV) text file that can be displayed in a spreadsheet.
	Click **Refresh** to refresh the CI list.

Composite CIs Pane

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

UI Elements (A-Z)	Description
	Click **Select All** to select all the CI entries.
	Click **Clear All** to clear all the CI entries.
	Click **Sort Composite CIs** to open the Sort CIs dialog box, which enables you to sort the CI list by different sort fields.
	Click **Show Composite CI Details** to open the CI Details dialog box, which displays the managed attributes of the selected CI.
	Click **Authorize** to approve the selected changes and change their status to authorized.
	Note: This button is only enabled if you have selected at least one CI (that has changed) in the list.
Launch ▾	Click ▾ to select an external application to open in the context of a selected CI or view. You must specify the URLs that will open on the System Settings page. For details, see "UI Integrations" (on page 180).
	Indicates that the selected CI was added to the view.
	Indicates that the selected CI was removed from the view.
	Indicates that the selected CI was updated.
	Indicates that the CI is in breach of at least one policy in the actual state.
	Indicates that the CI is in breach of at least one policy in the authorized state.
	Indicates that the CI satisfies all of its policies in the actual state.

UI Elements (A-Z)	Description
⊙	Indicates that the CI satisfies all of its policies in the authorized state.
▢	Indicates that there are one or more requests for change (RFCs) that are related to this CI.
\<List of CIs\>	The list displays all CIs currently or previously in the view. The icons appearing to the right of the CI indicate the changes that have occurred to this CI and its policy status. Click the triangle next to the CI to display each of the changes in a separate row. Hold the pointer over a CI in the list to display a tooltip containing the name and type of the CI. If no icons appear after a CI, it indicates that no changes have occurred to that CI. Click the check box next to a selected change to mark it for authorization.

Comparison Details Pane

Important information	When you select a CI in the Composite CIs pane or the Topology pane, the tabs that contain data for that CI are marked with an asterisk (*).

User interface elements are described below:

UI Elements (A-Z)	Description
Changed Attributes tab	The left pane displays the CI name and the change type icon. For composite CIs, the component CIs with changed attributes are displayed. The right pane displays the attribute names and actual and authorized values for the CI selected in the left pane.
Changed Outgoing Relationships tab	The left pane displays the CIs to which the selected CI is related by an outgoing relationship. Click the arrow to expand each entry and display the relationships of the component CIs. For each relationship, the relationship type is displayed and an icon indicates the relevant type of change. The right pane displays the source, target, and direction for the relationship selected in the left pane.
Policy Details tab	In the **Policy List pane**, the following data is displayed for each policy rule: ● the policy rule name ● the rule status in the actual state ● the rule status in the authorized state

UI Elements (A-Z)	Description
	• the related CI The **Details pane** displays the details for the policy rule selected in the Policy List pane, including the rule name, description, type, and validation dates.
Related RFCs tab	The left pane displays the RFC IDs that were correlated to the selected CI during the offline analysis process or that were manually attached by the user, as well as the title and relation type. The right pane displays the properties for the RFC ID selected in the left pane.

Filter Pane

User interface elements are described below:

UI Elements (A-Z)	Description
Changed CIs	Filter the CIs by their change status. When you select **Yes**, only CIs with changes appear in the view display. When you select **No**, only CIs without changes appear in the view display. **Available in:** State Management module.
CI Name	Filter the CIs by CI name. Only the selected CIs appear in the view display. Enter a CI name manually in the value box or click **More...** to open a dialog box which enables you to select CIs from a list.
CI Type	Filter the CIs by CI type. Only CIs of the selected CI types appear in the view display. Click **More...** to open a dialog box that enables you to select available CI types from a list.
Has RFCs	Filter according to whether or not the selected CI has an RFC associated with it. **Available in:** State Management module.
Managed Status	Filter the CIs by their management status. Only CIs of the selected status appear in the view display. Select **Managed** or **Not Managed**.
Policy Name	Filter the CIs by the names of their policies. Only CIs affected by the selected policies appear in the view display. Click **More...** to open a dialog box that enables you to select available policies from a list.
Policies Status	Filter the CIs by their policy status. Only CIs of the selected status

UI Elements (A-Z)	Description
	appear in the view display.
	If no policy is specified in the Policy Name field, the selected policy status condition will apply to all policies that are assigned to the CIs in the view; otherwise, the selected policy status condition will be applied only to the policies that were specified by name.
	Select **In-breach** or **Satisfied**.
Related RFCs	Filter the CIs by specific RFC titles.
	Click **More...** to open a dialog box that enables you to select related RFC values from a list.
	Available in: State Management module.

View Topology Dialog Box

This page displays the topology map in a large format.

To access	Click the **Show Topology in Full Screen** button from the Topology pane toolbar.

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

UI Elements (A-Z)	Description
	Click the small arrow next to the **Highlight Topology Nodes** button to open the menu.
	Select the display mode for the map:
	• Highlight Actual State
	• Highlight Authorized State
	• Highlight Both
<Topology pane toolbar buttons>	The toolbar buttons from the Topology pane are also available in the View Topology dialog box. For details, see "Topology Pane" (on page 150).

Troubleshooting and Limitations

Note the following limitations about authorizing CIs that are managed in multiple views:

- When automatic authorization occurs, a snapshot will be created only for the view that invoked the authorization.

- If an authorized CI follows a different folding view in each of the managed views, only the view containing the specific CI being authorized will be updated.

Chapter 16

Historical Comparison

This chapter includes:

Historical Comparison Overview

A **snapshot** of a view is a documentation of a state of a view at a particular time, which is recorded as part of the view history. Configuration Manager automatically records a snapshot of the actual and authorized states of a view at the time of each authorization. In addition, Configuration Manager periodically checks for changes in managed views and takes a snapshot of the actual or authorized state when a change is identified. Snapshots can be useful in problem management by providing accurate information about a system from the time an incident occurred.

An example of an application of snapshots is where a snapshot is taken after an installation, and later compared to the original configuration baseline.

The Actual State Historical Comparison module enables you to display a comparison of two snapshots of a view in the actual state. The Authorized State Historical Comparison module enables you to display a comparison of two snapshots in the authorized state. In both modules, the topology map and CI list display all CIs included in the view in either snapshot. The CIs with differences have icons indicating the changes in the CI between the two snapshots.

The snapshots for comparison can be selected from a list of previously saved snapshots as well as the current (actual or authorized) state of the view. For details on selecting snapshots, see "Select Snapshot to View Dialog Box" (on page 129).

> **Note:** You must have one of the following permissions to access the Historical Comparison module:
>
> - View Read permits you to select views.
>
> - View Write permits you to select views and save a snapshot.

Compare Snapshots

This task describes how to select two snapshots of the actual or authorized state of a view and compare them.

To compare snapshots:

1. In Actual State Historical Comparison or Authorized State Historical Comparison, click in the first selection box or click the **Select Snapshot** button 📷 in the toolbar. The **Select snapshot to view** dialog box opens.

2. Select a snapshot from the list and click **OK**.

3. Click in the second selection box to select a different snapshot and click **OK**.

   The data displayed in the topology map reflects the difference between the two selected snapshots of the view.

Historical Comparison User Interface

This section includes (in alphabetical order):

Actual State Historical Comparison Page

This page enables you to compare two snapshots of a view in the actual state.

To access	Select **Application > Historical Comparison > Actual State**.
Important information	The Actual State Historical Comparison page includes the following panes: ● **Composite CIs.** Displays a list of CIs in the view with icons indicating the types of changes that occurred for each CI between the two selected snapshots. ● **Topology.** Displays a topology map of the CIs in the view with icons indicating the types of changes that occurred for each CI between the two selected snapshots. Each node in the topology map displays the name, CI type, and management status, as well as the change type and current and previous policy status for both snapshots. For details, see "Topology Pane" (on page 150). **Note:** In inventory mode, the Topology pane is called **Related CIs**. ● **Comparison Details.** Displays details of the changes for the selected CI. Click the relevant tab to view the change details for the selected CI. ● **Filter.** In inventory mode, the Filter pane enables you to filter the composite CI list. For details, see "Filter Pane" (on page 152).

User interface elements are described below:

UI Elements (A-Z)	Description
🔗	Click **Select View** to select a different view to open on the Actual State Historical Comparison page.
▦	Click to change the display to inventory mode.
📊	Click to change the display to topology mode.
<Compare between snapshots> 📷	Select the two snapshots you want to compare by clicking the snapshot selection boxes to open the **Select snapshot to view** dialog box. **Note:** The comparison is done on all the changes that occurred to the CIs after the time of the first selected snapshot, up to and including the time of the second snapshot.

UI Elements (A-Z)	Description
(icon)	Click **Edit Comments** to edit the comments for the selected snapshot.
(icon)	Click the arrows to jump to the previous or the next pair of snapshots.
(icon)	Click **Export Report** to choose a report to export and the export format for the data. The available reports are: ● **Change Report.** Displays the changes (add, remove, or update) that occurred to CIs and their attributes between the selected snapshots. ● **Changes Over Time.** Displays all the changes (add, remove, or update) that occurred to CIs and their attributes between the selected snapshots, including changes that occurred during intermediate snapshots. This report also displays the policy status summary of each changed CI. ● **Policy Analysis Report.** Displays the CIs, their relevant policies, and the status of each policy at the time of each snapshot. The available format 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. ● **CSV.** The table data is formatted as a comma-separated values (CSV) text file that can be displayed in a spreadsheet.
(icon)	Click **Refresh** to refresh the CI list.

Composite CIs Pane

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

UI Elements (A-Z)	Description
(icon)	Click **Sort Composite CIs** to open the Sort CIs dialog box which enables you to sort the CI list by different sort fields.
(icon)	Click **Show Composite CI Details** to open the CI Details dialog box which displays the managed attributes of the selected CI.
(icon)	Indicates that the selected CI was added to the view.
(icon)	Indicates that the selected CI was removed from the view.
(icon)	Indicates that the selected CI was updated.
(icon)	Indicates that the CI is in breach of at least one policy in the primary snapshot.

UI Elements (A-Z)	Description
⏷	Indicates that the CI is in breach of at least one policy in the secondary snapshot.
⬤	Indicates that the CI satisfies all of its policies in the primary snapshot.
⬤	Indicates that the CI satisfies all of its policies in the secondary snapshot.
<List of CIs>	The list displays all CIs currently or previously in the view. The icons appearing to the right of the CI indicate the changes that have occurred to this CI and its policy status. Click the triangle next to the CI to display each of the changes in a separate row. Hold the pointer over a CI in the list to display a tooltip containing the name and type of the CI. If no icons appear after a CI, it indicates that no changes have occurred to that CI.

Comparison Details Pane

Important information	When you select a CI in the Composite CIs pane or the Topology pane, the tabs that contain data for that CI are marked with an asterisk (*).

User interface elements are described below:

UI Elements (A-Z)	Description
Changed Attributes tab	The left pane displays the CI name and change type icon. For composite CIs, the component CIs with changed attributes are displayed. The right pane displays the names and the primary and secondary snapshot attribute values for the CI selected in the left pane.
Changed Outgoing Relationships tab	The left pane displays the CIs to which the selected CI is related by an outgoing relationship. Click the arrow to expand each entry and display the relationships of the component CIs. For each relationship, the relationship type is displayed and an icon indicates the relevant type of change. The right pane displays the source, target, and direction for the relationship selected in the left pane.
Policy Details tab	In the **Policy List pane**, the following data is displayed for each policy rule: • the policy rule name • the rule status in the primary snapshot (Status) • the rule status in the secondary snapshot (Previous Status) • the related CI

UI Elements (A-Z)	Description
	The **Details pane** displays the details for the policy rule selected in the Policy List pane, including the rule name, description, type, and validation dates.

Authorized State Historical Comparison Page

This page enables you to compare two snapshots of a view in the authorized state.

To access	Select **Application > Historical Comparison > Authorized State**.
Important information	The Authorized State Historical Comparison page includes the following panes: • **Composite CIs.** Displays a list of CIs in the view with icons indicating the types of changes that occurred for each CI between the two selected snapshots. • **Topology.** Displays a topology map of the CIs in the view with icons indicating the types of changes that occurred for each CI between the two selected snapshots. Each node in the topology map displays the name, CI type, and management status, as well as the change type and current and previous policy status for both snapshots. For details, see "Topology Pane" (on page 150). **Note:** In inventory mode, the Topology pane is called **Related CIs**. • **Comparison Details.** Displays details of the changes for the selected CI. Click the relevant tab to view the change details for the selected CI. • **Filter.** In inventory mode, the Filter pane enables you to filter the composite CI list. For details, see "Filter Pane" (on page 152).

User interface elements are described below:

UI Elements (A-Z)	Description
	Click **Select View** to select a different view to open on the Actual State Historical Comparison page.
	Click to change the display to inventory mode.
	Click to change the display to topology mode.
<Compare between snapshots>	Select the two snapshots you want to compare by clicking the snapshot selection boxes to open the **Select snapshot to view** dialog box. **Note:** The comparison is done on all the changes that occurred to the CIs after the time of the first selected snapshot, up to and including the time of the second snapshot.

UI Elements (A-Z)	Description
💬	Click **Edit Comments** to edit the comments for the selected snapshot.
🔼🔽	Click the arrows to jump to the previous or the next pair of snapshots.
📄	Click **Export Report** to choose a report to export and the export format for the data. The available reports are: ● **Change Report.** Displays the changes (add, remove, or update) that occurred to CIs and their attributes between the selected snapshots. ● **Changes Over Time.** Displays all the changes (add, remove, or update) that occurred to CIs and their attributes between the selected snapshots, including changes that occurred during intermediate snapshots. This report also displays the policy status summary of each changed CI, and the related RFCs. ● **Policy Analysis Report.** Displays the CIs, their relevant policies, and the status of each policy at the time of each snapshot. The available format 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. ● **CSV.** The table data is formatted as a comma-separated values (CSV) text file that can be displayed in a spreadsheet.
🔄	Click **Refresh** to refresh the CI list.

Composite CIs Pane

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

UI Elements (A-Z)	Description
⬇	Click **Sort Composite CIs** to open the Sort CIs dialog box which enables you to sort the CI list by different sort fields.
📋	Click **Show Composite CI Details** to open the CI Details dialog box which displays the managed attributes of the selected CI.
➕	Indicates that the selected CI was added to the view.
➖	Indicates that the selected CI was removed from the view.
⬆	Indicates that the selected CI was updated.
🔻	Indicates that the CI is in breach of at least one policy in the primary

UI Elements (A-Z)	Description
	snapshot.
▼	Indicates that the CI is in breach of at least one policy in the secondary snapshot.
●	Indicates that the CI satisfies all of its policies in the primary snapshot.
●	Indicates that the CI satisfies all of its policies in the secondary snapshot.
<List of CIs>	The list displays all CIs currently or previously in the view. The icons appearing to the right of the CI indicate the changes that have occurred to this CI and its policy status. Click the triangle next to the CI to display each of the changes in a separate row.

Hold the pointer over a CI in the list to display a tooltip containing the name and type of the CI.

If no icons appear after a CI, it indicates that no changes have occurred to that CI. |

Comparison Details Pane

Important information	When you select a CI in the Composite CIs pane or the Topology pane, the tabs that contain data for that CI are marked with an asterisk (*).

User interface elements are described below:

UI Elements (A-Z)	Description
Changed Attributes tab	The left pane displays the CI name and change type icon. For composite CIs, the component CIs with changed attributes are displayed.

The right pane displays the names and the primary and secondary snapshot attribute values for the CI selected in the left pane. |
| **Changed Outgoing Relationships tab** | The left pane displays the CIs to which the selected CI is related by an outgoing relationship. Click the arrow to expand each entry and display the relationships of the component CIs. For each relationship, the relationship type is displayed and an icon indicates the relevant type of change.

The right pane displays the source, target, and direction for the relationship selected in the left pane. |
| **Policy Details tab** | In the **Policy List pane**, the following data is displayed for each policy rule:

- the policy rule name
- the rule status in the primary snapshot (Status)
- the rule status in the secondary snapshot (Previous Status) |

UI Elements (A-Z)	Description
	• the related CI
	The **Details pane** displays the details for the policy rule selected in the Policy List pane, including the rule name, description, type, and validation dates.

CI Details Dialog Box

This dialog box enables you to view details of a selected CI.

To access	Click **Show Composite CI Details** ▤ or double-click a CI in the Composite CIs pane or Topology pane.

User interface elements are described below:

UI Elements (A-Z)	Description
⧃	Click **Show Only Differences** to display only those attributes where the value differs between the two states displayed.
⧂	In the Attributes tab, click **Next Difference** to jump to the next component CI in the list.
▤	In the Attributes tab, toggle between displaying all attributes for the selected CI and displaying only the managed attributes.
⧸	Indicates a difference between the value in the two states displayed.
Attributes tab	The left pane displays the CI name. For composite CIs, you can expand a CI entry to display the individual component CIs. The right pane displays the attribute names and values for this CI. The attribute values of the two compared snapshots are displayed.
Incoming Relationships tab	Displays all the relationships of the selected CI in the incoming direction. For composite CIs, you can expand a CI entry to display the individual component CIs. When you select one of the component CIs, the Internal Relationship Path Details pane at the bottom of the dialog box displays more detailed information about the relationship.
Outgoing Relationships tab	Displays all the relationships of the selected CI in the outgoing direction. For composite CIs, you can expand a CI entry to display the individual component CIs. When you select one of the component CIs, the Internal Relationship Path Details pane at the bottom of the dialog box displays more detailed information about the relationship.

Policy Details Dialog Box

This dialog box enables you to display detailed information on CI policy breaches for baseline policy rules.

To access	Click **Show Policy Details in Snapshot** 🖼 in the Policy Details tab of the Comparison Details pane. You can select either **Show Policy Details in Snapshot** or **Show Policy Details in Previous Snapshot**.
Important information	The Policy Details dialog box is only relevant when a CI with a baseline policy is selected. Click the small arrow next to the icon and select the dialog box displaying policy details for either of the selected snapshots.

User interface elements are described below:

UI Elements (A-Z)	Description
🔍	Toggle between displaying all attributes and only those with breaches, for the selected CI.
🔍	Jump to the next breach in the list.
<Left pane>	Displays the CI names and their respective baselines. For composite CIs, click the arrow to expand it and display the component CIs. For each CI for which there is a baseline value, an icon indicates whether it is in breach of the policy or not. **Note:** A CI is considered in breach of a policy if at least one of its attributes breaches the policy or if it does not match a CI in the baseline.
<Right pane>	Displays the attribute names and values, as well as the baseline values, for the CI selected in the left pane. For attributes with baseline values, an icon indicates whether or not the selected CI is in breach of the policy with reference to that attribute.

Select Snapshot to View Dialog Box

This dialog box enables you to select two snapshots to compare.

To access	Click one of the snapshot selection boxes from the toolbar.
Important information	Select a snapshot in the first selection box and then select another snapshot in the second selection box. A comparison of the two snapshots is displayed.
Relevant tasks	"Compare Snapshots" (on page 121)

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

UI Elements (A-Z)	Description
<Calendar>	Select a date in the calendar.
<List of snapshots>	The list includes all snapshots taken of the selected view on the selected date.
Authorized By	Displays the name of the user who authorized the snapshots.
	Use the drop-down list to filter the list to display only snapshots that were authorized by a selected user.
	The user "Internal Process" may appear in the **Created by** field. This means that the authorization was caused by an internal Configuration Manager process (not a user), and occurred during one of the following occasions:
	● the first time a view was managed and some CIs were authorized.
	● when a user added policies.
	● when a user performed authorization on a different view that shares some CIs with the selected view.
	Note: This field appears only for snapshots of the authorized state.
Change Details	A brief description of the snapshot.
Comments	Notes regarding the snapshot.
Creation Time	The time that the snapshot was taken.

Sort CIs Dialog Box

This dialog box enables you to sort the CI list in the Composite CIs pane.

To access	Click the **Sort Composite CIs** button from the toolbar in the Composite CIs pane.
Important information	After sorting the CIs, click the **Refresh** button for the change to take effect.

User interface elements are described below:

UI Elements (A-Z)	Description
	Move all the fields from the Available Sort Fields pane to the Selected Sort Fields pane.
	Move the selected field from the Available Sort Fields pane to the Selected Sort Fields pane.
	Remove the selected field from the Selected Sort Fields pane.

UI Elements (A-Z)	Description
✖	Remove all the fields from the Selected Sort Fields pane.
⬆ ⬇	Move a selected field up or down within the Selected Sort Fields list.
⬇ ⬆	For each selected field, select **Ascending** or **Descending** for the sort direction.
Available Sort Fields	All the available fields by which to sort the CIs.
Selected Sort Fields	The selected fields by which to sort the CIs. The sort order follows the order of the list.

Topology Page

This page displays the topology map in a large format.

To access	Click the **Show Topology Map in Full Screen** button 🖥 from the Topology pane toolbar.

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

UI Elements (A-Z)	Description
⚖	Click the small arrow next to the **Highlight Topology Nodes** button to open the menu. Select the display mode for the map: ● Highlight <Primary Snapshot> ● Highlight <Secondary Snapshot> ● Highlight Both
<Topology pane toolbar buttons>	The toolbar buttons from the Topology pane are also available in the View Topology dialog box. For details, see "Topology Pane" (on page 150).

Chapter 17

Configuration Explorer

This chapter includes:

Configuration Explorer Overview

The Configuration Explorer module enables you to survey the current status of your IT environment in either the actual or authorized state. It also enables you to display a saved snapshot of a managed view in the actual or authorized state. You can view CI and policy information for the view and check if the view's policies are satisfied or in breach.

The CIs of the view are listed in the Composite CIs pane and a topology map of the view is displayed in the Topology pane. You can specify the layout of the topology map, including the option to organize the CIs in the map by layer or classification. Also note that only the composite CIs of the view appear in the topology map, however, you can drill down to the component CIs using the CI Details dialog box. This makes the topology map much simpler and easier to read.

The CIs for which policies are defined have icons indicating the CI's policy status. Details of any policy breaches of the view's CIs are displayed in the Policy Details pane.

For details on the Configuration Explorer user interface, see "Configuration Explorer User Interface" (on page 138).

> **Note:**
>
> - You can only select views on which you have View Read permission.
>
> - If you have exceeded your licensed capacity of managed composite CIs, a warning notification is displayed. Contact your HP sales representative to purchase a license.

Impact Analysis

Impact analysis calculates the effects of an automation on CIs. It uses the CI and relationship information from HP Universal CMDB.

You can view the impact analysis calculation results for an automation in the Automation Analysis > Impact - <State> pane. This pane displays the business and system CIs that are affected by the automation. This includes general information about the affected business or system CIs and an indication of the severity of the impact of the automation. For details, see "Automation Analysis > Impact - <State> Pane" (on page 142).

The impact severity level of a CI is determined by the following rules:

- A triggered CI is automatically set to **Critical**.

- An impacted CI takes the severity level of the CI to which it is directly connected.

- An impacted CI gets a severity level that is one lower than the severity level of the CI to which it is indirectly connected. For example, if a business CI is indirectly connected to a CI called **My_ CI**, and **My_CI** has a severity level of **Medium**, then the business CI gets a severity level of **Low**.

Automation Collisions

Automations are defined as colliding when a system or business CI is involved in more than one automation over the same period of time.

Automation collisions are calculated based on scheduling conflicts. If two or more automations share a common element, and their scheduled start and stop times overlap, these automations are considered to be colliding.
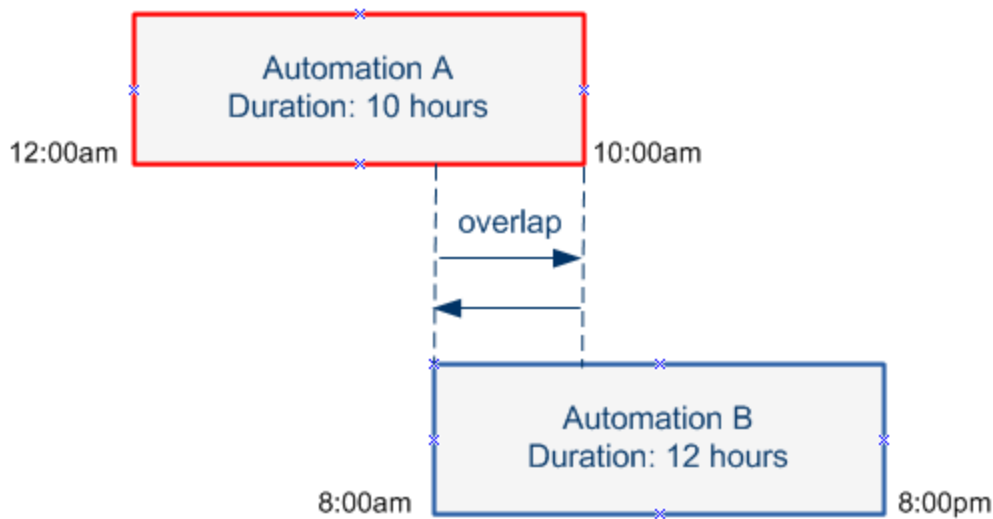
Two automations taking place at the same time do not necessarily have an effect on each other. Collisions occur only if they involve at least one common CI. There are two types of collisions:

- **Direct collision.** Occurs when two or more automations directly affect the same CI.

- **Indirect collision.** Occurs when one of the automations indirectly affects the same CI. For example, if an automation involves increasing the memory on Server A, Server A is directly affected. If Application B is connected to Server A, and is not directly involved in the automation, it is only indirectly affected by the automation.

Note: The collision type is determined by the highest severity level of the impacted CIs.

For information about viewing collision details, see "Automation Analysis > Collisions Pane" (on page 146).

Run a Controlled or Non-Controlled Automation

This task describes how to run a controlled or non-controlled automation.

This task includes the following steps:

- "Add a view to be managed" (on page 134)

- "Add a flow and configure the automation parameters" (on page 135)

- "Run a controlled or non-controlled automation" (on page 135)

Note: The controlled automation functionality is also referred to as automatic risk visualization.

1. **Add a view to be managed**

   In **Administration > View Management**, add a view from HP Universal CMDB, to be managed. For details, see "Add a View to be Managed" (on page 50).

2. **Add a flow and configure the automation parameters**

   In **Administration > Automation Management**, do the following:

   a. Click ![icon] to open the **Select Flow** window.

   b. In the left pane, click to expand the Flow Tree and select the HP Operations Orchestration flow that you want to run as an automation in Configuration Manager.

   c. Click **OK** to return to the Automation Management window.

   d. In the Automation Details pane, specify the CI type on which to run the automation from the **Associated CI Type** list.

   e. In the Execution Details pane, select the **Controlled Execution** check box to run the selected flow as a controlled automation. Non-controlled automations are run with no system intervention. To run a non-controlled automation, clear the **Controlled Execution** check box. By default, automations are set to run as controlled.

   For details on how to configure the other automation parameters, see "Automation Management Page" (on page 58).

3. **Run a controlled or non-controlled automation**

   a. Select **Application > Configuration Explorer**.

   b. In the Configuration Explorer toolbar, do the following:

      ○ In the **State** box, select **Actual State** or **Authorized State**.

      ○ In the **Select Snapshot** box, select **Latest**.

   c. In the Composite CIs pane, select a CI that is of the same CI type you chose in the **Managed CI Type** box in the Automation Management module, or a sub-class of it. For details, see "Automation Management Page" (on page 58).

   d. In the Composite CIs pane, click **Run Automation** ![icon] to open the Automation Execution dialog box**.**

   e. In the Automations pane, select the required automation.

   f. In the **Execution Parameters** pane, enter the required execution parameters for the automation you selected. Only the parameters with an asterisk are required.

      ○ If the automation you selected is a non-controlled automation, a **Run** button appears at the bottom of the dialog box. Click **Run** to run the automation.

         Note: A red asterisk indicates a required parameter. If you do not fill in the required value, the **Run** button is disabled.

      ○ If the automation you selected is a controlled automation, a **Next** button appears at the bottom of the dialog box. Click **Next** to open the Automation Planner page.

         Note: A red asterisk indicates a required parameter. You must fill in the required values to run the automation. If you do not fill in the required parameter(s), the **Next** button is disabled.

For details on how to define an automation as controlled or non-controlled, see "<Automation> Pane - Execution Details Area" (on page 59) in the "Automation Management Page" (on page 58).

> **Note:** The following steps are for controlled automations only.

g. In the Implementation Details pane of the Automation Planner dialog box, set the date and time for the automation using the calendar. You can select the current or a future date. The default is set to the current date and time.

h. Before running the automation, check the status of the policies in the Policies pane. If any of the policies have been breached, you need to examine whether the breach is critical to your IT environment. For example, the automation may cause server downtime. For information on the automation analysis information, see "Automation Analysis > Automation Pane" (on page 144) in the "Automation Planner Page" (on page 140).

If you find that the breach does not pose a risk, you can choose to ignore the breached policies and run the automation. The automation runs regardless of whether policies have been breached or not. For details, see the "Implementation Details Pane" (on page 141)and the "Policies Pane" (on page 141) in the "Automation Planner Page" (on page 140).

i. Click **Run** to run the automation.

○ If you ran a controlled automation, you can view the automation result details in the Controlled Automations tab. For details, see "Controlled Automations Tab" (on page 151) in the"Configuration Explorer Page" (on page 148).

○ If you ran a non-controlled automation, a window opens with the following message: `The automation has been launched. Click here to view a detailed report.` The word **here** is a link that opens HP Operations Orchestration, where you can view the automation results.

Create an RFC to Remediate a Policy Breach

This task enables you to create an RFC to change a CI that is in breach of a previously defined configuration policy. You are able to select multiple CIs, but if the selected CIs breach more than one policy, you are prompted to select the specific policy that you want to remediate, and the CIs that breach other policies are then discarded for this procedure.

1. In the Configuration Explorer module, click **Select View** to open a view that contains CIs that breach policies.

2. In the Composite CIs pane, select the CIs that breach policies by clicking the check box to the left of each CI.

3. Click **Remediate Policy** . The Select Policy Rule dialog box opens. For details, see "Select Policy Rule Dialog Box" (on page 154).

4. From the dropdown list, select the breached policy that you want to remediate.

At this point, you can select all the CIs in the view that breach the selected policy, even if you did not previously select them in the Composite CIs pane, by selecting the **Select all CIs that breach the policy** check box.

5. Click **Continue**. The **Create RFC for Policy Remediation** dialog box opens.

Enter the required information and click **Submit**. For details, see "Create RFC for Policy Remediation Dialog Box" (on page 148).

Set Folding Rules for Composite CIs

This task describes how to configure the folding rules which define the composite CIs. Composite CIs form the content of the managed views. You set the folding rules for your composite CIs in HP Universal CMDB.

> **Note:** In previous versions of Configuration Manager, folding rules were defined in Configuration Manager. If you are upgrading from a previous version, the folding rules you previously defined are automatically imported into HP Universal CMDB.

This task includes the following steps:

- "Prerequisites" (on page 137)
- "Define the calculated relationship" (on page 137)
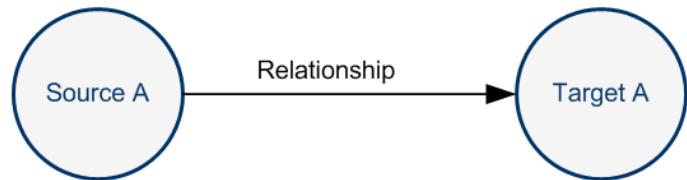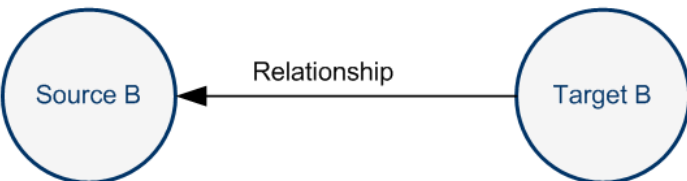
1. **Prerequisites**

   Consider how you want to display the data in composite CIs in Configuration Manager and then decide on the rules for the scope of the composite CIs.

2. **Define the calculated relationship**

   a. Select **Administration** > **UCMDB Foundation** to open HP Universal CMDB.

   b. Go to **Managers** > **Modeling** > **CI Type Manager**.

   c. Select **Calculated Relationships** from the list box in the CI Types pane. Under **Calculated Links**, select **Folding Rules (Configuration Manager)**.

   d. In the right pane, click the **Triplets** tab.

   e. In the **Triplets** tab, click ⊞ to open the Add Triplet dialog box. Define the triplet as follows:

UI Element	Description
Source	Select the required source CI type.
Target	Select the required target CI type.
Relationship	Select the required relationship connecting the source and target CI types. **Note**: The list of available relationships appears only after defining the source and target CI types.
Relationship Direction	Select the required direction. ○ ⇨ The direction is from source to target. ○ ⇦ The direction is from target to source. The direction of the relationship determines which is the

UI Element	Description
	composite CI and which is the component CI.

○ When the relationship's arrow is pointing to the target, the source query node is the composite CI and the target query node is the component CI:

Composite CI   **Component CI**

Source A —— Relationship ——▶ Target A

○ When the relationship's arrow is pointing to the source, the target query node is the composite CI and the source query node is the component CI:

Component CI   **Composite CI**

Source B ◀—— Relationship —— Target B

f. Click **OK** to save your changes.

After saving the changes, Configuration Manager receives notification of the change and recalculates the relevant views.

For more information about the Add Triplet dialog box, see the HP Universal CMDB documentation.

Configuration Explorer User Interface

This section includes (in alphabetical order):

Automation Execution Dialog Box

This dialog box enables you to run a controlled or non-controlled automation.

To access	Select **Application** > **Configuration Explorer**. In the Composite CIs pane, select the required CI and click **Run Automation** ▷ .
Important information	• To enable the **Run Automation** ▷ button, ensure that: ▪ You select **Actual State** or **Authorized State** from the toolbar. ▪ There is a managed automation mapped to a CI type in the Automation Management module that is the same as the CI type of the selected CI in the Composite CIs pane. For details, see "Automation Management Page" (on page 58). • Only users with Automation Execution permission are able to run an automation.
Relevant tasks	"Run a Controlled or Non-Controlled Automation" (on page 134)
See also	• "Automation Policy Management" (on page 70) • "System Operation Automation" (on page 19)

Automation Execution Page

This page enables you to select the automation you want to run.

User interface elements are described below:

UI Elements (A-Z)	Description
Automation Details	**Name**. The name of the automation as defined in **Administration** > **Automation Management**. **Flow UUID**. The HP Operations Orchestration instance name that uniquely identifies the HP Operations Orchestration instance being used by Configuration Manager. **Flow Path**. The full path and original name of the flow in HP Operations Orchestration. **Description**. The description of the automation as defined in **Administration** > **Automation Management**.

UI Elements (A-Z)	Description
Automations	Displays a list of automations you can run. The automations appear after they are imported from **Administration > Automation Management**. For details, see "Import a flow from HP Operations Orchestration" (on page 57). The automations that appear are relevant to the CI type you chose in the Composite CIs pane in the Configuration Explorer page.
Execution Parameters	The execution parameters needed to run the flow. Only required fields, as indicated by a red asterisk, are mandatory. **Note:**Configuration Manager does not allow you to run an automation whose required execution parameters values have not been configured. • If you do not configure the required parameters when running a non-controlled automation, the **Run** button is disabled. • If you do not configure the required parameters when running a controlled automation, the **Next** button is disabled.
Execution Type	Displays whether the automation was configured as controlled or not controlled in **Administration** > **Automation Management**.
Next/Run	• This button appears as **Next** for a controlled automation. Click this button to take you to the Automation Planner. • This button appears as **Run** for a non-controlled flow. This button is disabled if the required fields have not been filled in. If you ran a non-controlled automation, a window opens with the following message: `The automation is running. Click here to view a detailed report`. The word **here** is a link that opens HP Operations Orchestration, with the report of the automation result.

Automation Planner Page

User interface elements are described below:

Important information	This page is only available only when you are running a controlled automation. It contains the following panes: • "Implementation Details Pane" (on page 141) • "Policies Pane" (on page 141) • "Automation Analysis > Impact - <State> Pane" (on page 142) • "Automation Analysis > Automation Pane" (on page 144) • "Automation Analysis > Collisions Pane" (on page 146)

Implementation Details Pane

This pane enables you to set the date and time for the planned start of the automation.

User interface elements are described below:

UI Elements (A-Z)	Description
Expected End Time	The estimated time at which the automation process is expected to end.
	Hold the pointer over the expected end time to display a tooltip showing the expected duration time of the automation process. The first time the automation is run, the duration is 10 minutes.
	After the automation has been run for the first time, Configuration Manager updates the duration time by calculating the average time each automation took, and adding a safety buffer.
Flow Properties	Displays the automation parameters.
	Note: If you delete the required execution parameters, the **OK** button is disabled.
Planned Start Time	Use the calendar to set the date and time you want the automation to start running. You can use the default, which is the current time, or choose a future date to reschedule the automation execution to run at a later time.
	If you choose a future date, Configuration Manager recalculates all the automation analysis and policy information in the Automation Planner page.

Policies Pane

This pane enables you to view the status of the policies defined in the Automation Policies module.

See also	"Configuration Policy Management" (on page 61)

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

UI Elements (A-Z)	Description
◀ ▶	Enables you to toggle between hiding/displaying the policy details. Hold the pointer over the policy name and click ▶ to display the policy information, as defined in **Administration** > **Policies** > **Automation Policies**. For details, see "Automation Policies Page" (on page 73).
	• **Description.** The policy description.
	• **Associated Views.** The view(s) assigned to the policy.
	• **Associated CI Type.** The CI type with which the policy is associated.

UI Elements (A-Z)	Description
	Restriction. The conditions defined for the policy. **Type of condition.** The options are **Automation Related** or **CI Related**. **Condition.** The automation/CI conditions defined for this policy. **Automation Analysis.** The condition value defined for that restriction. The policy is breached only if the automation complies with all of the conditions defined for this policy. Click ◀ to hide the policy details.
<List of automation policies >	Display the list of the automation policies defined in the Automation Policies module. Each policy is determined to be either in-breach or not breached. 🛡 notes a situation in which the automation fulfills all of the conditions defined for this policy. 🛡 Denotes a situation in which the automation does not fulfill all of the conditions defined for this policy. You can choose to either ignore the breached policies if you find that the breach does not pose a risk to your IT environment and run the automation despite the breach, or decide not to run the automation if the breach is critical. In addition, you can choose to reschedule the automation to run at a later time. For example, if a breached policy defines that an automation whose elapsed time since the last execution is greater than a month causes a breach, you might decide that this does not pose a risk, as opposed to a breach which causes server downtime. **Note:**Configuration Manager enables you to run the automation even if there are automation policies that are breached.

Automation Analysis > Impact - <State> Pane

This pane describes how to view the impact analysis calculation results for an automation. It displays the business and system CIs that are affected by the automation. This includes general information about the affected business or system CIs and an indication of the severity of the impact of the automation.

Important information	The title of the pane indicates whether analysis calculates the effects of the automation on CIs from the **Actual** or **Authorized** state of the view. The default is **Actual**. To select the state by which you want to manage your view, go to **System** > **Settings** > **Application Management** > **Impact**.

See also	• "Configuration Policy Management" (on page 61)
	• "Impact Analysis" (on page 133)
	• "Data Control - Actual and Authorized States" (on page 17)

User interface elements are described below:

UI Elements (A-Z)	Description
Highest Business Criticality	Displays the CIs having the highest business criticality level of the CIs impacted by the automation.
	The Business Criticality attribute is defined in HP Universal CMDB, in which levels of importance are assigned to your business CIs. Each business CI can be assigned an importance level between 1 and 10.
	The business criticality level of a CI in HP Universal CMDB is mapped as follows:
	• 0-2 in HP Universal CMDB ---> **Low** in Configuration Manager
	• 3-5 in HP Universal CMDB ---> **Medium** in Configuration Manager
	• 6-8 in HP Universal CMDB ---> **High** in Configuration Manager
	• 9-10 in HP Universal CMDB ---> **Critical** in Configuration Manager
	The following icons indicate the business criticality levels:
	![1] Critical
	![2] High
	![3] Medium
	![4] Low
	Click the drill down arrow ![arrow] to display a table that contains a list of the CIs that have the highest business criticality level. The table includes the **CI name**, **CI type**, **impact severity** level, and **business criticality** level of each CI in the table.
	A tooltip indicating the impact severity and business criticality levels of the CI is visible when you hold your pointer over the severity and criticality icons.
	Click this arrow ![arrow] to hide the table.
Total Business CIs	Displays the total number of business CIs impacted by the automation.
	Click the drill down arrow ![arrow] to display a table that contains a list of the impacted business CIs. The table includes the **CI name**, **CI type**, **impact severity** level, and **business criticality** level of each CI in the table.

UI Elements (A-Z)	Description
	For information on the icons that indicate the impact severity levels, see **Worst Impact Severity** in this table. A tooltip indicating the impact severity and business criticality levels of the CI is visible when you hold your pointer over the severity and criticality icons. Click this arrow ⊖ to hide the table.
Total System CIs	Displays the total number of system CIs that were impacted by the automation. Click the drill down arrow ⊕ to display a table that contains a list of the impacted CIs. The table includes the **CI name**, **CI type**, and **impact severity** level of each CI in the table. A tooltip indicating the impact severity level of the CI is visible when you hold your pointer over the severity icon. Click this arrow ⊖ to hide the table.
Worst Impact Severity	Displays the CIs that have the highest impact severity level of the business CIs that have been impacted. The following icons indicate the following impact severity levels: ⬥ Critical ▽ High ⚠ Medium ❗ Low 🟩 Very Low Click the drill down arrow ⊕ to display a table that contains a list of the business CIs that have the highest impact severity level. The table includes the **CI name**, **CI type**, **impact severity** level, and **business criticality** level of each CI in the table. A tooltip indicating the impact severity and business criticality levels of the CI is visible when you hold your pointer over the severity and criticality icons. Click this arrow ⊖ to hide the table.

Automation Analysis > Automation Pane

This pane provides general information regarding previous automation runs.

Important information	Statistics are calculated for controlled and non-controlled automation runs, but only the statistics for controlled executions are displayed in the Automation Analysis > Automation pane.
See also	"Configuration Policy Management" (on page 61)

User interface elements are described below:

UI Elements (A-Z)	Description
Causes Configuration Change	Specifies whether the automation causes a change to the CI in HP Universal CMDB.
Causes Downtime	Specifies whether or not the managed automation causes the CI to become unavailable during the execution.
Execution Ratio	Displays the percentages of successful and failed runs for this automation. The success ratio is displayed in green. The failure percentage is displayed in red.
Expected Duration	The estimated time duration of the automation process. The first time the automation is run, the expected duration is 10 minutes. After the automation has been run for the first time, Configuration Manager updates the duration time by calculating the average time each automation took, and adding a safety buffer.
Last Execution	The date and time, or just date, on which the last automation execution ran. • If the automation ran in the last 48 hours, it displays both the date and the time. • If it ran more than 48 hours before the current time, it only displays the date.
Number of Executions	The number of times the automation has run.
Risk Evaluation	The level of risk in the managed automation. Valid values are: • Unknown • None • Low • Medium • High
Successful Consecutive Executions	The number of consecutive times the automation has run successfully.

Automation Analysis > Collisions Pane

This pane displays the details of the factors causing the automation collision.

Relevant tasks	"Run a Controlled or Non-Controlled Automation" (on page 134)
See also	• "Automation Collisions" (on page 133)
	• "Requests for Change" (on page 22)

UI Elements	Description
✴ **<Collision exists>** ✴ **<Collision does not exist>**	Indicates whether or not the automation is colliding with another automation/RFC. A collision occurs when a common CI is impacted by more than one automation/RFC running over the same period of time. The collision can be caused due to an automation that is: • Colliding with other automations currently running or scheduled to run in Configuration Manager. or • Colliding with an RFC that is currently being implemented or scheduled to be implemented in HP Service Manager.
Total Collisions on CIs	Displays all the commonly affected business/system CIs that are involved in collisions. Click the drill down arrow ⊙ to display a table that contains a list of the CIs involved in collisions. The table includes the **CI name**, **CI type**, **collision type**. The following icons indicate the collision types: ✴ **Direct collision**. The business/system CI is directly affected by the collision. ✴ **Indirect collision.** The business/system CI is indirectly affected by the collision. A tooltip indicating the collision type of the CI is visible when you hold your mouse over the collision type icons. **Note regarding system CIs only:** Only top level (composite) CIs are displayed. If colliding automations cause collisions on more than one CI, the severity is determined by the collision with the highest severity. Click the arrow ⊙ to hide the table.
Total Colliding Activities	• **Colliding Automations**

UI Elements	Description
	Indicates the total number of colliding automations running or scheduled to run in Configuration Manager.
	• **Colliding RFCs**
	Configuration Manager imports from HP Universal CMDB requests for change (RFCs) that were opened in HP Service Manager. Every RFC is associated with at least one CI.
	Colliding RFCs refer to the total number of automations currently running or scheduled to run in Configuration Manager that collide with RFCs that are currently running or scheduled to run in HP Service Manager.
	For information on how Configuration Manager retrieves RFCs, see "Requests for Change" (on page 22).

CI Details Dialog Box

This dialog box enables you to view details of a selected CI.

To access	Click **Show Composite CI Details** 📖 or double-click a CI in the Composite CIs pane or Topology pane.

User interface elements are described below:

UI Elements (A-Z)	Description
🔍	Click **Next Difference** to jump to the next component CI in the list.
📖	In the Attributes tab, toggle between displaying all attributes for the selected CI and displaying only the managed attributes.
Attributes tab	The left pane displays the CI name. For composite CIs, you can expand a CI entry to display the individual component CIs.
	The right pane displays the attribute names and values for this CI.
Incoming Relationships tab	Displays all the relationships of the selected CI in the incoming direction.
	For composite CIs, you can expand a CI entry to display the individual component CIs. When you select one of the component CIs, the Internal Relationship Path Details pane at the bottom of the dialog box displays more detailed information about the relationship.
Outgoing Relationships tab	Displays all the relationships of the selected CI in the outgoing direction.
	For composite CIs, you can expand a CI entry to display the individual component CIs. When you select one of the component CIs, the Internal Relationship Path Details pane at the bottom of the dialog box displays more detailed information about the relationship.

Create RFC for Policy Remediation Dialog Box

This dialog box enables you to create an RFC to remediate a CI that breaches a configuration policy, which will be validated in Service Manager.

To access	Click Remediate Policy 🔊 Remediate Policy in the Composite CIs pane of the Configuration Explorer page and select a policy.
Important information	Enter a title and select the relevant information for the RFC that you are creating to remediate the policy. By clicking Submit, you are creating an RFC and manually relating it to the selected CIs.

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

UI Elements (A-Z)	Description
Affected CIs	The list of changes that were marked for authorization in the Composite CIs pane.
Category	Select a category from the displayed list of category values (set on the System Settings page). For details, see "RFC Creation" (on page 177).
Description	The list of CIs and the required actions that should be performed for each CI. If a single CI has been selected, an automatically generated description is displayed.
Impact	Select the widest range of impact that the change will have from the displayed list of values (set on the System Settings page). For details, see "RFC Creation" (on page 177).
Requested end date	The date by which the RFC should be executed.
Risk assessment	Select the level of risk for the changed CI from the displayed list of values (set on the System Settings page). For details, see "RFC Creation" (on page 177).
Service	The list of services that are available to the CI.
Title	Enter a title for the RFC, for example, a short summary of the requested changes.
Urgency	Select the level of urgency for the change in the CI from the displayed list of values (set on the System Settings page). For details, see "RFC Creation" (on page 177).

Configuration Explorer Page

This page enables you to display a snapshot of a view in the actual or authorized state.

To access	Select **Application > Configuration Explorer**.

Important information	The Configuration Explorer page includes the following:
	• **Composite CIs pane.** Displays a list of CIs in the view with icons indicating the policy status for each CI.
	• **Topology pane.** Displays a topology map of the CIs in the view with icons indicating the policy status for each CI. Each node in the topology map displays the name, CI type, and management status, as well as the policy status and whether or not related RFCs exist for the selected CI.
	Note: In inventory mode, the Topology pane is called **Related CIs**.
	• **Policy Details tab.** Displays details of policy breaches and satisfaction for the selected CI.
	• **Controlled Automations tab**. Displays the currently running controlled automations, as well as automations that are scheduled to run at a future date.
	• **Filter pane.** In inventory mode, the Filter pane enables you to filter the composite CI list.
	The Composite CIs pane and the Topology pane are linked; when you select a CI in one pane, it is automatically selected in the other.

User interface elements are described below:

UI Elements (A-Z)	Description
	Click **Select View** to select a different view to open on the Configuration Explorer page.
	Click to change the display to inventory mode.
	Click to change the display to topology mode.
Actual State ▼ Actual State Authorized State	Select the state of the view to display: • **Actual State.** Displays all CIs and relationships in the actual state of the view. • **Authorized State.** Displays all CIs and relationships in the authorized state of the view.
	Click **Select Snapshot** to open the Select Snapshot to View dialog box which enables you to select a saved snapshot of the view.
	Click **Edit Comments** to edit the comments for the selected snapshot.
	Click **Export Report** to choose a format for the Policy Analysis report data. The available data format options are: • **Excel.** The table data is formatted as an .XLS (Excel) file that can be displayed in a spreadsheet.

UI Elements (A-Z)	Description
	• **PDF.** The table data is exported in PDF format. • **CSV.** The table data is formatted as a comma-separated values (CSV) text file that can be displayed in a spreadsheet.
🔄	Click **Refresh** to refresh the CI list.

Composite CIs Pane

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

UI Elements (A-Z)	Description
↓	**Sort Composite CIs**. Opens the Sort CIs dialog box which enables you to sort the CI list by different sort fields.
📋	**Show Composite CI Details**. Opens the CI Details dialog box, which displays the managed attributes of the selected CI.
Launch ▾	Click ▾ to select an external application to open in the context of a selected CI or view. You must specify the URLs that will open on the System Settings page. For details, see "UI Integrations" (on page 180).
▷	**Run Automation.** Enables you to run a controlled or non-controlled automation. Opens the Automation Execution dialog box.
▼	Indicates that the CI is currently in breach of at least one policy.
●	Indicates that the CI is currently satisfying all of its policies.
<List of CIs>	The list displays all CIs currently or previously in the view. Hold the pointer over a CI in the list to display a tooltip containing the name and type of the CI. If no icons appear next to a CI, it indicates that no policies are defined for that CI.

Topology Pane

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

UI Elements (A-Z)	Description
🔍	Click **Show Topology Overview Display** to toggle between displaying and hiding the Topology Overview Display.
☰	Click **Layers Layout** to display the topology map in a layout consisting of CIs grouped according to their layer.
⊞	Click **Hierarchical Layers Layout** to display the topology map in a layout consisting of CIs grouped according to their

UI Elements (A-Z)	Description
	layer arranged in a hierarchy.
	Click **Classification Layout** to display the topology map in a layout consisting of CIs grouped according to their classification.
	Click **Circular Layout** to display the topology map in a circular layout.
	Use the zoom control bar to zoom in or out of the topology map.
	Click **Fit to Window** to resize the topology map to the size of the Topology Pane.
	Click **Show Topology in Full Screen** to display the topology map in the View Topology box.
<Topology Overview Display>	The Topology Overview Display appears in the upper right corner of the pane. It indicates which portion of the topology map is displayed in the Topology pane. This is useful for large views or when you zoom in on a view.

Policy Details Pane

User interface elements are described below:

UI Elements (A-Z)	Description
	Click to open the Policy Details dialog box. **Note:** This button is only active when a baseline rule is selected in the policy list.
Details pane	Displays the details for the policy rule selected in the Policy List pane, including the rule name, description, type, and validation dates.
Policy List pane	Displays all the policy rules defined for the selected CI. For each rule, the name, , status in the selected state, and related CIs are displayed.

Controlled Automations Tab

This tab displays the currently running controlled automations, as well as automations that are scheduled to run at a future date.

User interface elements are described below:

UI Elements (A-Z)	Description
Recent Automations pane	Displays all automations that ran in the last 24 hours. The automation disappears from the pane 24 hours after it started running. The following data is available for each automation:

UI Elements (A-Z)	Description

	• **The name of the automation.** The automation name is a link to the flow execution report in HP Operations Orchestration.
	
	• **Start time and duration of the automation.**
	
	    ▪ The date and time at which the automation started to run and the duration if the automation has finished running.
	
	    ▪ The date and time at which the automation started to run and the estimated duration time if the automation is still running.
	
	• **The icons that indicate the automation status:**
	
	Unknown. Indicates that either the status data is not available or the status indicated in HP Operations Orchestration is not recognized by the system. This icon appears when you first run an automation and is replaced once the updated status arrives from HP Operations Orchestration.
	
	Running. The automation is running.
	
	Successful. The automation has run successfully.
	
	Successful with Problems. The automation has run successfully but with problems.
	
	Failed. The automation has failed.
	
	Canceled. The automation has been canceled.
	
	Error. Indicates a general error. For example, if you run an automation without having a connection to HP Operations Orchestration.

Planned Automations pane	Displays all the automations that are scheduled to run at a future date. After the automation starts to run, the automation appears in the Recent Automations pane. The following data is available for each automation: • **The name of the automation.** • **Start time and estimated duration of the automation.** • **Cancel**. Click to cancel the planned automation. After the automation is canceled, a ⊘ icon appears. The automation appears in the Recent Automations pane at the scheduled start time and disappears from the pane 24 hours after it was scheduled to start running.

Filter Pane

User interface elements are described below:

UI Elements (A-Z)	Description
Changed CIs	Filter the CIs by their change status. When you select **Yes**, only CIs with changes appear in the view display. When you select **No**, only CIs without changes appear in the view display. **Available in:** State Management module.
CI Name	Filter the CIs by CI name. Only the selected CIs appear in the view display. Enter a CI name manually in the value box or click **More...** to open a dialog box which enables you to select CIs from a list.
CI Type	Filter the CIs by CI type. Only CIs of the selected CI types appear in the view display. Click **More...** to open a dialog box that enables you to select available CI types from a list.
Has RFCs	Filter according to whether or not the selected CI has an RFC associated with it. **Available in:** State Management module.
Managed Status	Filter the CIs by their management status. Only CIs of the selected status appear in the view display. Select **Managed** or **Not Managed**.
Policy Name	Filter the CIs by the names of their policies. Only CIs affected by the selected policies appear in the view display. Click **More...** to open a dialog box that enables you to select available policies from a list.
Policies Status	Filter the CIs by their policy status. Only CIs of the selected status appear in the view display. If no policy is specified in the Policy Name field, the selected policy status condition will apply to all policies that are assigned to the CIs in the view; otherwise, the selected policy status condition will be applied only to the policies that were specified by name. Select **In-breach** or **Satisfied**.
Related RFCs	Filter the CIs by specific RFC titles. Click **More...** to open a dialog box that enables you to select related RFC values from a list. **Available in:** State Management module.

Policy Details Dialog Box

This dialog box enables you to display detailed information on CI policy breaches for baseline policy rules.

To access	Click **Show PolicyDetails in Snapshot** 🔲 in the Policy Details tab of the bottom pane.
Important information	The Policy Details dialog box is only relevant when a CI with a baseline policy is selected. The dialog box displays policy details for the selected state (actual or authorized).

User interface elements are described below:

UI Elements (A-Z)	Description
🔍	Toggle between displaying all attributes and only those with breaches, for the selected CI.
🔍	Jump to the next breach in the list.
<Left pane>	Displays the CI names and their respective baselines. For composite CIs, click the arrow to expand it and display the component CIs. For each CI for which there is a baseline value, an icon indicates whether it is in breach of the policy or not. **Note:** A CI is considered in breach of a policy if at least one of its attributes breaches the policy or if it does not match a CI in the baseline.
<Right pane>	Displays the attribute names and values, as well as the baseline values, for the CI selected in the left pane. For attributes with baseline values, an icon indicates whether or not the selected CI is in breach of the policy with reference to that attribute.

Select Policy Rule Dialog Box

This dialog box enables you to select a breached policy for remediation.

To access	Click **Remediate Policy** [Remediate Policy] in the Composite CIs pane.
Relevant tasks	"Create an RFC to Remediate a Policy Breach" (on page 136)

User interface elements are described below:

UI Elements (A-Z)	Description
Policy Name	Select the name of the breached policy to be remediated from the dropdown list. CIs that do not breach the selected policy will be discarded.

UI Elements (A-Z)	Description
Select all CIs that breach the policy	Select the check box to include all CIs that breach the selected policy, even if they were not selected in the Composite CIs pane.

Select Snapshot to View Dialog Box

This dialog box enables you to select a snapshot to display.

To access	Click one of the snapshot selection boxes from the toolbar.

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

UI Elements (A-Z)	Description
<Calendar>	Select a date in the calendar.
<List of snapshots>	The list includes all snapshots taken of the selected view on the selected date.
Authorized By	Displays the name of the user who authorized the snapshots.
	Use the drop-down list to filter the list to display only snapshots that were authorized by a selected user.
	The user "Internal Process" may appear in the **Created by** field. This means that the authorization was caused by an internal Configuration Manager process (not a user), and occurred during one of the following occasions:
	• the first time a view was managed and some CIs were authorized.
	• when a user added policies.
	• when a user performed authorization on a different view that shares some CIs with the selected view.
	Note: This field appears only for snapshots of the authorized state.
Change Details	A brief description of the snapshot.
Comments	Notes regarding the snapshot.
Creation Time	The time that the snapshot was taken.

Sort CIs Dialog Box

This dialog box enables you to sort the CI list in the Composite CIs pane.

To access	Click the **Sort CIs** button ![icon] from the toolbar in the Composite CIs pane.
Important information	After sorting the CIs, click the **Refresh** button for the change to take effect.

User interface elements are described below:

UI Elements (A-Z)	Description
⮆	Move all the fields from the Available Sort Fields pane to the Selected Sort Fields pane.
→	Move the selected field from the Available Sort Fields pane to the Selected Sort Fields pane.
✖	Remove the selected field from the Selected Sort Fields pane.
✖	Remove all the fields from the Selected Sort Fields pane.
↑ ↓	Move a selected field up or down within the Selected Sort Fields list.
⬇ ⬆	For each selected field, select **Ascending** or **Descending** for the sort direction.
Available Sort Fields	All the available fields by which to sort the CIs.
Selected Sort Fields	The selected fields by which to sort the CIs. The sort order follows the order of the list.

Topology Page

This page displays the topology map in a large format.

To access	Click the **Show Topology Map in Full Screen** button 🖵 from the Topology pane toolbar.

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

UI Elements (A-Z)	Description
<Topology pane toolbar buttons>	The toolbar buttons from the Topology pane are also available in the View Topology dialog box. For details, see "Topology Pane" (on page 150).

System Setup

Chapter 19

System Settings

This chapter includes:

System Settings Overview

The System Settings module enables you to define the configuration settings needed to set up your environment.

A configuration set contains the properties defined for the system. You can create any number of configuration sets and then select one with which to run your system. Configuration Manager maintains a history of all the configuration sets created. For details on how to display a list of all the existing configuration set versions, see "Open Configuration Set Dialog Box" (on page 170).

Configuration Manager enables you to move configuration sets from one system to another. You can:

- Export a configuration set to your local directory.

- Import a configuration set from your local directory to another system. For example, from a test to a production environment.

A new configuration set is initially saved as a draft. A draft is a configuration set that has not yet been activated. A draft can be edited only until it is first activated. The new configuration properties are only applied to Configuration Manager after a draft is activated. For details on how to activate a draft, see "Save and Apply Configuration Changes" (on page 161).

You cannot edit a configuration set after it has been activated. You must rather create a new draft. You can create a new draft based on an existing configuration set and save it with a new name.

For details on how to create a draft, see "Save as Draft Dialog Box" (on page 171).

Configuration Manager calculates the validation of the configuration setting and identifies the problems in the configuration - for example, a field with a missing value. If a problem is found, Configuration Manager displays a description of the problem, a link to the configuration pane in which the problem was found, and an icon that indicates the severity of the problem.

Configuration validation is performed after the following operations:

- Saving a configuration set

- Opening a configuration set

- Importing a configuration set

For details on handling problems, see "Problems Pane" (on page 182).

> **Note:** You must have System Settings permission to make changes to the Configuration Manager setup.

User Management Configuration Overview

Configuration Manager provides the ability to connect to an organizational LDAP for Authentication/Users/Groups management, or to use an out-of-the-box user repository supported by a relational database.

The following are the providers of user management information:

- The **Authentication provider** contains login information for authenticating users.

- The **User provider** contains definitions for users.

- The **Group provider** contains definitions for groups.

You can configure the providers to work with the management information stored in either the out-of-the-box user repository provided by Configuration Manager (a **Shared** data repository), or in an external LDAP server (an **External** data repository). Any user information that you modify in Configuration Manager is updated in the appropriate provider repository.

In a common application implementation, **User**, **Group** and **Authentication** providers are all directed to the same data repository that can be either **External** or **Shared**.

The shared data repository is managed by Configuration Manager in the relational database.

For details on how to edit **System > Settings > User Management** configurations, see "System Settings Page" (on page 172).

Save and Apply Configuration Changes

This task describes how to save configuration changes and then apply the new configuration properties to Configuration Manager.

1. Select **System** > **Settings** and make the required configuration changes.

2. In the left pane, click the **Save current editable configuration set** button 💾 to open the Save as Draft dialog box and save the modified configuration set as a draft. A draft is a configuration set that has not yet been activated. After a draft is activated, the new configuration properties are applied to Configuration Manager.

3. In the **Draft name** box, enter the name of the draft and click **Save**.

4. In the left pane, click **Open Configuration Set** 📂 to open the Open Configuration Set dialog box.

5. Click the **Drafts** button to display only the existing drafts.

6. Select the required draft and click **Open**. The name of the currently selected configuration set appears at the top of the left pane.

7. In the left pane, click the **Activate current configuration set** button ⚙ to activate the selected draft and apply the new configuration properties to Configuration Manager.

Set Up Configuration Manager to Use the Out-of-the-Box Shared User Repository

This task describes how to configure Configuration Manager to use a **Shared** user repository.

1. In **System > Settings > User Management Configuration**, set the following to **Shared**:

   - Authentication Provider

   - Users Provider

   - Groups Provider

2. Select all the **Users <attribute> Mandatory** options to indicate that they are mandatory for input when creating a user.

3. In **System > Settings > User Management Configuration > Shared User Repository > Personalization**, ensure that all the attribute values are selected.

Set Up Configuration Manager to Use an External User Repository (LDAP)

Configuration Manager works directly with the LDAP server for user authentication. The **external-ldap.properties** file contains the LDAP customization metadata file.

This task describes how to configure Configuration Manager to use LDAP for user authentication.

This task includes the following steps:

1. **Configure the LDAP connection**

   a. Download and install the Apache Directory Studio LDAP browser from http://directory.apache.org/studio.

   b. Open the LDAP browser and click the **New Connection** button from the Connections tab located at the bottom left hand side of the application window.

   c. Enter the LDAP host name (**ldapHost**) and port number (**ldapPort**)

   d. Select the appropriate encryption level (**enableSSL**).

   e. Click **Check Network Parameters**.

   f. Click **Next**.

   g. Select one of the following authentication methods:

      ○ No Authentication useAdministrator=false

      ○ Simple Authentication useAdministrator=true

   h. Click **Finish**. The connection is automatically tested.

i. In the event that SSL is selected, the Certificate trust window may open. If applicable, select **View Certificate**. Ensure that the certificate appears in the java key store used by Configuration Manager.

2. **Configure the LDAP server connection properties in Configuration Manager**

   In this step, you configure the connection between Configuration Manager and the LDAP server.

   a. In **System > Settings > User Management Configuration> External User Repository**, define the following user login information:

Attribute Name	Description
enableSSL	If this parameter is set to **true**, SSL is used to connect to the LDAP server.
ldapHost	Host name of the machine running the LDAP server.
ldapPort	Port number of the LDAP server. If **enableSSL** is set to **true**, then this port is used for the SSL connection.
useAdministrator	If set to **true**, the LDAP connection is created with the Administrator's user name and password provided in the **Administrator username** and **password** parameters. Otherwise the LDAP connection is created without a user name or password. **Note:** The v2 guest user is not supported by the library.

   b. In **System > Settings > User Management Configuration> External User Repository > Ldap Credentials Configuration**, define the following user login information:

Attribute Name	Description
Administrator User	Administrator's user name used for creating the initial LDAP connection. **Note:** This parameter is only required if the **useAdministrator** option is set to `true`.
Administrator Password	Administrator's password used for creating the initial LDAP connection. **Note:** This parameter is only required if the **useAdministrator** option is set to `true`.
Using Credentials	If selected, the LDAP connection is created with the Administrator's user name and password provided in the **Administrator User** and **Administrator password** parameters. Otherwise the LDAP connection is created without a user name or password. **Note:** The v2 guest user is not supported by the library.

3. **Configure the LDAP server login**

   In this step, you specify whether to log on to Configuration Manager anonymously or to use a user name and password.

   To log on anonymously:

   a. In **System > Settings > User Management Configuration> External User Repository**, set **useAdministrator** to **false**.

   b. In **System > Settings > User Management Configuration> External User Repository > Ldap Credentials Configuration**, make sure the **Using Credentials** check box is not selected.

   To log on with a user name and password:

   a. In **System > Settings > User Management Configuration> External User Repository**, set **useAdministrator** to **true**.

   b. In **System > Settings > User Management Configuration> External User Repository > Ldap Credentials Configuration**, make sure the **Using Credentials** check box is selected.

   c. When logging on, enter the user name and password in the relevant fields.

4. **Map user objects in Configuration Manager to user objects in LDAP**

   In this step, you define the LDAP vendor, or customized implementation-specific objects, that represent the user objects in Configuration Manager.

   > **Note:** More than one comma-separated object class is supported.

   To map the user configuration properties in Configuration Manager to the LDAP server configuration properties:

   a. Select a user from the LDAP browser tree menu.

   b. Review the user information appearing in the main window of the LDAP browser.

   c. In **System > Settings > User Management Configuration> External User Repository**, assign LDAP property names for the following attributes:

   > **Note:** The attribute names that appear may vary depending on the LDAP tool you are using.

Attribute Name	Description
Mandatory Attributes	
usersLoginName Attribute	Contains the user name with which the user logs on to LDAP.
usersObjectClass	The LDAP object class used for storing the user information.

Attribute Name	Description
Optional Attributes	
usersDisplayName Attribute	The attribute used to store the user's LDAP display name.
usersEmailAttribute	The attribute used to store the user's LDAP email address.
usersFirstName Attribute	The attribute used to store the user's LDAP first name.
usersLastName Attribute	The attribute used to store the user's LDAP last name.
usersPreferred LanguageAttribute	The attribute that displays the user interface in a specific language.
usersPreferredLocationAttribute	The attribute that stores the preferred location for the specified language.

Using External Read/Write User and Group Providers

All user attributes that require update functionality via the UI should be mapped to the LDAP attributes that are not part of the user RDN (relative distinguished name).

To extend the LDAP schema to include additional attributes, update the **external-ldap.properties** configuration file.

5. **Configure the group search properties**

In this step, you define the search properties used on LDAP groups. There are two sets of properties: The first for regular (non-root) groups, and the second for root groups. Only groups that are returned by a root group search are displayed at the root level in **System** > **User Management** > **User Management** window > **Users and Groups** tab.

This enables the user to narrow the group search to the relevant groups only. To display only a limited number of groups, restrict the root group search criteria appropriately. The same search criteria for both root and non-root groups can also be used. This configuration is recommended when the overall number of groups is small.

> **Note:** You must first validate the user search configuration using the LDAP browser. Then, only after the validation succeeds, update Configuration Manager with the corresponding property definitions.

a. Select the **Search** folder in the LDAP browser tree menu.

b. Right-click the **Search** folder. From the **New** menu, select **New Search**.

c. Define the following properties in their corresponding input fields:

Attribute Name	Description
groupsBase	The distinguished name (DN) used to search for groups in the LDAP directory.
groupsFilter	Indicates what instances should be returned from the LDAP group search.
groupsScope	The scope for the group search is as follows: ○ **SCOPE_SUB.** Searches the subtree under the group's base. ○ **SCOPE_ONE.** Searches only the first level of the subtree under the group's base. ○ **SCOPE_BASE.** Searches only the root of the subtree. **Note:** The group's base is defined in the groupsBase attribute.
rootGroupsBase	The distinguished name (DN) used to search for root groups in the LDAP directory.
rootGroupsScope	The scope for the rootgroup search is as follows: ○ **SCOPE_SUB.** Searches the subtree under the group's base. ○ **SCOPE_ONE.** Searches only the first level of the subtree under the group's base. ○ **SCOPE_BASE.** Searches only the root of the subtree. **Note:** The group's base is defined in the rootGroupsBase attribute.

    d. Click **Search**.

    e. Once the search is validated, update the properties you defined above in **System > Settings > User Management Configuration> External User Repository**.

6. **Map group objects in Configuration Manager to group objects in LDAP**

   In this step, you define the LDAP vendor or custom implementation-specific objects representing static groups.

   > **Note:** More than one comma-separated object class is supported. You can define the appropriate corresponding comma-separated attribute names.

   To map the group configuration properties in Configuration Manager to those of the LDAP server:

   a. Select a group from the LDAP browser tree menu.

   b. Review the group information appearing in the main window of the LDAP browser.

   c. In **System > Settings > User Management Configuration> External User Repository**, assign LDAP property names for the following attributes:

> **Note:** The attribute names that appear may vary depending on the LDAP tool you are
> using.

Attribute Name	Description
Mandatory Attributes	
groupsMembers Attribute	Used to store the group's member information. This multi-value attribute contains the full distinguished names (DNs) of static group members.
groupsObjectClass	LDAP object class used for storing the static group's information.

Attribute Name	Description
Optional Attributes	
dynamicGroupsClass	LDAP object class used for storing the dynamic group's information.
dynamicGroups MemberAttribute	Attribute used to store the search URL that defines the members of the dynamic group.
dynamicGroups NameAttribute	Attribute used to store the dynamic group's unique name. This attribute is usually the same as **dynamicGoupsDisplayNameAttribute**.
dynamicGroups DescriptionAttribute	Attribute used to store the dynamic group's description.
dynamicGroupsDisplay NameAttribute	Attribute used to store the dynamic group's display name. This attribute is usually the same as **dynamicGoupsNameAttribute**.
enableDynamicGroups	If the value of this attribute is true, Configuration Manager is instructed to search for users in dynamic groups as well as in static groups. **Note:** Searching for members of very large dynamic groups may be time consuming.
groupsNameAttribute	Used to store the group's unique name. This attribute is usually the same as **groupsDisplayNameAttribute**.
groupsDisplayName Attribute	Used to store the group's display name. This attribute is usually the same as **groupsNameAttribute**.
groupsDescription Attribute	Used to store the group's description.

External Read/Write User and Group Providers

All attributes that require an update via UI should be mapped to the LDAP attributes that are not part of the group RDN (relative distinguished name).

Extend the LDAP schema to add an additional attribute, and map the relevant group attribute to the new LDAP attribute in the **external-ldap.properties** configuration file.

7. **Configure support for nested groups**

Define whether Configuration Manager takes LDAP server group hierarchy information into account when configuring a user search in the LDAP directory.

Attribute Name	Description
enableNestedGroups	Configuration Manager is instructed to search recursively for all users in subgroups. **Note:** Instances are returned by the groups' search filter.
maximalAllowedGroups HierarchyDepth	Defines the maximum allowed depth for the groups hierarchy. No groups are searched beneath this level. If you define a negative value, an unlimited depth is allowed. **Note:** This parameter is relevant only if the **enableNestedGroups** parameter is set to true.

8. **Configure advanced attributes for the Configuration Manager - LDAP connection**

You can define advanced configuration attributes to fine-tune the Configuration Manager - LDAP connection.

Attribute Name	Description
ldapVersion	**LDAP protocol version.** Possible values are: ■ **3 -** Default ■ **2 -** For old versions of LDAP
baseDistinguishName Delimiter	**Base DN delimiter.** Symbol used in configuration when using multiple base DNs for users or groups or a user search. **Note:** This symbol must not appear as part of the base DN used in this configuration. If it appears in the base DN, change the default value to another symbol.
scopeDelimiter	**Scope delimiter.** Symbol used in configuration when using multiple scopes for a user or group search. **Note:** This symbol must not appear as part of the scope name used in this configuration. If it appears in the scope name, change the default value to another symbol.
attributeValues	Symbol used in configuration when using multiple attribute names

Attribute Name	Description
Delimiter	of users or groups.
	Note: This symbol must not appear as part of attributes used in this configuration. If it appears in attribute names, then change the default value to anther symbol.

9. **Configure Configuration Manager to Use an LDAP Server**

   a. In **System > Settings > User Management Configuration**, set the following to **External**:

      ○ Users Provider

      ○ Groups Provider

   b. In **System > Settings > User Management Configuration> Enablement**, ensure that following attributes are **selected**:

      ○ Group Readable

      ○ Group Role Assignable Read

      ○ Group Role Assignable Write

      ○ Principle Readable

      ○ Principle Role Assignable Read

      ○ Principle Role Assignable Write

      ○ Role Creatable

      ○ Role Deletable

      ○ Role Readable

      ○ Role Updatable

   c. In **System > Settings > User Management Configuration> Enablement**, ensure that the following attributes are **not selected**:

      ○ Group Creatable

      ○ Group Updatable

      ○ Group Deletable

      ○ Principle Creatable

      ○ Principle Deletable

      ○ Principle Updatable

      > **Note:** Any additional attributes that exist in the external user repository should be set to read-only.

   d. In **System > Settings > User Management Configuration> Personalization**, ensure that following attributes are **selected**.

- ○ User Display Name Attribute Readable

- ○ User First Name Attribute Readable

- ○ User Last Name Attribute Readable

- ○ User Login Name Attribute Readable

e. Save and activate your configuration changes. For details, see "Save and Apply Configuration Changes" (on page 161).

f. Restart Configuration Manager.

10. **Set the Authentication Provider to External**

a. Go to **System > User Management** and define the login permissions for users or groups. For details, see "Set Up Configuration Manager Users and Permissions" (on page 186).

b. In **System > Settings > User Management Configuration**, set Authentication Provider to **External**.

c. Save and activate your configuration changes. For details, see "Save and Apply Configuration Changes" (on page 161).

d. Restart Configuration Manager.

System Settings User Interface

This section includes (in alphabetical order):

Open Configuration Set Dialog Box

This dialog box displays a list of all the existing configuration set versions.

To access	Select **System** > **Settings** > **Open Configuration Set** 📂 in the left pane.
Important Information	You cannot change the name of any of the configuration set versions.
Relevant tasks	"Save and Apply Configuration Changes" (on page 161)

User interface elements are described below:

UI Elements (A-Z)	Description
📄	**Currently active configuration set.** Denotes the currently activated configuration set.
📄	**Previously active configuration set.** Denotes a previously active configuration set.

UI Elements (A-Z)	Description
🖼	**Draft.** Denotes a draft, that is, a configuration set that has not yet been activated. The changes in the draft are only applied and saved in Configuration Manager's history after the draft is activated.
Activated	Displays the currently activated configuration set.
All	Displays all existing configuration sets and drafts.
Drafts	Displays all existing drafts.
Last Activated By	The name of the user who last activated the draft/configuration set.
Last Activated On	The time and date on which the draft/configuration set was last activated.
Last Modified By	The name of the user who last modified the draft/configuration set.
Last Modified On	The time and date on which the draft/configuration set was last modified.

Save as Draft Dialog Box

This dialog box enables you to create a draft of a new configuration set. A draft is a configuration set that has not yet been activated. It can be edited only until it is first activated. When the draft is activated, the configuration properties are applied to Configuration Manager. For details on how to activate a draft, see "Save and Apply Configuration Changes" (on page 161).

To access	Select **System** > **Settings** > **Save the current editable configuration set** 🖼 in the left pane.
Important Information	You cannot change the name of an existing draft.
Relevant tasks	"Save and Apply Configuration Changes" (on page 161)

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

UI Elements (A-Z)	Description
<List of existing drafts>	Displays a list of all existing drafts.
Draft name	Enter a unique name for the new draft.
Last Modified By	The name of the user who last modified the draft.
Last Modified on	The time and date on which the draft was last modified.
Name	The name of the draft.

System Settings Page

This page enables you to modify the configuration settings for Configuration Manager.

To access	Select **System > Settings**.
Important information	An asterisk appears next to the category name in the left pane when a change is made to one of the settings in that category.
Relevant tasks	• "Set Up Configuration Manager to Use the Out-of-the-Box Shared User Repository" (on page 161) • "Set Up Configuration Manager to Use an External User Repository (LDAP)" (on page 162)

Left Pane

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

UI Elements (A-Z)	Description
💾	**Save the current editable configuration set.** Enables you to create a draft of a new configuration set. A draft is a configuration set that has not yet been activated and can still be edited. This button is enabled when you make a change to the currently activated configuration set. For details, see "Save as Draft Dialog Box" (on page 171).
📂	**Open configuration set.** Displays a list of all the existing configuration set versions. For details, see "Open Configuration Set Dialog Box" (on page 170).
📥	**Import configuration set.** Enables you to import a configuration set from your local directory to the same or another system. Opens the Import Configuration Set dialog box. **Important:** Configuration Manager enables you to import a partially exported configuration set from the same version of Configuration Manager, to an existing configuration set. • You can override an existing configuration set with all its properties. • You cannot delete an existing configuration that is missing from the imported configuration set. For example: 1. Select **System** > **Settings** > **Application Manager** > **Topology Presentation** > **Topology Layout**. 2. In the Layers pane, remove the field **Software** and its associated color. 3. Export that configuration set.

UI Elements (A-Z)	Description
	4. Then import that configuration set into another draft where the field **Software** exists. The field **Software** is not deleted from the draft by the import operation. It only overrides other existing entries or adds new entries to that draft. To delete the entry, you must do it manually.
	Note:
	● If you import a configuration set while working with a configuration set that has not yet been activated (a draft), the imported configuration set overrides the current draft.
	● If you want to import a partially exported configuration set while working with a configuration set that has already been activated, you must provide a different draft name in the Draft name box in the Import Configuration Set dialog box to create a draft.
	Limitations:
	● A configuration set that has been exported through the Configuration Manager user interface, cannot be imported using the Export Configuration Set utility. For details, see "Export Configuration Set" (on page 215).
	● A configuration set that has been exported using the Export Configuration Set utility, can be imported through the Configuration Manager user interface. In this case, the current active configuration set is completely overridden, including deleting configuration items that are missing from the imported set.
	The current active configuration set is also overridden when importing the configuration set from the **vanilla.zip** file located in the **<Configuration Manager installation directory>\conf** folder.
	Export configuration set to a zip file. Enables you to Export a whole configuration set or part of a configuration set to your local directory as a zip file. Opens the Export Configuration Set dialog box.
	Select the configuration settings you want to export from the tree in the Export Configuration Set tree dialog box.
	Activate current configuration set. Applies the configuration properties in the draft/configuration set to Configuration Manager and becomes the active configuration set.
	Note: Only one configuration set is considered active at any given point of time.
	Add configuration to configuration set. This button is only enabled when you select a node on the configuration tree that allows you to add a child configuration.
	Remove configuration from configuration set. This button is only

UI Elements (A-Z)	Description
	enabled when you select a node on the configuration tree that allows you to delete a child configuration.
📁	Denotes a configuration category. **Note:** The arrow next to each category enables you to expand or collapse the lower-level categories.
<Configuration tree>	Contains the configuration categories. The configuration fields for each selected node in the tree are displayed in the right pane. Select a file from the tree to open in the right pane.

The following categories contain configuration settings:

Automation Impact

To access	Select **System > Settings > Application Management > Automation Impact**.

User interface elements are described below:

Setting	Description
Impact analysis state	Enables you to determine whether impact analysis calculates the effects of the automation on CIs from the actual or authorized state of a view. The options are: • Actual (default) • Authorized For details, see "Automation Analysis > Impact - <State> Pane" (on page 142).

Change Management

To access	Select **System > Settings > Integrations > Change Management**.

User interface elements are described below:

Setting	Description
Change Management integration enabled	Select the check box to: • enable direct integration with the change management system to create an RFC. • log authorization actions for the relevant RFC in the change management system. These can either be rollback RFCs in the State Management module or

Setting	Description
	policy remediation RFCs in the Configuration Explorer module.

Daily View Refresh Settings

To access	Select **System > Settings > Application Management > Jobs Synchronization > Offline Analysis and Authorization > Daily View Refresh Settings**.

User interface elements are described below:

Setting	Description
Start time (0-23)	Select the hour at which offline analysis will be run.

Fetched RFCs Criteria

To access	Select **System > Settings > Application Management > RFC > Fetched RFCs Criteria**.

User interface elements are described below:

Setting	Description
RFC maximum days	The maximum number of days that can pass since the RFC was scheduled to end.
RFC CI Types	Configure the CI types for which RFCs can be defined: • [icon] Click to add a new CI type. • [icon] Click to delete the selected CI type. You can edit the CI type names manually.
RFC Filters	Filter the RFCs analyzed and displayed by property names and values: • [icon] Click to add a new property. • [icon] Click to delete the selected property. You can edit the property names and values manually. **Note:** Every row represents a different property and the values should appear in a comma-separated list. Each property listed must have one of the specified values for the RFC to be displayed.

Mail Settings

To access	Select **System > Settings > Application Management > Mail Settings**.

User interface elements are described below:

Setting	Description
Enable mail	Select this option to enable the sending of emails. For details, see "User Preferences Dialog Box" (on page 208).
Hour at which to send emails (0-23)	The time at which the notifications are sent by the system.
SMTP server address	The outgoing address of the SMTP server.
SMTP port	The SMTP server port number.
SMTP sender email address	The email address of the SMTP server from which the notifications are sent.
SMTP requires authentication	Specify whether or not the SMTP server requires authentication.
SMTP username	The username of the SMTP server. Only relevant when **SMTP requires authorization** is selected.
SMTP password	The password of the SMTP server. Only relevant when **SMTP requires authorization** is selected.
Configuration Manager full URL	The full URL of the Configuration Manager server. When this option is specified and detailed information is requested, links to Configuration Manager are inserted into the emails.
Administrator's email address	The email address of the system administrator. This is used to send emails (about problems that occur when trying to send the notifications) directly to the system administrator.

Offline Analysis and Authorization Tasks

To access	Select **System > Settings > Application Management > Jobs Synchronization > Offline Analysis and Authorization > Offline Analysis and Authorization Tasks**.

User interface elements are described below:

Setting	Description
Offline Analysis repeat interval	Define a base interval in seconds. The other task settings are configured using multiples of this interval.
Delete candidate repeat cycles	The number of cycles between successive runs of candidate deletion.
Automatic authorization repeat cycles	The number of cycles between successive runs of automatic authorization.

Offline Purging

To access	Select **System > Settings > Application Management > Jobs Synchronization > Offline Purging**.

User interface elements are described below:

Setting	Description
Offline purge repeat interval	The number of days between successive purges of policy history and statistics history.
Keep history	The number of days to store environment snapshots, and policy and statistics history. Policy and statistics history older than this limit is deleted at the next purge.

Operations Orchestration

To access	Select **System > Settings > Integrations > Operations Orchestration > Operations Orchestration**.

User interface elements are described below:

Setting	Description
Cyclic Interval	Defines the interval (measured in seconds) which determines how often the HP Operations Orchestration server is checked for automation flow results. **Default:** 60 seconds
Host	The host name of the machine on which the HP Operations Orchestration server is installed.
Password	The password required to connect to the HP Operations Orchestration server.
Port	The port used by the HP Operations Orchestration server.
User name	The user name required to connect to the HP Operations Orchestration server.
Version	The HP Operations Orchestration version.

RFC Creation

To access	Select **System > Settings > Application Management > RFC > RFC Creation**.

User interface elements are described below:

Setting	Description
Category	The possible range of categories that can be used when creating an RFC. **Relevant to:** planned RFCs
Default assignment group	Set the default assignment group that will be used when creating an RFC.
Default change coordinator	Set the default change coordinator value that will be used when creating an RFC.
Default service name	Set the default service name value that will be used when creating an RFC.
Impact	The possible range of impact of the RFC.
Urgency	The urgency of the RFC.
Risk Assessment	The assessment of the risk of the RFC. **Relevant to:** planned RFCs
Reason for change	The reason why the RFC is required.

RFC Display

To access	Select **System > Settings > Application Management > RFC > RFC Display**.

User interface elements are described below:

Setting	Description
RFC Properties	Configure the RFC properties for display: • Click to add a new property. • Click to delete the selected property. You can edit the property names manually.

Service Manager

To access	Select **System > Settings > Integrations > Change Management > Service Manager**.

User interface elements are described below:

Setting	Description
Connection strategy	Select HTTP.

Setting	Description
Host Name	The host name of the Service Manager server.
Port Number	The port number of the Service Manager server.
User Name	The Service Manager user name.
Password	The Service Manager password.
Date format	Select the date format to be used. The selected date format must be supported by the change management system such as Service Manager.

Topology Layout

To access	Select **System > Settings > Application Management > Topology Presentation > Topology Layout**.

User interface elements are described below:

Setting	Description
Layers	Configure the layers of the topology map display: • Click to add a new layer. • Click to delete the selected layer. You can edit the name, display name, level number, and color of the layers.
Classifications	Configure the classifications of the topology map display: • Click to add a new classification. • Click to delete the selected classification. You can edit the name, display name, and color of the classifications.
Layout Exceptions	Configure exceptions to the classifications defined above: • Click to add a new exception. • Click to delete the selected exception. For the selected CI type, if the specified attribute has the specified value, the specified classification applies.

Topology Limitations

To access	Select **System > Settings > Application Management > Topology Limitations**.

User interface elements are described below:

Setting	Description
Graphical layout limit	The maximum number of composite CIs that can be displayed in the topology map.

UCMDB Foundation

To access	Select **System > Settings > Integrations > UCMDB Foundation > UCMDB Foundation**.

User interface elements are described below:

Setting	Description
Connection strategy	The method of connection to UCMDB.
Customer	The UCMDB customer name.
UCMDB server name	The name of the UCMDB server.
UCMDB server port	The port number of the UCMDB server.
UCMDB access URL	The URL for accessing UCMDB.
User name	The UCMDB user name.
Password	The UCMDB user password.

UI Integrations

To access	Select **System > Settings > Integrations > UI Integrations**.

User interface elements are described below:

Setting	Description
Configured UIs	Configure the URLs that can be opened: • Click to add a new URL to the list. For each URL that you add to the list, specify a display name and the URL that will be opened. A URL can contain one of the following variables: ▪ **${ucmdbId}**—The ID of the composite CI (as it appears in UCMDB) ▪ **${ucmdbName}**—The name of the composite CI (as it appears in UCMDB) ▪ **${ucmdbViewName}**—The name of the view (as it appears in UCMDB)

Setting	Description
	• **${ucmdbcmViewId}**—The ID of the view (Configuration Manager view ID) • Click to delete the selected URL.

User Management Configuration

This page defines the connection information for the LDAP server. Any user information that you modify in Configuration Manager is updated in the appropriate server.

To access	Select **System > Settings > User Management Configuration**.

User interface elements are described below:

UI Elements	Description
<type> Provider	The repository containing the Authentication, Groups, Personalization, and Users providers. For each provider, specify the LDAP server, **EXTERNAL** or **SHARED**. For a description of the providers, see "User Management Configuration Overview" (on page 160).
User <attribute> Attribute Mandatory	Indicates whether the attribute is mandatory for user creation.

Value Suggestions

To access	Select **System > Settings > Application Management > Jobs Synchronization > Offline Analysis and Authorization > Value Suggestions**.

User interface elements are described below:

Setting	Description
Max count to save	The maximum number of suggested attribute values stored in the database.
Max count to show	The maximum number of suggested attribute values displayed.
Attribute Values statistics repeat cycles	The number of cycles between successive recalculations of attribute value statistics.

External/Shared User Repository

This page contains the connection properties for the LDAP servers.

To access	Select **System > Settings > User Management Configuration > External/Shared User Repository**.

User interface elements are described below:

UI Elements	Description
External Repository	The properties in this page come from the LDAP properties table for the repository called External or Shared.
External - Enablement	Defines the access information for the roles, users, groups, and principles. Specify whether the groups, roles, and principles can be created, deleted, readable, and assigned.
External/Shared - Personalization	Specifies which user attributes are readable or editable. The settings in this page define which information is editable and which is read-only when you create or modify users in the User Management module. For user interface details, see "User Management Tab" (on page 195).

Problems Pane

User interface elements are described below:

UI Elements (A-Z)	Description
⚠	Indicates the severity level of the problem. The following icons appear: ❌ . Indicates that there is an error in the configuration settings. In this case, Configuration Manager does not allow you to activate the configuration set and the **Activate current configuration set** ⚙ button is disabled. ⚠ . Indicates a warning. In this case, Configuration Manager allows you to activate the configuration set. - ℹ️ . Provides an informative message. In this case, Configuration Manager allows you to activate the configuration set.
Code	Contains a link to the pane containing the problem. When you click the link, the relevant node in the configuration tree is selected and its relevant pane appears on the right.
Description	Contains a description of the problem.

Troubleshooting and Limitations

This section describes known LDAP issues.

Problem: Communication with LDAP server cannot be established. Communication exception appears in logs.

Solution: Check the LDAP host, port, and SSL mode settings:

1. Check that LDAP host and port are configured correctly:
   Select **System > Settings > User Management Configuration > External User Repository** and check the **ldapHost** and **ldapPort** settings.

2. Check that SSL mode is configured correctly. Check with your organizational LDAP

administrator whether the administrator user is required for LDAP connection. Select **System > Settings > User Management Configuration > External User Repository** and check the **enableSSL** setting.

3. Check that appropriate server certificate is installed. Run the following command:

```
<Configuration Manager installation directory>\java\windows\
x86_64\bin\keytool.exe -list -trustcacerts [-alias
<certificate alias>] -keystore <Configuration Manager
installation directory>\java\windows\x86_64\lib\security\cacerts
-storepass changeit
```

4. Check with your organizational LDAP administrator whether the administrator is required for LDAP connection. Select **System > Settings > User Management Configuration > External User Repository** and check the following settings: **useAdministrator, ldapAdministrator**, and **ldapAdministratorPassword**.

Problem: No groups appear on the users or groups management screen. No exception appears in the logs.

Solution: Check the following:

1. Check that Users and Groups search filters are configured correctly: Select **System > Settings > User Management Configuration > External User Repository** and modify the following properties: **usersBase, usersScope, usersFilter, groupsBase, groupsScope, groupsFilter, rootGroupsBase, rootGroupsScope**, and **rootGroupsFilter**.

2. Open the LDAP client browser and look for the users under the base DNS.

Problem: UI is too slow.

Solution: Usually this is because too many groups or users are configured in your LDAP. Configure the base DNS and filters to reduce the number of groups to the relevant subset as follows:

1. Select **System > Settings > User Management Configuration > External User Repository**.

2. Modify the following settings: **usersBase, usersScope, usersFilter, groupsBase, groupsScope, groupsFilter, rootGroupsBase, rootGroupsScope**, and **rootGroupsFilter**.

Problem: Some known users do not appear on the groups or users management screen.

Solution: The Users and Groups management screen shows only users that belong to some group. Put the users into the appropriate groups in LDAP in order to see them on the main screen.

Problem: Login takes a long time.

Solution: The user may belong to too many groups. You can optimize the startup time by changing the groups search filter, so it will return fewer groups as follows:

1. Select **System > Settings > User Management Configuration > External User Repository**.

2. Modify the **groupsFilter** setting.

Chapter 20

User Management

This chapter includes:

User Management Overview

HP Universal CMDB Configuration Manager enables you to define users, groups, and their associated roles, permissions, and environments. A user's role defines which actions they can perform in Configuration Manager on which instances of data. For example, if none of the user's roles have permission for View Management, the View Management module is not available.

> **Note:** You must have User Management permission to work with this module.

Environments

In Configuration Manager, an environment is defined as one or more Managed View instances. For more information about Configuration Manager managed views, see "View Management" (on page 46). Once you define environments, you attach the environment to a permission. For example, you can specify that the Configuration Manager Administrator has View Read and View Write permissions in all environments, while the DB Manager has View Read and View Write permissions only in an environment defined as local_lab_databases.

Roles and Permissions

Each role is associated with permissions. Permissions define which Configuration Manager actions the role can perform according to their responsibilities in the organization. For example, you could create a role that enables its users to create views, or you could create a role that enables its users to edit configuration policies but not to create views. For details, see "Permissions and Permission Sets" (on page 188).

Out of the box, Configuration Manager provides a single role (System Administrator), which includes all permissions.

Users and Groups

Every user has a list of roles that define their permissions for working with Configuration Manager. When you assign a role, that user will only have access to specific portions of the program and specific environments that are relevant to their role. You can also define groups of users with the same roles or access rights. When you attach a user/group to a group, the user/group inherits all of the group's roles.

User Management Diagram

The following diagram illustrates the relationship between users, groups, roles, permissions, and environments in Configuration Manager.
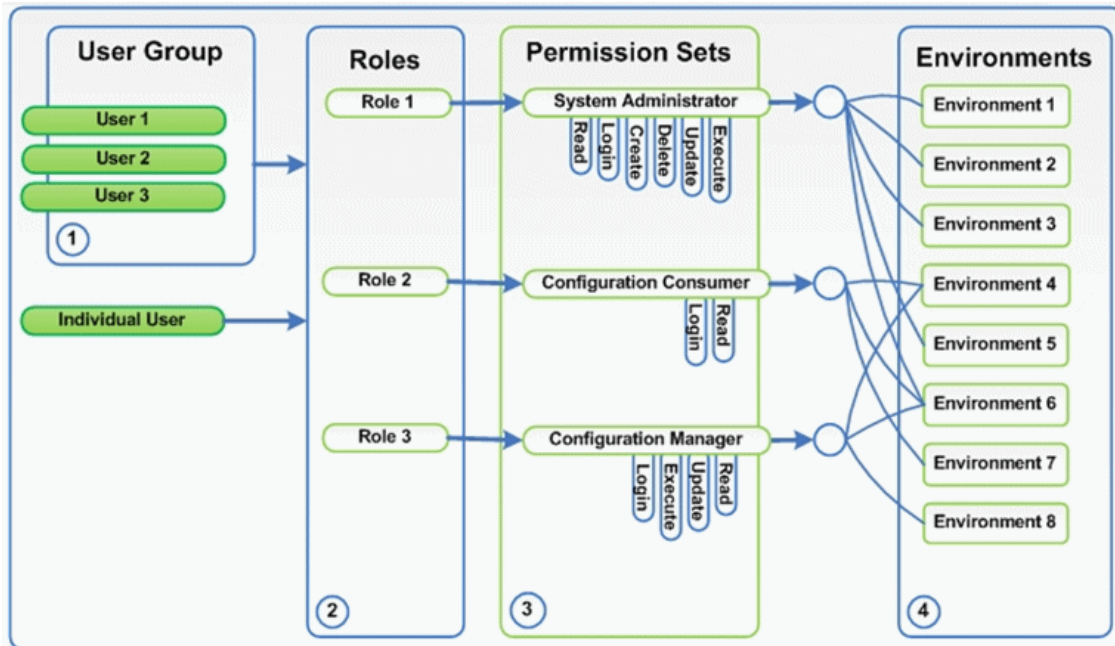
Set Up Configuration Manager Users and Permissions

This task describes the working order for defining users and permissions in Configuration Manager.

This task includes the following steps:

- "Prerequisites" (on page 186)
- "Define the environment" (on page 186)
- "Define the roles and permissions" (on page 187)
- "Define groups" (on page 187)
- "Define users" (on page 187)

1. **Prerequisites**

   Select views to manage in Configuration Manager. This will enable you to define the environments for users and permissions. For details, see "View Management" (on page 46).

2. **Define the environment**

   a. Select **System > User Management** and click the **Environment Management** tab.

   b. Select an environment type.

   c. Click the **Create Environment** button. Enter a name and description for the new environment and click **OK**.

   d. Click the **Add Instances** button in the Environment Details pane. Select an instance in the Available Instances pane and use the arrow to move it to the Selected Instances pane. When finished, click **OK**.

   For user interface details, see "Environment Management Tab" (on page 192).

3. **Define the roles and permissions**

   a. Select **System > User Management** and click the **Role Management** tab.

   b. Click the **Create Role** 📧 button. Enter a name and description for the new role.

   c. Click the **Attach Permission** ➕ button in the **Role Details** pane.

   d. Select an eligible role permission and click **Next**.

      All permissions, except for global permissions, must have an Environment assignment.

   e. Click **Finish**, or click **Commit** and **Add Another Permission** to assign additional permissions to the role.

      For user interface details, see "Role Management Tab" (on page 194) and the "Assign Permissions to Role Wizard" (on page 190).

4. **Define groups**

   > **Note:** When you create groups, the data repository must be set to read/write.

   a. Select **System > User Management** and click the **User Management** tab.

   b. Click the **Create Group** 👥 button. Enter a name and description for the new group, and click **OK**.

   c. Click the **Assign Role** button located under Roles and Permissions in the Group Details pane

   d. Click **OK**.

      For user interface details, see "User Management Tab" (on page 195).

5. **Define users**

   > **Note:** When you create users, the data repository must be set to read/write.

   a. On the Users and Groups tab, select the group to which you want to add a new user.

   b. Click the **Create User** 👤 button on the **Users and Groups** tab. Enter a name and description for the new group, and click **OK**.

   c. Enter information in all fields.

   d. Click **OK**.

      For user interface details, see "User Management Tab" (on page 195).

Specify an Email Address

This task describes how to specify an email address. This task is generally performed by a system administrator.

1. Navigate to **System > User Management**.

2. In the **Users and Groups** pane, click **+** to expand the list of Configuration Manager users.

3. Select the user for which you want to enter an email address

4. In the **User Details** area, click **Edit details**.

5. Enter your email address and password, and click **OK**.

> **Note:** Leave the password field empty if you want to use your previous password.

Specify Email Options

This task describes how to specify the time and SMTP account information for email notifications.

> **Note:** You must have System Settings permission to perform this operation.

1. Navigate to **System > Settings > Application Management > Email settings**.

2. Specify the time that the emails should be sent.

3. Provide the required SMTP account information.

4. Click 💾.

> **Note:** If requested, enter a name and click **Save**.

Permissions and Permission Sets

Permissions

There are two types of permissions in Configuration Manager:

- Static permissions – permissions that determine which modules you can access and which actions you can perform (for example, Configuration Analysis and Views Administration).

- Data level permissions – permissions that specify the actions you can perform on specific data (View Read and View Write).

The following permissions can be assigned in Configuration Manager:

Name	Description
Automation Execution	Permission to execute any automation in Configuration Manager.
Automation Management	Permission to configure automations (**Administration > Automation Management**).
Automation Policies All Views	Permission to select **All Views** when defining the scope of an automation policy (**Administration > Policies > Automation Policies**).
Automation Policies Administration	Permission to define automation policies (**Administration > Policies > Automation Policies**).
Configuration Analysis	Permission to use the Configuration Modeling and Environment Segmentation Analysis modules (**Application > Configuration**

Name	Description
	Analysis).
Configuration Policies Administration	Permission to add, edit, and delete configuration policies (**Administration > Policies > Configuration Policies**).
License Management	Permission to install licenses in Configuration Manager (**System > License**).
Login	Permission to log in to Configuration Manager. **Note:** This permission is assigned to all users.
System Settings	Permission to edit the Configuration Manager configuration (**System > Settings**).
User Management	Permission to manage users, roles, environments, and permissions (**System > User Management**).
View Read	Permission to view selected views.
View Write	Permission to view, edit, and authorize changes to selected views.
Views Administration	Permission to manage, unmanage, and edit views, as well as to view, edit, and authorize changes to all views (**Administration > View Management**).

Permission Sets

Permission sets are predefined groups of permissions that you can apply to a role, without having to select each permission individually. The following predefined permission sets are available:

Name	Description
Configuration Consumer	Includes the following permissions: ● Configuration Analysis ● Login
Configuration Contributor	Includes the following permissions: ● Automation Execution ● Automation Policies Administration ● Configuration Analysis ● Login ● View Write
Configuration Manager	Includes the following permissions: ● Automation Management ● Automation Policies All Views

Name	Description
	• Automation Policies Administration • Configuration Analysis • Login • View Write
Policies Administrator	Includes the following permissions: • Automation Policies Administration • Configuration Policies Administration • Login • View Read
System Administrator	Includes all permissions.
Views Administrator	Includes the following permissions: • Login • Views Administration

User Management User Interface

This section includes:

Assign Permissions to Role Wizard

This wizard enables you to assign permissions to the selected role.

To access	Select **System > User Management > Role Management**.Select a role and click ⊞ in the Role Details pane.
Wizard map	The Assign Permissions to Role Wizard contains: "Select a Permission or a Permission Set Page" (on page 191) > "Assign Environments to Permissions Page" (on page 191) > "Confirmation Page" (on page 192)
See also	"Permissions and Permission Sets" (on page 188)

Select a Permission or a Permission Set Page

This wizard page enables you to select the permissions to assign.

Important information	Select a permission or a permission set from the tree.
Wizard map	The "Assign Permissions to Role Wizard" (on page 190) contains: **Select a Permission or a Permission Set Page** > "Assign Environments to Permissions Page" (on page 191) > "Confirmation Page" (on page 192)
See also	"Permissions and Permission Sets" (on page 188)

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

UI Elements (A-Z)	Description
<Permissions tree>	Pre-defined permission sets and individual permissions for Configuration Manager.

Assign Environments to Permissions Page

This wizard page enables you to assign environments to permissions.

Important information	This page only appears if the permission are applicable for an environment.
Wizard map	The "Assign Permissions to Role Wizard" (on page 190) contains: "Select a Permission or a Permission Set Page" (on page 191) >**Assign Environments to Permissions Page** > "Confirmation Page" (on page 192)
See also	"Permissions and Permission Sets" (on page 188)

User interface elements are described below:

UI Elements (A-Z)	Description
→ ←	Select a permission and use the arrows to move the required environments from the Available Environments list to the Selected Environments list.
Available and Selected Environments	Each permission can be applicable for specific environments, for all environments, or not applicable to an environment.
Permission	A tree containing the permission or permission set.

Confirmation Page

This wizard page confirms the permissions assignments you have made.

Wizard map	The "Assign Permissions to Role Wizard" (on page 190) contains:
	"Select a Permission or a Permission Set Page" (on page 191) > "Assign Environments to Permissions Page" (on page 191) > **Confirmation Page**

User interface elements are described below:

UI Elements (A-Z)	Description
Environment	List of environments associated with the selected permission.
Permission	The new permissions assigned to this role.

Assign Roles Dialog Box

This dialog box enables you to assign roles to users or groups.

To access	Click the **Assign Roles** button ⊞ from the Roles and Permissions section of the Group Details pane of the User Management tab.
Important information	When users launch Configuration Manager, the actions that they can access depend on their roles and permissions.

User interface elements are described below:

UI Elements (A-Z)	Description
→ ←	Select a role from the Available Roles list and use the arrows to move the role to the Selected Roles list.
Available and Selected Roles	Each user or group can have one or more assigned roles.
Permission details	Displays read-only details about the permissions and corresponding environments for the selected role.

Environment Management Tab

This page enables you to define working environments that contain views.

To access	Select **System > User Management > Environment Management** tab.
Important information	Environments are the basis for user and role management. For each user or group, you assign permissions to perform specific actions in specific environments.

	Click **Refresh** ⟳ to refresh the display.
Relevant tasks	"Set Up Configuration Manager Users and Permissions" (on page 186)

Environments Pane

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

UI Elements (A-Z)	Description
⬚	Select an environment type and click **Create environment** to create a new environment of that type.
✖	Click **Delete environment** to delete the selected environment. **Note:** If the environment is the only environment attached to a permission and that permission is attached to any roles, deleting the environment will detach the corresponding permissions and permission sets from these roles.
<Environments Tree>	Contains the environment types and the environments defined for each type.

Environment Details Pane

When you select an environment in the Environments pane, the details appear in this pane. User interface elements are described below:

UI Elements (A-Z)	Description
➕	Click **Add instances** to add view instances to the selected environment using the Manage Instances dialog box. Each environment can have one or more assigned view instances. In the Manage Instances dialog box, select a view instance from the **Available Instances** list and use the arrows to move the instance to the **Selected Instances** list. → ← To filter the displayed list, enter a specific instance name or part of a name from the Available Instances list. **Note:** These instances are views defined in the View Management module. For more information, see "View Management" (on page 46).
⊘	Click **Remove instances** to remove the selected instance from the environment.
Edit details	Click **Edit details** to edit the selected environment name and description.

UI Elements (A-Z)	Description
Environment Description	The description of the selected environment.
Environment Name	The name of the selected environment.
Instance	List of view instances for the selected environment. The instances can be displayed either as a hierarchical tree or as a list.

Environment Type Details Pane

When you select an environment type in the Environments pane, the details appear in this pane. User interface elements are described below:

UI Elements (A-Z)	Description
Environment Description	The description of the selected environment type.
Environment Name	The name of the selected environment type.

Role Management Tab

This page enables you to define the user roles and application permissions for working with Configuration Manager.

To access	Select **System > User Management > Role Management** tab
Important information	It is recommended to define environments prior to defining roles. For details, see "Environment Management Tab" (on page 192).
	Click **Refresh** to refresh the display.
Relevant tasks	"Set Up Configuration Manager Users and Permissions" (on page 186)

Roles Pane

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

UI Elements (A-Z)	Description
	Click **Create role** to create a new role.
	Click **Delete role** to delete the selected role.
<Role list>	A list of roles currently defined in Configuration Manager. When you select a role, the details appear in the Role Details and Permissions panes.

Role Details Pane

User interface elements are described below:

UI Elements (A-Z)	Description
![plus icon]	Click **Attach permission** to select permissions to attach to the selected role. You select permissions using the "Assign Permissions to Role Wizard" (on page 190).
![pencil icon]	Click **Manage permission** to modify the selected permission. You modify permissions using the "Assign Permissions to Role Wizard" (on page 190).
![no icon]	Click **Detach permission** to remove permissions from the selected role.
Edit details	Click **Edit details** to edit the selected role name and description.
Environment	The list of environments for each permission. If the list does not fit into the environment column, use the tool-tip to view the entire list. **Not Applicable:** Used for permissions that do not require a specific environment setting. **<Environment Name>:** The permission is attached to a specific environment. **All:** The permission is applicable to all environments.
Permission	The permission sets and permissions attached to the selected role.
Role Description	The description of the selected role.
Role Name	The name of the selected role.

User Management Tab

The user management settings for Configuration Manager control the users, groups, roles, and permissions. This page enables you to configure these settings.

To access	Select **System > User Management > User Management** tab.
Important information	It is recommended to define environments and roles prior to defining users. For details, see "Environment Management Tab" (on page 192) and "Role Management Tab" (on page 194). Click **Refresh** ![refresh icon] to refresh the display.
Relevant tasks	"Set Up Configuration Manager Users and Permissions" (on page 186)

Search Users Pane

User interface elements are described below:

UI Elements (A-Z)	Description
Search	Click **Search** to search for users that match the details in the Search Users section.
Search Users	The search criteria. To search for users, enter some or all of the user details: **First Name**, **Last Name**, **Login Name**, **Display Name**, **Email**.
User Name	A list of all users that match the search criteria.

Users & Groups Pane

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

UI Elements (A-Z)	Description
	Click **Create user** to create a new user under the selected group. The user will inherit the group's roles.
	Click **Create group** to create a new group under an existing group. the group will inherit the group's roles.
	Click **Add group under the root** to create a new group under the root.
	Click **Delete** to delete the selected user or group from the system.
	Click **Attach to group** to attach the selected user or group to groups. The users/groups will inherit all of the group's roles.
	Click **Detach from group** to detach the selected user or group from a group. When you detach a user/group from a group, they will no longer have the roles that they inherited from the group. **Note:** • Users that are not attached to a group will not be displayed in Configuration Manager. To find users that are not attached to a group, use the Search pane. For user interface details, see "Search Users Pane" (on page 195). • When you detach a group from a group, it moves to the "root" of the groups and users tree.
<Users and Groups list>	A tree containing all of the existing groups and users attached to those groups. **Note:** Users that are not attached to a group will not be displayed in Configuration Manager. To find users that are not attached to a group, use the Search pane. For user interface details, see "Search Users Pane" (on page 195).

Group Details Pane

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

UI Elements (A-Z)	Description
	Click **Assign role** to open the "Assign Roles Dialog Box" (on page 192) and assign a role to the selected group. For details, see "Assign Roles Dialog Box" (on page 192).
	Click **Remove role** to remove the selected role from the group.
<Roles and Permissions list>	The assigned roles and corresponding permissions and environments for the selected group.
Edit Details	Click **Edit Details** to edit the details of the selected group.
Group Description	The description of the selected group.
Group Name	The name of the selected group.

User Details Pane

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

UI Elements (A-Z)	Description
	Click **Assign role** to open the "Assign Roles Dialog Box" (on page 192) and assign a role to the selected user.
	Click **Remove role** to remove the selected role from the user.
<Roles and Permissions list>	The assigned roles and corresponding permissions and environments for the selected user.
Edit Details	Click **Edit Details** to edit the details of the selected user.
Display Name	The system display name for the selected user.
Email	The email address for the selected user. This address is used when sending system notifications.
First Name	The first name of the selected user.
Last Name	The last name of the selected user.
Login Name	The user ID of the selected user.
New/Confirm Password	Enter the user's password in the New Password field, and enter it again to confirm in the Confirm password field.
	The minimum password length is six characters and a password must conform to at least four of the following policies:
	• A minimum of one numeric character must exist in the password.
	• A minimum of one special character must exist in the password.

UI Elements (A-Z)	Description
	• A minimum of one uppercase character must exist in the password.
	• A minimum of one lowercase character must exist in the password.
	• All characters must be in Unicode.
	No spaces are allowed in a password.

Troubleshooting and Limitations

This section describes troubleshooting and limitations for User Management. Configuration Manager configuration settings for these solutions are in **System > Settings > User Management > User Management Configuration**.

Problem. The user cannot log in to Configuration Manager.

Solution. Validate the user definitions and permissions. The user login information is checked by the Authentication Provider.

1. Make sure that the correct authentication provider is configured in the **User Management Configuration** page, **Authentication Provider** (**SHARED** or **EXTERNAL**).

2. Make sure that the user has login permissions in the **conf\permissions-mode.xml** file.

Problem. Cannot create a user under a group

Solution. Validate the group settings and the user settings.

1. Make sure that the correct user provider is configured in the **User Management Configuration** page, **User Provider** (**SHARED** or **EXTERNAL**).

2. In the **User Repository > Enablement** page, enable **Principle updatable**.

Problem. Cannot update a user

Solution. Verify that the User Provider can be updated. In the **User Repository > Enablement** page, enable **Principle updatable**.

Problem. Cannot update a user field

Solution. Verify that the User Provider and the user fields can be updated:

1. In the **User Repository > Enablement** page, enable **Principle updatable**.

2. In the **User Repository > Personalization** page, verify that the fields ending in "Editable" are enabled. (For example, **User Display Name Attribute Editable**).

Problem. Cannot create a group

Solution. In the **User Repository > Personalization** page, enable **Group Creatable**.

Problem. Cannot update a group

Solution. In the **User Repository > Personalization** page, enable **Group Updatable**.

Problem. Cannot assign a role to a user

Solution. Verify the Roles Provider and the fields can be updated:

1. Make sure that the correct roles provider is configured in the **User Management Configuration** page, **Roles Provider** (**SHARED** or **EXTERNAL**).

2. In the **User Repository > Enablement** page, enable **Principle Role Assignable Write**.

Problem. Security error appears in Configuration Manager.

Solution. If the security error message indicates an issue with configuration, it should provide enough details for finding the correct configuration setting.

For example, if a security exception appears when you try to change group details, the message will indicate "group was defined non updatable." In this case, in the **User Repository > Enablement** page, enable **Group Updatable**.

Problem. Cannot update the password field when updating user information

Solution. Verify the User Provider settings.

1. Make sure that the correct user provider is configured in the **User Management Configuration** page, **User Provider** (**SHARED** or **EXTERNAL**).

2. In the **User Repository > Personalization** page, enable **User PasswordAttribute Editable**.

Chapter 21

Licensing

This chapter includes:

Licensing Overview

The advanced Configuration Analysis module features of auto-segmentation and auto-baselining are provided with an Instant-on license that is free of charge for an unlimited number of managed CIs and is valid for 60 days from the first use of Configuration Manager. Following this 60-day period, a permanent license must be purchased for the specific amount of composite CIs that are managed by Configuration Manager. When additional composite CIs will be managed, additional permanent licenses must be purchased.

The Automation Risk Visualizer provides a one-time ability to execute 500 controlled automations (or usage for 60 days, whichever comes later) free of charge. Following the first 500 free controlled automations (or 60 days), a permanent license must be purchased for the number of controlled automation executions to be analyzed with a 30-day (moving) period. You can estimate this number based on your actual usage during the previous 60 days.

Note: For all of these modules, following the initial free licenses, you may be permitted to obtain an additional 60 days of usage free (Evaluation license). For details, contact your HP sales representative.

Permanent licenses are additive, meaning that additional purchases of permanent licenses are added to your existing total capacity, and do not replace it.

When the license limit has been exceeded, the following occurs:

- During Configuration Manager usage, a warning notification is displayed. If such a message appears, you should purchase and install a license with additional capacity. Contact your HP sales representative to purchase licenses for these modules.

- When an administrator (who has Install New License permission) logs in to Configuration Manager, a popup message is displayed, and they are automatically redirected to the License module to install a new license.

Note: You must have License Management permission to install new licenses in Configuration Manager.

Install a License

This task describes how to install a new license in Configuration Manager.

1. Contact your HP sales representative to purchase a new license.

2. Select **System > License**.

3. Click to open the **Install License** dialog box.

4. Copy the entire new license key that you obtained from your HP representative and click **OK**. Make sure that you copy the license string from the .**dat** file that is attached to the email you receive with the license, and not directly from the browser window or from the text of the email.

> **Note:**
>
> - Some licenses include a few separate license keys. Install each license key separately.
>
> - Inverted commas (") may be part of the license key and should be copied as well.

If the license has already been installed or if an invalid license key is entered, an error message is displayed.

When the installation is successful, the relevant license section will be refreshed and display the status of the new license.

License User Interface

This section includes:

License Page

This page enables you to view the licenses that you have installed, and to install new licenses.

To access	Select **System > License**.
Relevant tasks	"Install a License " (on page 201)

User interface elements are described below:

UI Element (A-Z)	Description
Install	Opens the Install License dialog box, where you enter the license key for a new license.
Actual Usage	The number of composite CIs managed or automations run for the selected license. This number is updated once per day.
Capacity	The number of composite CIs that can be managed or automations that can be run for the selected license.
Description	A description of the license.
Expiration Date	The expiration date and time of the license.
License Type	Specifies the type of the selected license, which can be Instant-on, Evaluation, or Permanent.
Name	The license name, which can be either **Controlled Automations per Month** or **Advanced Configuration Analysis**.
Status	Specifies the status of the selected license (for example, whether or not the purchased usage of the license has been exceeded). • ⚠ Appears when the permitted usage of the current license has

UI Element (A-Z)	Description
	been exceeded.
	• Appears when the permitted usage of the current license has not yet been reached.

Preferences

Chapter 23

User Preferences

This chapter includes:

User Preferences Overview

The User Preferences module enables you to select favorite views, localization settings, and notification options for your work in Configuration Manager.

Configure Email Notifications

This task describes how to configure your system so that you can be sent an overview of events for which you may need to perform some action.

This task includes the following steps:

1. "Prerequisites " (on page 207)

2. "Specify notification content and frequency" (on page 207)

1. **Prerequisites**

   Make sure that the system administrator has specified the following:

   - Your email address. For details, see "Specify an Email Address" (on page 187).

   - Time and SMTP account information for emails. For details, see "Specify Email Options" (on page 188).

2. **Specify notification content and frequency**

   a. Navigate to **Preferences > User Preferences > Notifications**.

   b. Select the **Enable notifications** check box.

   c. Do the following:

      i. Select the views for which you want to receive notifications.

      ii. Specify the types of items for which you want to receive notifications, and whether or not to received details about these items, or only a summary.

      > **Note:** If you want to receive direct links to these items in the State Management module of Configuration Manager, you must choose to receive details.

      iii. Specify the frequency at which you will receive the notifications.

   d. Click **Apply**, and then click **OK**.

User Preferences User Interface

This section includes:

User Preferences Dialog Box

This dialog box enables you to:

- select favorite views for display in all Configuration Manager modules

- select the language for the display

- specify whether or not to receive email notifications about policy breaches or changes in views, and to configure the frequency and scope of these notifications.

To access	Select **Preferences > User Preferences**.
Important information	The following options are available: • **Favorite Views.** To select views as favorite views, select them in the left table and double-click them or use the arrow buttons to move them to the right table. • **Localization Settings.** Select the language for the Configuration Manager display. • **Notifications.** Select this option to be notified when changes occur in your views that require attention. **Note:** • When you define favorite views, you then have the option of displaying all views or only favorite views in the different modules. • Preferences are automatically applied when you click **OK**. You do not need to log out and then log in again.

Favorite Views

Only views for which you have View Read permission are displayed.

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

UI Elements (A-Z)	Description
✖	Click to remove the selected view from the favorite views list.
✖	Click to remove all views from the favorite views list.
⮞	Click to add all views to the favorite views list.
→	Click to add the selected views to the favorite views list.
<Left table>	Displays the names and descriptions of all the available views.
<Right table>	Displays the names of the favorite views.
Select favorite views	Enables or disables the favorite view filter. Select one of the following options:

UI Elements (A-Z)	Description
	• **All views.** No favorite views list is defined. All views are displayed. • **Selected views.** Select the views for the favorite views list. Only the favorite views are displayed.

Localization Settings

User interface elements are described below:

UI Elements (A-Z)	Description
Language	Select a language from the drop-down box. **Note:** After changing the language settings, you must log in again for the changes to take effect.
Samples	The date and number format reflect the selected language.

Notifications

User interface elements are described below:

UI Elements (A-Z)	Description
Frequency	Select the frequency at which you want to receive notifications. Select one of the following options: • **Daily.** Specify the interval (in number of days) at which you want to receive the notifications. • **Weekly.** Specify the interval (in number of weeks) at which you want to receive the notifications, and the day of the week on which you want to receive them. • **Monthly.** Specify the interval (in number of months) at which you want to receive the notifications, and the date on which you want to receive them.
General	Select the **Enable notifications** check box to enable email notifications.
Views	Specifies the views for which you want to received notifications. Select one of the following options: • **All views.** Receive notifications for all views for which you have View Read permission. • **Only views for which I have View Write permission.** Receive notifications for all views for which you have View Write permission (default). • **Favorite views.** Receive notifications only for your favorite views. • **Selected views.** Receive notifications for a customized list of views

UI Elements (A-Z)	Description
Notifications scope	Select one or both of the Configuration Manager actions for which you want to received notifications: ● authorizations that are pending approval ● policies that are in breach In addition, select **Show detailed information** to specify whether you want to receive detailed information about the items that require your attention, including links to Configuration Manager.

Appendixes

Appendix A: Capacity Limitations

The following table lists the capacity limits for Configuration Manager.

Maximum number of views	500
Maximum number of high priority views (views that are updated more than once per day)	100
Maximum number of policies	300
Maximum number of component CIs per view	300,000
Maximum number of composite CIs per view	300,000
Maximum number of composite CIs in a policy preview	1000
Maximum number of composite CIs per view (if support for large views has been enabled) For details about enabling support for large views, see "Enable Large Views" in the *HP Universal CMDB Configuration Manager Deployment Guide*.	20,000
Maximum number of concurrent users	50
Maximum number of composite CIs in the Configuration Analysis module	1000
Maximum number of composite CIs that can be tested simultaneously for automatic authorization	1000
Maximum number of views that can concurrently be configured to refresh each time a view is updated	100

Appendix B: Utilities

This section provides information on the following utilities:

Note: Do the following when running these utilities on a Linux system:

- Change the direction of the slashes in the instructions to forward (/) slashes.

- Replace **.bat** with **.sh** in each utility name.

Export Configuration Set

The Export Configuration Set utility enables you to export a configuration set to a configuration dump file. Configuration dump files can later be imported to the same instance of Configuration Manager but with a different name, or a different instance of Configuration Manager. This is useful, for example, when you have a staging/test environment and would like to migrate the configuration set to a production environment.

> **Note:** This functionality is also available within the Configuration Manager UI. Use this utility only in situations where for some reason the UI is locked, for example, when you started Configuration Manager with an invalid configuration and the server cannot start.
>
> This utility does not require the Configuration Manager server to be up.

To export a configuration set:

Run the following command:

```
<Configuration Manager installation directory>\bin\export-cs.bat
<database properties> <configuration set ID><dump file name>
```

where **<database properties>** can be specified by pointing to the location of the **database.properties** file or by specifying each database property.

To locate the configuration set ID, run the Export Configuration Set utility using the **--history** or **--drafts** options to list all historic and draft configuration sets. Historic configuration sets include all configuration sets that were ever activated, including the current configuration set.

Following are the command line <options>:

Option	Description
--connection-url	Database connection URL **Note**: Use this only if **-p** is not used. Use it with --dialect, --driver, --username and --password.
--dialect	Database dialect. **Supported dialects:** H2Dialct, SQLServerDialect, Oracle9iDialect, Oracle10gDialect **Note:** Use this only if **-p** is not used. Use it with --connection-url, --driver, --username and --password.
--driver	Database driver class name. For example: org.h2.Driver, net.sourceforge.jtds.jdbc.Driver, oracle.jdbc.OracleDriver. **Note:** Use this only if **-p** is not used. Use it with --connection-url, --dialect, --username and --password.
--drafts	Display the configuration set drafts - all non-activated configuration sets

Option	Description
-f <filename> **--file <filename>**	Dump file name **Note:** This option is required
-h **--help**	Usage message
--history	Display the configuration set history - all activated configuration sets
-i <id> **--Id <id>**	ID of the configuration set to export
-p <file> **--database-properties <file>**	Location of the **database.properties** file. **Note:** This option is required unless you use --connection-url, --driver, --username and --password to specify the database properties.
--password	Database password **Note:** Use this only if **-p** is not used. Use it with --connection-url, --dialect, --driver and --username.
--username	Database username **Note:** Use this only if **-p** is not used. Use it with --connection-url, --dialect, --driver and -password
--verbose	Verbose mode

- An example of how to list historic configuration sets is:

```
cd <CM installation home>\bin\
export-cs.bat -p ..\conf\database.properties --history
```

- To export a configuration set:

```
<cm-install>\bin\export-cs.bat -p <database.properties location> -i
<configuration set id> -f <dump filename>
```

For example, to export a configuration set with an id 1 to the dump.zip:

```
cd <CM installation home>\bin\
export-cs.bat -p ..\conf\database.properties -i 1 -f dump.zip
```

Import Configuration Set

The import configuration set utility enables you to import a configuration set dump file into an instance of Configuration Manager. Importing a configuration set is useful, for example, when migrating to a different environment, for example, from staging/test to production.

> **Note:**
>
> - This functionality is also available within the Configuration Manager UI. and it is recommended to use the UI option which also performs validations on the imported configuration set.
>
> - The imported configuration set is given the name of the dump file. The configuration set name is unique which means that it is not possible to import the same dump file name twice.

To import a configuration set:

1. Although the server may be up when using this utility, it is recommended that you first stop all running instances of Configuration Manager, since some of the configurations may require a system-wide restart.

2. Run the following command:

   ```
   <Configuration Manager installation directory>\bin\import-cs.bat
   <database properties> <dump file name>
   ```

   where **<database properties>** can be specified by pointing to the location of the **database.properties** file or by specifying each database property.

Following are the command line <options>:

Option	Description
--activate	Activate the imported configuration.
--connection-url	Database connection URL **Note**: Use this only if **-p** is not used. Use it with --dialect, --driver, --username and --password.
--dialect	Database dialect **Supported dialects:** H2Dialct, SQLServerDialect, Oracle9iDialect, Oracle10gDialect **Note:** Use this only if **-p** is not used. Use it with --connection-url, --driver, --username and --password.
--driver	Database driver class name. For example: org.h2.Driver, net.sourceforge.jtds.jdbc.Driver, oracle.jdbc.OracleDriver. **Note:** Use this only if **-p** is not used. Use it with --connection-url, --dialect, --username and --password.
-f <filename>	Dump file name

Option	Description
--file <filename>	**Note:** This option is required
-h **--help**	Usage message
-p <file> **--database-properties <file>**	Location of the **database.properties** file. **Note:** This option is required unless you use --connection-url, --driver, --username and --password to specify the database properties.
--password	Database password **Note:** Use this only if **-p** is not used. Use it with --connection-url, --dialect, --driver and --username.
--username	Database username **Note:** Use this only if **-p** is not used. Use it with --connection-url, --dialect, --driver and -password
--verbose	Verbose mode

To import a configuration set:

```
<cm-install>\bin\import-cs.bat -p <database.properties location> -f
<dump filename>
```

For example, to import a configuration set dump file called mydump.zip:

```
cd <CM installation home>\bin
import-cs.bat -p ..\conf\database.properties -f mydump.zip
```

Password Encryption

To encrypt a password:

1. Ensure that your Configuration Manager installation directory contains a **security** directory that includes the following file:

   encrypt_security

   This file is created during the installation process. However if this file does not exist, then run the following in the **<Configuration Manager installation directory>\bin** directory:

   ```
   generate-keys.bat
   ```

2. Run the following command:

   ```
   <Configuration Manager installation directory>\bin\encrypt-password
   <options>
   ```

   The command line <options> can be:

Option	Description
-p <password> **--password <password>**	Encrypt a single plain-text password.
-d <folder> **--dir <folder>**	Use the encryption keys located at the specified path. If this option is not specified, the default key location is **<cm-installation>\security**, which is where the Generate Keys utility creates the private and public key.
-h **--help**	Print this message.

   For example, to encrypt a single password, run the following:

   ```
   EncryptPassword.bat -p <password to encrypt>
   ```

3. Copy and paste the generated encrypted password (**{ENCRYPTED} <encrypted password>**) into the appropriate Configuration Manager configuration file.

Populate

The Populate utility enables you to create tables in the Configuration Manager database.

> **Note:** This utility deletes any data that was previously stored in the database.

To use the Populate utility:

Run the following command:

```
<Configuration Manager installation directory>\bin\populate.bat i
```

Generate Keys

The Generate Key utility runs automatically during installation and creates the public and private key. If any of the values in the Encryption Properties file change, you must:

- Use the Generate Keys utility to regenerate the public and private key

- Regenerate the database password using the Password Encryption utility and then update the database property file

To use the Generate Keys utility:

Run the following command:

```
<Configuration Manager installation directory>\bin\generate-keys.bat
```

Appendix C: Exporting and Importing System Data

This chapter includes:

Importing and Exporting System Data Overview

You can import and export Configuration Manager data using the JMX console. You might perform these operations, for example, if you want to move the system data from a staging to a production environment, or during recovery following a system crash.

The exported data includes the following resources:

- The list of views managed by Configuration Manager and the managed CI types defined for each view in the View Management module. The TQLs which the views reference are not exported.

- The configuration policy setting defined in the Configuration Policies module. The TQLs that are referenced are not exported.

- The saved configuration analysis results in the Configuration Analysis module, including the saved model and the composite CIs. The actual CI information for the composite CIs, for example its attributes, are not exported.

The export operation migrates the data and stores it in the file system of the machine on which Configuration Manager is running. You can also provide a network path and store the exported data on a different server. The data is exported as an XML file.

You can import the XML file containing the system data from Configuration Manager's file system to another Configuration Manager system of the same version. You can also provide a network path to import the exported data from a different server.

> **Caution:**
>
> When importing system data from one Configuration Manager system to another, you must ensure that the Configuration Manager version is the same or compatible.
>
> Before migrating data between two Configuration Manager instances, which means that each Configuration Manager instance is connected to a different HP Universal CMDB instance, you must first export the relevant TQLs and views from one HP Universal CMDB instance to the other.
>
> If you applied a baseline policy, you need to export the TQL selected in the **Advanced Filter** box in the Configuration Policies module.
>
> If you applied a topology policy, you need to export the Condition TQL in the **Condition TQL** box and the TQL selected in the **Advanced Filter** box in the Configuration Policies module.
>
> To export the referenced TQLs, use the Package Manager in HP Universal CMDB. For details, read the HP Universal CMDB documentation.

Log File for the Import Operations

During each import operation, an **amber_import_export.log** file is generated to the **<Configuration Manager installation directory>\servers\<Configuration Manager server extension name>\logs** directory.

All import actions are written to **amber_import_export.log**, including error messages and the reason for the error. For example,

- Managing view 'View1'

    - View 'View1' already exists

    - View 'View1' was created

    - View 'View1' was not created: reason...

- Adding configuration analysis (adhoc) model 'Model1'

    - Configuration analysis (adhoc) model 'Model1' was created

    - Configuration analysis (adhoc) model 'Model1' already exists

- Adding policy rule 'Rule1'

    - Policy rule 'Rule1' was created

    - Policy rule 'Rule1' already exists

    - Policy rule 'Rule1' was not created: reason...

For information on how to set the message severity levels of the log file, see "Set Log Verbosity Levels" (on page 225).

Export the System Data

This task describes how to list and export the system data, views, and policies of Configuration Manager and store this information in its file system.

1. Launch your Web browser and enter the following address: **http://<server_name>:<port_number>/cnc/jmx-console,** where **<server_name>** is the name of the machine on which Configuration Manager is installed.

2. Enter the JMX console authentication credentials, which by default are:

    - Login name = **admin**

    - Password = **admin**

3. Under **Amber**, click **ImportExport service**.

4. Locate one of the following operations:

    - **exportData**

    - **listAllViews**

    - **exportViews**

    - **listAllPolicies**

    - **exportPolicies**

5. In the **Value** field, enter the file name and the full path of the directory in the file system of the Configuration Manager server to which the data is exported. You can also provide a network path if you do not want the exported file to reside on the same server.

6. Click **Invoke** to export the data. The data is exported as an XML file to the specified directory.

Import the System Data

This task describes how to import the XML file containing the system data from Configuration Manager's file system to another Configuration Manager of the same version using the JMX console.

1. Launch your Web browser and enter the following address: **http://<server_name>:<port_number>/cnc/jmx-console,** where **<server_name>** is the name of the machine on which Configuration Manager is installed.

2. Enter the JMX console authentication credentials, which by default are:

   ▪ Login name = **admin**

   ▪ Password = **admin**

3. Under **Amber**, click **ImportExport service**.

4. Locate the **importData** operation.

5. In the **Value** field, enter the file name and the full path of the directory in the file system of the Configuration Manager server from which the data is imported. You can provide a network path to import data from a file which does not reside on the same server.

6. Click **Invoke** to import the data.

Set Log Verbosity Levels

The **amber_import_export.log** file is the log file which import operations are written. This task describes how to modify the message severity level for the **amber_import_export.log** file.

For information about the **amber_import_export.log** file, see "Log File for the Import Operations" (on page 223).

To modify the message severity level displayed:

Edit the following line in the **<Configuration Manager installation directory>\conf\cmlog4j.properties** file:

```
log4j.logger.amber.import-export=INFO, amber_import_export_fileout
```

The following types of log message commands can be used:

- **ERROR**. Shows error messages only.

- **WARN.** Warning and error messages are displayed.

- **INFO.** Informational messages that record the processing activity that the system performs are displayed, in addition to warning and error messages.

- **DEBUG.** All types of messages and additional debug messages.

> **Caution:** Setting a log to **DEBUG** level may impact performance.