

HP Universal CMDB Configuration Manager

For the Windows and Red Hat Enterprise Linux operating systems

Software Version: 10.00

User Guide

Document Release Date: December 2013

Software Release Date: June 2012



Legal Notices

Warranty

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

The information contained herein is subject to change without notice.

Restricted Rights Legend

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

Copyright Notice

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

Trademark Notices

Adobe™ is a trademark of Adobe Systems Incorporated.

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

UNIX® is a registered trademark of The Open Group.

Documentation Updates

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

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

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

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

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

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

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

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

Support

Visit the HP Software Support Online web site at:

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

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

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

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

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

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

To find more information about access levels, go to:

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

Contents

Introduction	12
Introduction to Configuration Manager	14
HP Universal CMDB Configuration Manager Overview	14
Configuration Modeling and Analysis	15
Offline Analysis	15
Policies	15
Out-of-the-Box Policies	16
Data Control - Actual and Authorized States	17
Historical Comparison	18
Topology Mode and Inventory Mode	18
System Operation Automation	19
User Management	19
Licensed Content	19
Home Page	20
UCMDB Browser	21
Use Cases	23
Best Practices for Working with Configuration Manager	23
Content Management	25
Content Management Overview	25
Requests for Change	26
Configuration Manager Content Workflow	26
Manage Configuration Manager Content - Use Case	28
Troubleshooting and Limitations	30
Federating Data to UCMDB	32
Federated Data Overview	32
Federating Policy Compliance Data	33

Supported TQL Queries	33
Creating Reports	34
Federating KPIs	35
Identifying Business Service Views	37
Supported TQL Queries	38
Creating Reports	38
Consuming KPIs in BSM	38
Federation Workflow with UCMDB	39
Troubleshooting and Limitations	46
Working with Configuration Manager	47
Quick Value	49
View Management Wizard	49
View Definition Page	49
View Details Page	50
Reports Page	50
Similarity Policy Wizard	51
View Selection Page	51
CI Type Selection Page	51
Definition Page	52
Policy Details Page	52
KPI Summary	53
KPI Summary Overview	53
KPI Summary User Interface	53
KPI Summary Page	53
View Summary	57
View Summary Overview	57
Review Automatic State Transition Status	57
View Summary User Interface	58
View Summary Page	58
Policy Summary	61
Policy Summary Overview	61
Policy Summary User Interface	61

Policy Summary Page	61
Explore Views	64
Explore Views Overview	64
Impact Analysis	65
Automation Collisions	65
Reports	66
Run a Controlled or Non-Controlled Automation	66
Create an RFC to Remediate a Policy Breach	68
Create an RFC for a Specific CI	69
Set Folding Rules for Composite CIs	69
Launch External Applications	71
Explore Views User Interface	72
Automation Execution Dialog Box	72
Implementation Details Pane	74
Policies Pane	75
Automation Analysis > Impact - <State> Pane	76
Automation Analysis > Automation Pane	78
Automation Analysis > Collisions Pane	79
CI Details Dialog Box	80
Create New RFC Dialog Box	81
Create RFC for Policy Remediation Dialog Box	82
Explore Views Page	83
Policy Details Dialog Box	89
Select Policy Rule Dialog Box	90
Select Snapshot to View Dialog Box	90
Sort CIs Dialog Box	91
Topology Page	92
Troubleshooting	92
Baseline Analysis	95
Baseline Analysis Overview	95
Define a Configuration Model for Comparison	96
Baseline Analysis User Interface	97

Add Composite CIs Dialog Box	97
Select Composite CI Dialog Box	97
Select Baseline Policy Dialog Box	98
Baseline Analysis Page	98
Comparison Details Dialog Box	101
Segmentation Analysis	103
Segmentation Analysis Overview	103
Select CIs that Contain Groups of Similar CIs	103
Segmentation Analysis User Interface	104
Add Composite CIs Dialog Box	104
CI Details Dialog Box	105
Segmentation Analysis Page	105
Segmentation Parameters Dialog Box	108
Review/Authorize	109
Review/Authorize Overview	109
Integration with Service Manager	110
Reports	111
Authorize Changes to CIs	111
Import a UNL File into Service Manager	112
Launch External Applications	113
Review/Authorize User Interface	113
Authorize Selected Differences Dialog Box	114
CI Details Dialog Box	114
Create RFC for Rolling Back Changes Dialog Box	115
Policy Details Dialog Box	116
Sort CIs Dialog Box	117
Review/Authorize Page	118
View Topology Dialog Box	123
Troubleshooting	124
Changes History	127
Changes History Overview	127
Reports	127

Compare Snapshots	128
Changes History User Interface	128
CI Details Dialog Box	128
Policy Details Dialog Box	129
Changes History Page	130
Select Snapshot to View Dialog Box	134
Sort CIs Dialog Box	135
Topology Page	136
Authorization History	137
Authorization History Overview	137
Reports	137
Compare Snapshots	138
Authorization History User Interface	138
CI Details Dialog Box	138
Policy Details Dialog Box	139
Authorization History Page	140
Select Snapshot to View Dialog Box	143
Sort CIs Dialog Box	144
Topology Page	145
Views	146
Views Overview	146
Out-of-the-Box Views	147
Topology Views and Inventory Views	147
View Refresh Rate	148
Automatic State Transition	149
Add a View to be Managed	150
Set Automatic State Transition Rules for a View	150
Specify the View Refresh Rate	151
Views User Interface	151
Views Page	151
Troubleshooting and Limitations	154
Policies	155

Policies Overview	155
Baselining	157
Policy Groups	157
Define a Baseline or Topology Policy	157
Define a Similarity Policy	158
Configuration Manager Topology Policy - Use Case	158
Configuration Manager Similarity Policy - Use Cases	163
Policies User Interface	166
Attribute Operators	166
Policies Page	167
Policy Preview Dialog Box	172
Select Composite CI Dialog Box	173
Troubleshooting and Limitations	173
Reports	174
Reports Overview	174
Schedule a Report	174
Reports User Interface	175
Report Details Wizard	175
Reports Page	177
Settings	178
Settings Overview	178
Add a New Layer to the Topology Layout	179
Save and Apply Configuration Changes	179
Settings User Interface	180
Open Configuration Set Dialog Box	180
Save as Draft Dialog Box	181
Settings Page	181
Automation Setup	193
Automation Setup Overview	193
Set Up an Automation	194
Automation Setup User Interface	195
Automation Setup Page	195

Automation Policies	198
Automation Policies Management Overview	198
Define an Automation Policy	199
Configuration Manager Automation Policy - Use Case	199
Automation Policies User Interface	200
Automation Policies Page	201
User Preferences	204
User Preferences Overview	204
Configure Email Notifications	204
User Preferences User Interface	205
User Preferences Dialog Box	205
Appendixes	208
Appendix A: Capacity Limitations	210
Appendix B: Utilities	211
Export Configuration Set	212
Import Configuration Set	214
Password Encryption	216
Populate	217
Generate Keys	218
Appendix C: Exporting and Importing System Data	219
Importing and Exporting System Data Overview	219
Export the System Data	220
Import the System Data	221
Set Log Verbosity Levels	221

Introduction

Chapter 1

Introduction to Configuration Manager

This chapter includes:

HP Universal CMDB Configuration Manager Overview	14
Configuration Modeling and Analysis	15
Offline Analysis	15
Policies	15
Data Control - Actual and Authorized States	17
Historical Comparison	18
Topology Mode and Inventory Mode	18
System Operation Automation	19
User Management	19
Licensed Content	19
Home Page	20
UCMDB Browser	21
Use Cases	23
Best Practices for Working with Configuration Manager	23

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 ["Baseline Analysis" on page 95](#).

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 ["Settings Page" on page 181](#).

Policies

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.

You can also bring in policy data from external applications by federation. This data can then be consumed by Configuration Manager in the same way as policies that you create directly within

Configuration Manager. The CI types that can be federated are Node, RunningSoftware and IpAddress.

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 157.

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 additional type of policy is the **similarity policy**, in which you select CIs and attributes that enforce similarity between either all CIs of a certain type in a view, or groups of CIs in a view (where each group is connected to a defined CIT).

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 "[Policies](#)" on page 155.

Out-of-the-Box Policies

Note: A license exists for this feature. Ask your system administrator to purchase the necessary license.

Configuration Manager comes with a group of out-of-the-box policies, based on TQL queries created in UCMDB. There are two types of these policies:

- Data quality policies – These policies ensure that no data is missing in UCMDB.
 - Every server must have a location – This policy is activated only if there is at least one Windows or UNIX machine connected to a Location CI.
 - Every server must have an owner – This policy is activated only if there is at least one Windows or UNIX machine connected to a person with an Ownership relation type.
 - Every MSSQL or Oracle database server must have a version.
- Cluster resiliency policies – These policies ensure that all clusters are resilient. For example, a policy might check for geo-redundancy (that there is no geographical single point of failure on the servers).

Policies are provided for different types of cluster resiliency scenarios:

- Geographical single point of failure – In a virtual environment, the policies ensure that the clusters' virtual machine hosts (for example, ESX servers) are located in at least two different locations. In a non-virtual environment, the policies ensure that all of the clusters' nodes are

located in at least two different locations. To benefit from these policies, the location of the servers should be modeled in UCMDB and you must activate the Apertura VISTA integration, which discovers power distribution units.

- Power distribution unit single point of failure – In a virtual environment, the policies ensure that the clusters' virtual machine hosts (for example, ESX servers) are connected to at least two different power distribution units. In a non-virtual environment, the policies ensure that the clusters' nodes are connected to at least two different power distribution units.
- Virtual machine host single point of failure – In a virtual environment, the policies ensures that the clusters' virtual machines are hosted on more than one server (for example, in more than one ESX server).
- Network single point of failure – In a virtual environment, the policies ensure that the virtual machines are connected to more than one virtual switch.
- Application server similarity – The policies ensure that all the application servers in the clusters are identical.
- Cluster node similarity – The policies ensure that all the nodes in the clusters (virtual or non-virtual machines) are identical.

These policies are located in UCMDB in the following location: **Modeling Studio > Resources** tab (select **Queries** as the resource type > **Configuration Manager > Configuration Manager - Do not modify** folder.

Note: To discover data for these policies, you must perform Universal Discovery (UD), including running all of the following activities:

- JEE
- Virtualization
- Database
- Cluster
- Layer2

For details about these activities and about performing discovery, see the *HP Universal CMDB Discovery and Integration Content Guide*.

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 ["Review/Authorize" on page 109](#). For details on automatic state transition, see ["Views" on page 146](#).

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 Changes History and Authorization History 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 Changes History module displays snapshots of the actual state of a view and the Authorization History 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 ["Changes History" on page 127](#) and ["Authorization History" on page 137](#).

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 66.

For information on how to define an automation policy, see ["Define an Automation Policy"](#) on page 199.

User Management

User, group, and role management functions are performed within the HP Universal CMDB application. For details about setup and configuration, see the section about setting up and working with users in the *HP Universal CMDB Administration Guide*.

Licensed Content

Some features of Configuration Manager require a License to Use (LTU), which is purchased separately. If you plan to use these features, contact your HP sales representative or HP Software business partner to obtain the appropriate license.

The following features require the Advanced Configuration Manager LTU and are included by default during installation:

- **Segmentation Analysis.** For details, see ["Segmentation Analysis"](#) on page 103.
- **Similarity Policies.** For details, see ["Policies"](#) on page 155.

- Topology Policies. For details, see "Policies" on page 155.
- Pre-defined out-of-the-box policies. For details, see "Out-of-the-Box Policies" on page 16
- Pre-defined out-of-the-box views. For details, see "Out-of-the-Box Views" on page 147.

The following features require the Automation Risk Visualizer LTU and are no longer included by default during deployment. These features are available only to users who have previously purchased a license for HP Universal CMDB Configuration Manager version 9.20 or 9.30:

- Automation Management
- Automation Policies

For information about these modules, see the *HP Universal CMDB Configuration Manager User Guide* for the relevant version.

Enabling Advanced Content

Licensed features are installed by default. The advanced content enabled during installation for evaluation purposes, by selecting the check box on the Advanced Content page of the installation wizard.

If you purchased the relevant license after deploying Configuration Manager, perform the following procedure to activate the content:

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.
3. Under **Configuration Manager**, click **ImportExport service**.
4. Locate the **activateAutomanageResource** operation and click **Invoke**.

Deleting Advanced Content

If you installed the advanced content during Configuration Manager deployment but you do not plan to purchase a license for it, you must disable or delete this functionality as follows:

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.
3. Under **Configuration Manager**, click **Licensed content service**.
4. Locate the **deactivateAutomanagedResources** operation and click **Invoke**.

Home Page

The Home page is your entry into Configuration Manager and provides a simple navigation interface to its major features and functionality.

Note: A key icon appears next to those features that require a license to use. Ask your system administrator to purchase the necessary license.

The Home page contains the following areas:

- Manage Your Configuration
 - In the **Views** section, you can:
 - Create and manage an inventory view. For details, see ["View Management Wizard" on page 49](#).
 - Manage an existing UCMDB view. For details, see ["Views" on page 146](#).
 - Open the Modeling Studio in UCMDB to create a new view. For details, see the *HP Universal CMDB Modeling Guide*.
 - In the **Policies** section, you can:
 - Create a new similarity policy, without a grouping option. For details, see ["Similarity Policy Wizard" on page 51](#).
 - Create new policies or manage existing policies. For details, ["Policies" on page 155](#).
 - In the **Reports** section, you can create new reports or edit existing reports. For details, see ["Reports" on page 174](#).
- Favorite Views

This section displays a list of your favorite views and a graphic representation of the policy status (satisfied, in-breach, or no data) for each of the views. Clicking on a link opens that view in the Explore Views module.

You can also click  to access the Show User Preferences window, where you can change preferences for your favorite views.

Note: Up to 40 views (those that have the highest percentages of in-breach policies) are displayed in the Favorite Views list.

- In addition, links on the Home page provide direct access to each of the main functional modules of Configuration Manager.

UCMDB Browser

The UCMDB Browser provides a simple and intuitive search for CIs in UCMDB and displays important data in the context of the selected CI. It is an ideal tool for providing quick access to specific CI information.

For a CI that is found as a result of a search query, relevant data is presented and gathered into information widgets (for example, the Policies widget). Data is presented by default in a Preview mode, with the option to view more comprehensive data in an Expanded mode.

The Browser has a lightweight UI that ensures simple access to UCMDB information. No user administration is required (this is handled by the UCMDB UI), and no upgrades are needed when updating to a newer version. The Browser has backward compatibility and works with different versions of the UCMDB server by using only the UCMDB SDK.

Policy information from Configuration Manager is displayed using the Policies widget in the UCMDB Browser. This widget is provided out of the box, and during installation the required federation configuration from Configuration Manager is created.

The Policies widget shows policy status (satisfied or in breach) for the selected CI that is federated to UCMDB from Configuration Manager. Additional federation adapters for policy information have been configured in UCMDB are also displayed.



Accessing the UCMDB Browser

You can navigate to the UCMDB Browser in several ways:

- To open the UCMDB Browser directly in a new window, enter:




```
http://<server name or IP address>.<domain name>:<port>/ucmdb-browser
```

where **<server name or IP address>.<domain name>** represents the fully qualified domain name (FQDN) of the Configuration Manager server and **<port>** represents the port selected during installation.

- To open the embedded UCMDB browser with no CI selected, click **Explore > UCMDB Browser**.
- To open the UCMDB Browser in the context of a selected CI, do one of the following:
 - Enter a term in the Search field at the top of the Configuration Manager screen and click .
 - In the Review/Authorize or Explore Views modules, select a CI and click .

Navigating from the UCMDB Browser to Configuration Manager

Three options are provided for navigating back to Configuration Manager from the UCMDB Browser:

UI Elements	Description
	Click to navigate back to the originating module in Configuration Manager.
	Click to navigate to the Review/Authorize module in the context of the selected CI. Note: This functionality is available only for composite CIs.
	Click to navigate to the Explore Views module in the context of the selected CI. Note: This functionality is available only for composite CIs.

Note: If you select a CI in the UCMDB Browser that does not appear in any view and you attempt to navigate the Review/Authorize Changes or Explore Views modules, you will be asked if you want to create a view for the selected CI. If you choose to do so, you will be redirected to the selected module when the wizard is completed. For details, see "[View Management Wizard](#)" on page 49.

Getting Help

When you are in the embedded UCMDB Browser, you can access the complete UCMDB Browser online help by clicking **Help > Help on this page**.

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	25
Requests for Change	26
Configuration Manager Content Workflow	26
Manage Configuration Manager Content - Use Case	28
Troubleshooting and Limitations	30

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 69.

Another method of organizing the data is by setting the layer and classification definitions for the composite CIs. **Layers** are categories used for grouping composite CIs functionally. Examples of layers include Business, Software, and Infrastructure. **Classifications** are categories for grouping the composite CIs 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 Review/Authorize, Changes History, and Authorization History 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 **Administration > Settings > Application Management > RFC** under **Fetches 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 Review/Authorize module. In the Changes History and Authorization History 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:

- "Prerequisites" below
- "Define the CI Composition" below
- "Define Layers and Classifications" on the next page
- "Define Managed Attributes" on the next page
- "Define Comparable Attributes" on the next page
- "Define Comparison Matching Rules" on the next page

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 69](#).

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 Explore Views module 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 **Administration > 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 **Managed** 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. Click the **UCMDB Foundation**  icon to open HP Universal CMDB.
- b. Navigate 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 Modeling Guide*.

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 26](#).

This scenario includes the following steps:

- "Background" below
- "Set the CI Composition in HP Universal CMDB" on the next page
- "Set Layer Definitions" on the next page
- "Set Classification Definitions" on the next page
- "Set Managed Attributes" on the next page
- "Set Comparable Attributes" on page 30
- "Define Matching Rules" on page 30


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

Click the **UCMDB Foundation**  icon 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 69.

3. Set Layer Definitions

Navigate 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

Navigate 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. Navigate 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 **Managed** 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. Click the **UCMDB Foundation**  icon to open HP Universal CMDB.
- b. Navigate 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. Click the **UCMDB Foundation**  icon to open HP Universal CMDB.
- b. Navigate 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 **Administration > Settings**.
- Execute a JMX call to run the offline analysis calculation on the relevant view.
- Navigate to **Policies**. Click the **Recalculate Policy Analysis** button. This invokes the offline analysis process for all views (which may take some time). You may also need to make an artificial change to one policy and save it.

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

Solution. In order to access UCMDB without logging in again, you need to enable single sign-on. For details, see the section about enabling LW-SSO between Configuration Manager and UCMDB in the *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 navigate to **Managers > Modeling > CI Type Manager**, and select **CI Types** from the list box in the CI Types pane.

Solution. Navigate to **Managers > Administration > Infrastructure Settings** in 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	32
Federating Policy Compliance Data	33
Federating KPIs	35
Federation Workflow with UCMDB	39
Troubleshooting and Limitations	46

Federated Data Overview

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 the next page.

UCMDB provides two adapters to federate data from Configuration Manager to UCMDB. The adapters sit on top of UCMDB and carry out the operation to bring the federated data from Configuration Manager. For details about these adapters, see "[Federation Workflow with UCMDB](#)" on page 39.

For details, see "[Federating Policy Compliance Data](#)" on the next page and "[Federating KPIs](#)" on page 35.

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	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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" on page 38
- "Creating Reports" on page 38

Supported TQL Queries

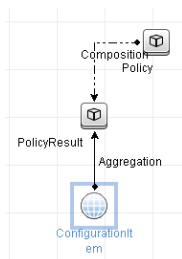
The basic way to consume data in UCMDB is by creating TQL queries that retrieve the information that you want from the CMDB. The TQL queries that support federated data from UCMDB are:

- 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**

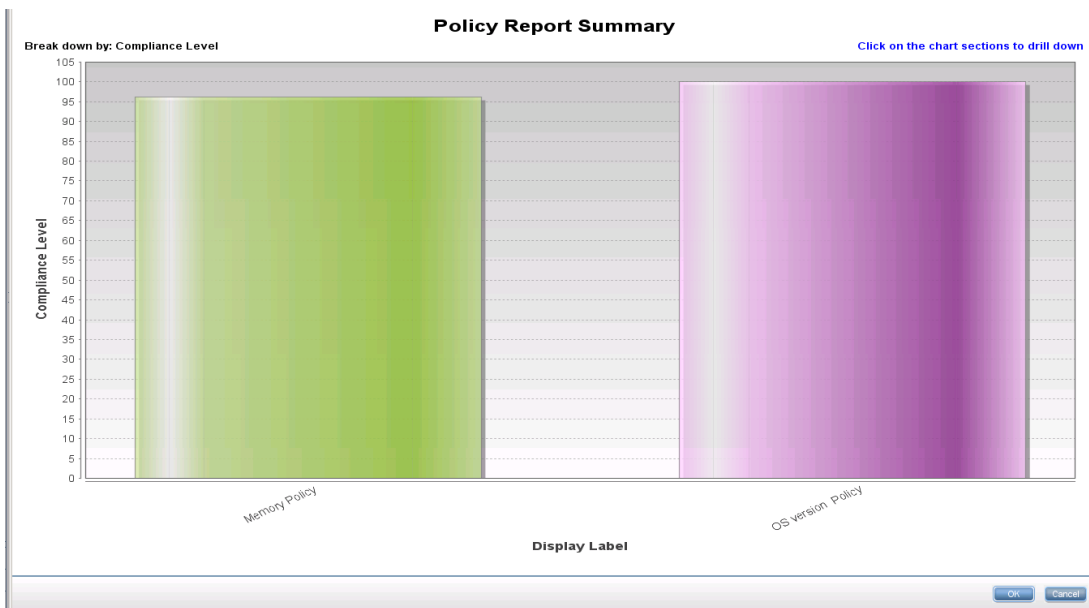
A policy compliance report displays the raw data about policy results of CIs, per policy.

Display Label	ComplianceLevel	PolicyDefinedBy
VMAMQA33		
in_breach	0	
New Baseline Policy		UCMDB-CM
VMAMQA35		
compliant	100	
New Baseline Policy		UCMDB-CM
VMAMQA62		
VMAMQA71		
VMAMQA88		
VMAMQA121		
VMAMQA134		
VMAMQA154		
VMAMQA187		

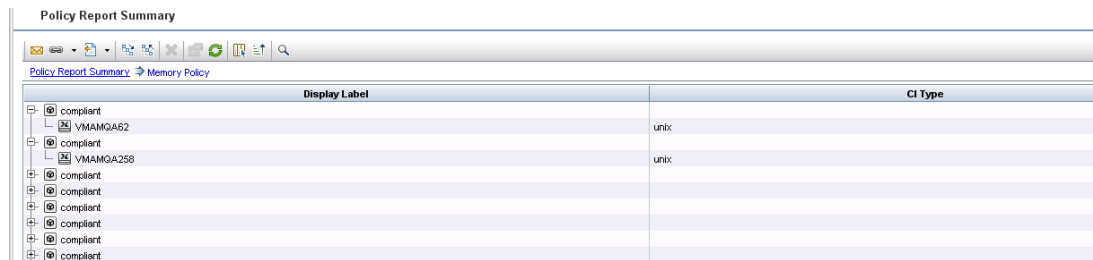
The following out-of-the-box policy reports are provided:

- 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 39](#).

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 37](#).

Configuration Manager federates its KPI data into these models:

Model	Description
Policy compliance KPI for composite CI	<ul style="list-style-type: none"> • 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)

Model	Description
Policy compliance KPI for business service	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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) • kpi_value—the value of this KPI, as a percentage (0-not authorized; 100-authorized))
Authorization status KPI for business service	<ul style="list-style-type: none"> • 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:

- ["Supported TQL Queries" on page 38](#)
- ["Identifying Business Service Views" on the next page](#)
- ["Creating Reports" on page 38](#)
- ["Consuming KPIs in BSM" on page 38](#)

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 ["Federation Workflow with UCMDB"](#) on the next page.

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 45.

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" below
- "Create an integration point to federate policy compliance data" below
- "Create an integration point to federate KPI data" on the next page
- "Create policy reports based on the CIs in a view or a custom TQL query" on page 41
- "Create summary policy reports based on the CIs in a view or a custom TQL query" on page 42
- "Create KPI reports" on page 44
- "Consume the KPIs in HP Business Service Management" on page 45

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  to create a new integration point.
3. Set the following adapter properties:


Field	Description
Adapter	Click  and select CMPolicyAdapter .
Credentials ID	Do the following: <ol style="list-style-type: none"> a. Click . b. Select Generic DB Protocol (SQL) and click OK. c. Click  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
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.




Field	Description
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 46
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 .
Configuration Manager URL	Provide the URL of the Configuration Manager server. Note: If you have changed the root context from http://<IP address>:<port>//cnc to http://<IP address>:<port>/<context>/cnc , you must specify a the URL includes this root context when configuring the integration point.
Credentials ID	Do the following: <ol style="list-style-type: none"> 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 Manage, Authorize, and Access to UI permissions. d. When finished, click OK
Integration Name	Enter a name for the new integration point.
Port	Enter the port number that is used for communication with the 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.

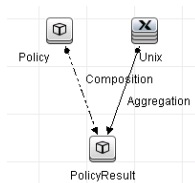
For further details about creating integration points, see the section about the Integration Studio in the *HP Universal CMDB Data Flow Management Guide*.

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 39, if one does not already exist.
2. In UCMDB, create a new view with a custom TQL query, or copy an existing view.

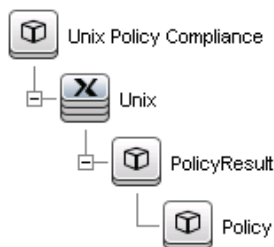
Note: When using a custom TQL query, make sure you take into account the limitations of the data capacity when using federation. You should filter the CIs in the TQL query to take this limitation into account. For details, see "Troubleshooting and Limitations" on page 46

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.

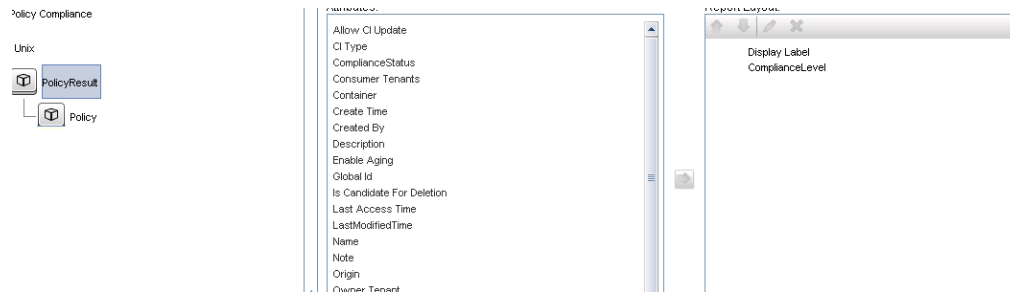
Hierarchy Method: Manual Rule Based



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*.

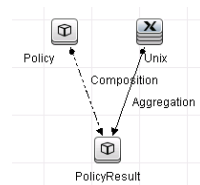
For details about creating reports, see the section about reports in the *HP Universal CMDB Modeling Guide*.

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 39, if one does not already exist.
2. In UCMDB, create a new view or copy an existing view.

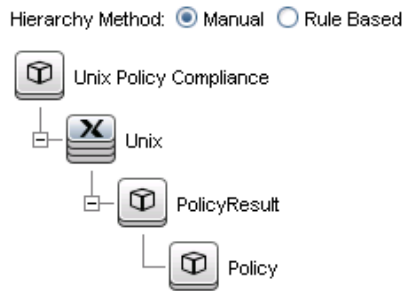
Note: When using a custom TQL query, make sure you take into account the limitations of the data capacity when using federation. You should filter the CIs in the TQL query to take this limitation into account. For details, see ["Troubleshooting and Limitations"](#) on page 46.

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.

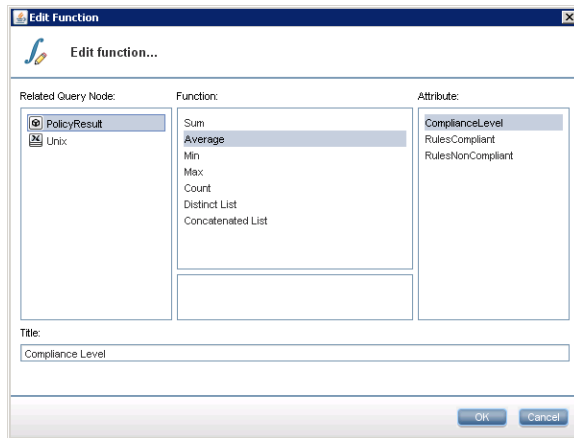


4. Specify the Configuration Manager integration point that you defined to be the data source that provides the policy and policy result data.

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



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



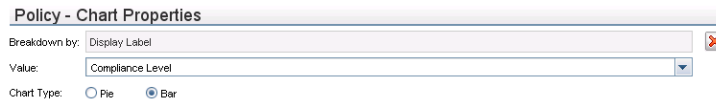
7. Add properties for the Policy CI type to the report layout. An example is shown below.



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

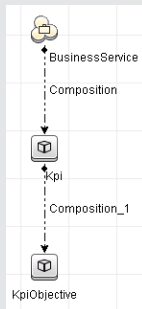
You can create KPI reports based on the CIs in a view, a custom TQL query, or business services.

1. Create an integration point as described in "[Create an integration point to federate policy compliance data](#)" on page 39, if one does not already exist.
2. In UCMDB, create a new view based on a custom TQL or copy an existing view.

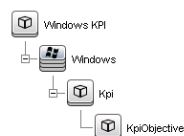
Note: When using a custom TQL query, make sure you take into account the limitations of the data capacity when using federation. You should filter the CIs in the TQL query to take this limitation into account. For details, see [Troubleshooting and Limitations](#).

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.

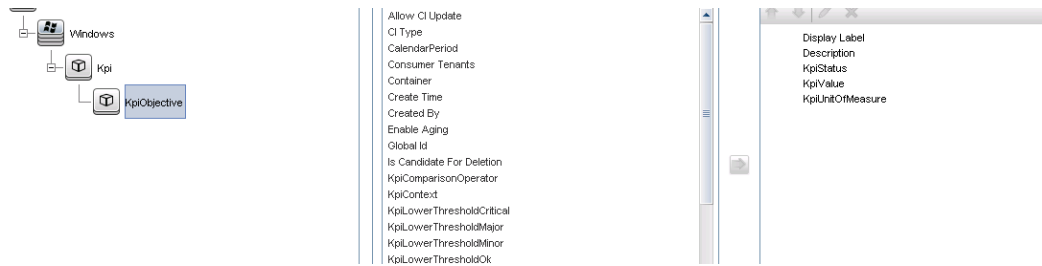
Note: If you want to create a business services report, select the BusinessService CI type when creating the TQL query.



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.

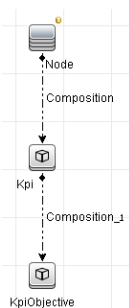


7. If desired, you can schedule these reports to be created periodically. For details, see the *HP Universal CMDB Data Flow Management Guide*.

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.
- The maximum number of CIs that can be federated is configurable. To change this number, edit the value of the Max Num To Federate setting in the Infrastructure Settings Manager in UCMDB. For details about changing settings, see 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 Deployment Guide*.
- If the test connection fails, click **Details** and check the first error in the stack trace for more information.
- Since a CI can be managed in multiple views, the same policy may be applied to the same CI in multiple views and may receive different similarity results, since the similarity group may be different in different views.

Working with Configuration Manager

Chapter 5

Quick Value

Configuration Manager comes with two wizards that provide an easy way to take advantage of its views and policies features.

- The View Management wizard enables you to create simple views and receive reports about them, without using UCMDB. For details, see "[View Management Wizard](#)" below.
- The Similarity Policy wizard enables you to create simple similarity policies. Such policies can enforce similarity and configuration on a set of CIs. For details, see "[Similarity Policy Wizard](#)" on page 51.

Both of these wizards can be accessed from links on the Home page in the Manage Your Configuration area.

View Management Wizard

This wizard enables you to create a simple UCMDB view and manage it in Configuration Manager.

When you create a view using this wizard, a new view is saved in UCMDB with the same default settings as if it had been created directly in the UCMDB UI. In addition, a managed view with the same name is saved and calculated in Configuration Manager.


To access	On the Home page, click the Create and Manage a Simple View link.
Wizard map	" View Definition Page " > " View Details Page " > " Reports Page "



View Definition Page

On this page, you specify the main CI type for the view you are creating. In addition, you can use a filter to retrieve a subset of the CIs of this main CI type, and you can also relate the main CI type to an additional CI type. For example, you might want to create a view that contains a group of UNIX machines that are all connected to Oracle databases. In this case, the main CI type for this view would be UNIX, and you would filter by a name pattern to include only UNIX machines that belong to some specific group, and choose an Oracle database as the related CI type.

Wizard map	The " View Management Wizard " contains: " View Definition Page " > " View Details Page " > " Reports Page "
-------------------	---

User interface elements are described below:

UI Element (A-Z)	Description
Attribute conditions on the main CI type	(Optional) Click the  icon. Specify the attributes to be used to filter the main CI type in the list of attributes, and click OK .

UI Element (A-Z)	Description
	<p>You can select attributes only for the CI type that is selected as the main CI type for the view.</p> <p>Note: If you want to use a wildcard as part of the attribute condition, use a % character (used in UCMDB) instead of a * character (used in Configuration Manager).</p>
Main CI type for the view	<p>Click the  icon to open the Select CI Type dialog box. Select a CI type from the CI type tree, and click OK.</p> <p>Only composite CIs are displayed for creating the view.</p>
Related CI Type	<p>Click the  icon to open the Select CI Type dialog box. Select an additional related CI type from the CI type tree, and click OK.</p> <p>Note: You should only select CI types that have some relationship to the main CI type.</p>

View Details Page

On this page, you enter details about the view you are creating.

Wizard map	<p>The "View Management Wizard" contains:</p> <p>"View Definition Page" > "View Details Page" > "Reports Page"</p>
-------------------	---

User interface elements are described below:

UI Element (A-Z)	Description
Description	(Optional) Enter a description for the view.
Name	Enter a name for the view.

Reports Page

On this page, you can optionally specify the daily reports you want to receive about the view.

Important information	<p>To receive reports, an administrator must configure the system to enable emails to be sent. For details, see "Configure Email Notifications" on page 204.</p>
Wizard map	<p>The "View Management Wizard" contains:</p> <p>"View Definition Page" > "View Details Page" > "Reports Page"</p>
See also	" Reports " on page 174

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

UI Element (A-Z)	Description
<Reports>	(Optional) You can select one or both of the following daily reports: <ul style="list-style-type: none"> all detected changes configuration comparison

Similarity Policy Wizard

This wizard enables you to create a simple similarity policy, without a grouping option. For details about creating a similarity policy based on a grouping pattern, see "Define a Similarity Policy" on page 158.

For example, consider the case where you are managing a view that contains a lab of Windows computers. You want to enforce that some or all the Windows computers must have the same operating system version and amount of memory. The similarity policy wizard provides an easy way to create such a policy.


To access	On the Home page, click the Create a New Similarity Policy link.
Wizard map	"View Selection Page" > "CI Type Selection Page" > "Definition Page" > "Policy Details Page"
See also	"Policies" on page 155

View Selection Page

On this page, you select the view that contains the CIs on which you want the policy to be enforced.

Wizard map	The "Similarity Policy Wizard" contains: "View Selection Page" > "CI Type Selection Page" > "Definition Page" > "Policy Details Page"
-------------------	---

User interface elements are described below:

UI Element (A-Z)	Description
View	Click the  icon to open the Select View dialog box. Double-click a view to select it.



CI Type Selection Page

On this page, you select the CI type to be checked for similarity. In addition, you can add a filter to apply the policy to a more specific subset of the specified CI type (for example, all Windows machines that have a specific naming convention).

Wizard map	The "Similarity Policy Wizard" contains:
-------------------	--

	"View Selection Page" > " CI Type Selection Page " > "Definition Page" > "Policy Details Page"
--	---

User interface elements are described below:

UI Element (A-Z)	Description
CI Type	Click the  icon to open the Select CI Type dialog box. Select the CI type that will be checked for similarity from the CI type tree, and click OK . This CI type must exist in the view that was selected on the " View Selection Page " on the previous page.
Filter by attribute conditions	(Optional) Click the  icon to open the Specify baseline for filter dialog box. Select the attributes that will be used to filter the CI type instances, and click OK .

Definition Page

On this page, you specify the components and attributes to be compared by the policy. This means that all CIs that are in the scope of this similarity policy scope must have the same values for these selected components and attributes.

Wizard map	The " Similarity Policy Wizard " contains: " View Selection Page " > " CI Type Selection Page " > " Definition Page " > " Policy Details Page "
-------------------	---

User interface elements are described below:

UI Element (A-Z)	Description
Definition	Specify the components and attributes to be compared for similarity.

Policy Details Page

On this page, you enter a name and description for the similarity policy.

Wizard map	The " Similarity Policy Wizard " contains: " View Selection Page " > " CI Type Selection Page " > " Definition Page " > " Policy Details Page "
-------------------	---

User interface elements are described below:

UI Element (A-Z)	Description
Description	(Optional) Enter a description for the policy.
Name	Enter a name for the policy.

Chapter 6

KPI Summary

This chapter includes:

KPI Summary Overview	53
KPI Summary User Interface	53

KPI Summary Overview

The KPI Statistics Page provides a dashboard view of the key metrics being monitored by Configuration Manager. 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 permission.

KPI Summary User Interface

This section includes (in alphabetical order):

KPI Summary Page	53
------------------------	----

KPI Summary 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 permission are displayed.

To access	Select Statistics > KPI Summary .
Important information	<p>The Managed CIs pane displays the number of authorized and unauthorized CIs over the selected period.</p> <p>The Policy Summary pane displays the number of satisfied and breaching CIs in each state for each of the policies under administration.</p> <p>The Authorized Changes pane displays the number of authorized changes over the selected period.</p> <p>The Non-Compliant CIs pane displays the total number of CIs satisfying or in breach of baseline policies.</p>

	Note: You can rearrange the layout of the 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.
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
	Select the time period for the data displayed in the graph. The options are: <ul style="list-style-type: none"> • 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.
	Select the view(s) reflected in the graph.
<Graph>	The graph displays the number of changes authorized over the selected time period.






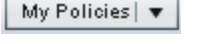
Managed CIs Pane

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

UI Elements (A-Z)	Description
	Select the time period for the data displayed in the graph. The options are: <ul style="list-style-type: none"> • Week • Month • Three Months • Year
	Click to display the graph's legend.
	Click to change the display to table format.
	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
	Select the time period for the data displayed in the graph. The options are: <ul style="list-style-type: none"> • 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.
	Select the view(s) reflected in the graph.
	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.
Source	The external product, if any, that is the source of the policy.
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: For external policies that contain CIs in the authorized state, the status bar displays only the actual state data.

Right Pane

This pane is available when you click  to maximize the Policy Summary 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. For each policy, you can drill down on the following items to view details in the Explore Views module: <ul style="list-style-type: none"> • View name • Satisfied CIs (Actual state) • In-breach CIs (Actual state) • Satisfied CIs (Authorized state) • In-breach CIs (Authorized state)

Chapter 7

View Summary

This chapter includes:

View Summary Overview	57
Review Automatic State Transition Status	57
View Summary User Interface	58

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 Review/Authorize 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). Note that external policies are not included in the authorized state statistics, and therefore if you drill down to see the details of external policies that contain CIs in the authorized state, only actual state data is displayed.


Note that you cannot drill down to see the details of external policies that contain CIs in the authorized state.

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 were authorized. You can drill down to view the last authorization in detail. It clearly indicates the number of related RFCs that are relevant to the pending authorizations.

Note: The View Summary displays only views for which you have View or Authorize 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 Authorization History 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 Review/Authorize 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 Authorization History module, and clicking the **See Details** link next to the changes that were not authorized takes you to the Review/Authorize module.

View Summary User Interface

This section includes:



View Summary Page58





View Summary Page

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

To access	Select Statistics > 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.
	Click Export Report to choose the export format for the View Summary report data. The available options are: <ul style="list-style-type: none"> • Excel. The table data is formatted as an XLS (Excel) file that can be displayed in a spreadsheet. • PDF. The table data is exported in PDF format. • CSV. The table data is formatted as a comma-separated values (CSV) text file that can be displayed in a spreadsheet. The currently applied filters are taken into account when generating output for reports.

UI Elements (A-Z)	Description
	Click Refresh to refresh the policy list.
<input type="checkbox"/> Hide empty views	Select the Hide empty views check box to display only views that contain data.
	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.
	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: <ul style="list-style-type: none"> • 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.
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. Note: The status bar does not display policy satisfaction status for federated policies that contain CIs in the authorized state.
Policy Status Legend	The legend for the policy status graph. The following categories are included: <ul style="list-style-type: none"> • Satisfied • In-breach
Related RFCs	Displays the number of requests for change which apply to CIs in the

UI Elements (A-Z)	Description
	current view.
View Name	Click on the view name to go to the Review/Authorize page for the selected view.

Chapter 8

Policy Summary

This chapter includes:

Policy Summary Overview	61
Policy Summary User Interface	61

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 permission.



Policy Summary User Interface

This section includes:




Policy Summary Page	61
---------------------------	----

Policy Summary Page

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

To access	Select Statistics > Policy Summary .
Important information	<p>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:</p> <ul style="list-style-type: none">•  Satisfied•  In-breach <p>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.</p>

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: <ul style="list-style-type: none"> • 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 formatted as a comma-separated values (CSV) text file that can be displayed in a spreadsheet. <p>The currently applied filters are taken into account when generating output for reports.</p>
	Click Refresh to refresh the policy list.
<input type="checkbox"/> Show only active policies	Select the Show only active policies check box to display only policies that are currently active.

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.
Source	The external product, if any, that is the source of the policy.
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: For external policies that contain CIs in the authorized state, the status bar displays only the actual state data.

Right Pane

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

UI Elements (A-Z)	Description
<p><Breakdown by View Table></p>	<p>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.</p> <p>For each policy, you can drill down on the following items to view details in the Explore Views module:</p> <ul style="list-style-type: none"> • View name • Satisfied CIs (Actual state) • In-breach CIs (Actual state) • Satisfied CIs (Authorized state) • In-breach CIs (Authorized state)

Chapter 9

Explore Views

This chapter includes:

Explore Views Overview	64
Impact Analysis	65
Automation Collisions	65
Reports	66
Run a Controlled or Non-Controlled Automation	66
Create an RFC to Remediate a Policy Breach	68
Create an RFC for a Specific CI	69
Set Folding Rules for Composite CIs	69
Launch External Applications	71
Explore Views User Interface	72
Troubleshooting	92

Explore Views Overview

The Explore Views 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.

This screenshot should show all of the features of the Explore Views module - including composite CIs with breaching and satisfied icons, added/removed/changed icons and RFC icons. A composite CI should be selected so that the lower pane contains meaningful information.

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 Explore Views module user interface, see ["Explore Views User Interface" on page 72](#).

Note: You can only select views on which you have View or Authorize permission.

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 76.

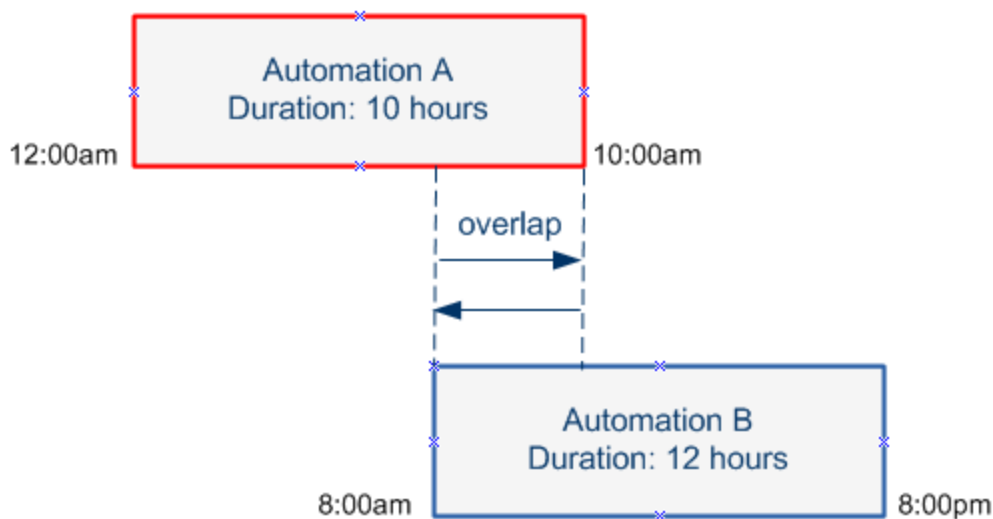
The impact severity level of a CI is determined by the following rules:

- 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 79](#).

Reports

Configuration Manager provides the ability to export policy information for a view, including information about CIs that are in breach of defined policies. Causes of in-breach CIs might be:

- CIs that do not satisfy a baseline condition.
- Missing CIs.
- Additional CIs in a composite CI.

Note: Information about breaching CIs is not included in reports that are exported in .pdf format.

The report contains an analysis of the CIs in a specific state (actual or authorized), at a particular point in time. The report lists which CIs are in breach, down to the attribute level, and also the cause of those breaches.

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](#)" below
- "[Add a flow and configure the automation parameters](#)" below
- "[Run a controlled or non-controlled automation](#)" on the next page


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

1. Add a view to be managed

In the **Views** module, add a view from HP Universal CMDB, to be managed. For details, see "[Add a View to be Managed](#)" on [page 150](#).


2. Add a flow and configure the automation parameters

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

- a. Click  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 Setup 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 Setup Page](#)" on page 195.

3. Run a controlled or non-controlled automation

- a. Select **Explorer > Explore Views**.
- b. In the Explore Views 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 Setup module, or a sub-class of it. For details, see "[Automation Setup Page](#)" on page 195.
- d. In the Composite CIs pane, click **Run Automation**  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 196 in the "[Automation Setup Page](#)" on page 195.

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 78 in the "[Automation Planner Page](#)" on page 74.

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 74 and the "[Policies Pane](#)" on page 75 in the "[Automation Planner Page](#)" on page 74.

- i. Click **Run** to run the automation.
 - o 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 87 in the "[Explore Views Page](#)" on page 83.
 - o 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 Explore Views 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.
3. Click  to create an RFC that remediates the policy breach. The Select Policy Rule dialog box opens. For details, see "[Select Policy Rule Dialog Box](#)" on page 90.
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. For details, see

"Create RFC for Policy Remediation Dialog Box" on page 82.

Enter the required information and click **Submit**.

Create an RFC for a Specific CI

This task enables you to create an RFC for specific CIs.

1. In the Explore Views module, click **Select View**  to open a view.
2. In the Composite CIs pane, select the CIs for which you want to create the RFCs.
3. Click . The **Create New RFC** dialog box opens. For details, see "Create New RFC Dialog Box" on page 81.

Enter the required information and click **Submit**.

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:



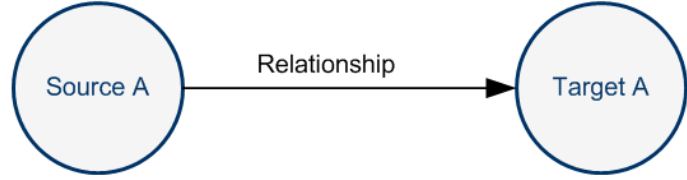
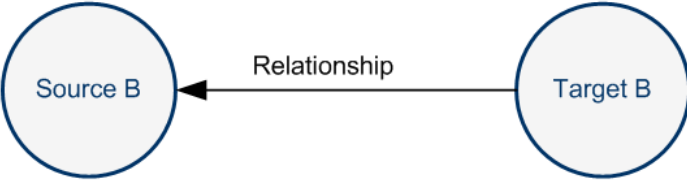
- "Prerequisites" below
- "Define the calculated relationship" below

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. Click the **UCMDB Foundation**  icon to open HP Universal CMDB.
- b. Navigate 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. <ul style="list-style-type: none">  The direction is from source to target.  The direction is from target to source. <p>The direction of the relationship determines which is the composite CI and which is the component CI.</p> <ul style="list-style-type: none"> 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: <div style="display: flex; justify-content: space-around; align-items: center;"> <div style="text-align: center;"> <p>Composite CI</p>  </div> <div style="text-align: center;"> <p>Component CI</p> </div> </div> <ul style="list-style-type: none"> 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: <div style="display: flex; justify-content: space-around; align-items: center;"> <div style="text-align: center;"> <p>Component CI</p>  </div> <div style="text-align: center;"> <p>Composite CI</p> </div> </div>

- 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 Modeling Guide*.

Launch External Applications

Configuration Manager now provides a mechanism to configure a generic UI integration that can launch any application user interface in the context of a UCMDB CI or a UCMDB view. For example, you can launch the HP Enterprise Collaboration user interface in order to open a new discussion related to an issue that may have been found on some CI, or launch UCMDB to view the CI properties of the selected CI). This functionality is available in the Review/Authorize and the Explore Views modules.

Note: In order to be able to integrate with external applications, it is recommended that all applications be configured with LW-SSO and work with the same user management system. This prevents the need to enter a user name and login for each external application.


To launch external applications:

1. Specify the URL of the application that you want to open. For example:

```
http://<UCMDB server machine or IP address>:8080/ucmdb-ui/cms/  
directAppletLogin.do?cmd=ShowProperties&objectId=  
${ucmdbId}&navigation=false&interfaceVersion=9.0.0
```

For this example, `${ucmdbId}` is replaced with the ID of the selected composite CI (as it appears in UCMDB).

For details, see "UI Integrations" on page 191.

Note: You must perform this step for the  icon to be visible.

2. In the Review/Authorize or the Explore Views module, click .

The application that you configured opens in a browser window.



Explore Views User Interface

This section includes (in alphabetical order):

Automation Execution Dialog Box	72
CI Details Dialog Box	80
Create New RFC Dialog Box	81
Create RFC for Policy Remediation Dialog Box	82
Explore Views Page	83
Policy Details Dialog Box	89
Select Policy Rule Dialog Box	90
Select Snapshot to View Dialog Box	90
Sort CIs Dialog Box	91
Topology Page	92

Automation Execution Dialog Box

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

To access	Select Explorer > Explore Views . In the Composite CIs pane, select the required CI and click Run Automation  .
Important information	<ul style="list-style-type: none">To enable the Run Automation  button, ensure that:<ul style="list-style-type: none">You select Actual State or Authorized State from the toolbar.There is a managed automation mapped to a CI type in the Automation Setup module that is the same as the CI type of the selected CI in the Composite CIs pane. For details, see "Automation Setup Page" on page 195.Only users with Automation Execution permission are able to run an automation.
Relevant tasks	"Run a Controlled or Non-Controlled Automation" on page 66
See also	<ul style="list-style-type: none">"Automation Policies" on page 198"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	<p>Name. The name of the automation as defined in Administration > Automation Setup.</p> <p>Flow UUID. The HP Operations Orchestration instance name that uniquely identifies the HP Operations Orchestration instance being used by Configuration Manager.</p> <p>Flow Path. The full path and original name of the flow in HP Operations Orchestration.</p> <p>Description. The description of the automation as defined in Administration > Automation Setup.</p>
Automations	<p>Displays a list of automations you can run. The automations appear after they are imported from Administration > Automation Setup. For details, see "Import a flow from HP Operations Orchestration" on page 194.</p> <p>The automations that appear are relevant to the CI type you chose in the Composite CIs pane in the Explore Views page.</p>
Execution Parameters	<p>The execution parameters needed to run the flow. Only required fields, as indicated by a red asterisk, are mandatory.</p> <p>Note: Configuration Manager does not allow you to run an automation whose required execution parameters values have not been configured.</p> <ul style="list-style-type: none"> • 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	<p>Displays whether the automation was configured as controlled or not controlled in Administration > Automation Setup.</p>
Next/Run	<ul style="list-style-type: none"> • 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. <p>If you ran a non-controlled automation, a window opens with the following message: <i>The automation is running. Click here to view a detailed report.</i> The word here is a link that opens HP Operations Orchestration, with the report of the automation result.</p>

Automation Planner Page

User interface elements are described below:

<p>Important information</p>	<p>This page is only available only when you are running a controlled automation.</p> <p>It contains the following panes:</p> <ul style="list-style-type: none"> • "Implementation Details Pane" below • "Policies Pane" on the next page • "Automation Analysis > Impact - <State> Pane" on page 76 • "Automation Analysis > Automation Pane" on page 78 • "Automation Analysis > Collisions Pane" on page 79
-------------------------------------	--

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
<p>Expected End Time</p>	<p>The estimated time at which the automation process is expected to end.</p> <p>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.</p> <p>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.</p>
<p>Flow Properties</p>	<p>Displays the automation parameters.</p> <p>Note: If you delete the required execution parameters, the OK button is disabled.</p>
<p>Planned Start Time</p>	<p>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.</p> <p>If you choose a future date, Configuration Manager recalculates all the automation analysis and policy information in the Automation Planner page.</p>

Policies Pane

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

See also	"Policies" on page 155
-----------------	------------------------

User interface elements are described below:

UI Elements (A-Z)	Description
◀ ▶	<p>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 201.</p> <ul style="list-style-type: none"> • 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. • Restriction. The conditions defined for the policy. <ul style="list-style-type: none"> ▪ 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. <p>Click ◀ to hide the policy details.</p>
<List of automation policies >	<p>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.</p> <p> Denotes a situation in which the automation does not fulfill all of the conditions defined for this policy.</p> <p> Denotes a situation in which the automation fulfills all of the conditions defined for this policy.</p> <p>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.</p> <p>For example, if a breached policy defines that an automation whose elapsed time since the last execution is greater than a month causes a</p>


UI Elements (A-Z)	Description
	<p>breach, you might decide that this does not pose a risk, as opposed to a breach which causes server downtime.</p> <p>Note: Configuration Manager enables you to run the automation even if there are automation policies that are breached.</p>











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	<p>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.</p> <p>To select the state by which you want to manage your view, navigate to Administration > Settings > Application Management > Impact.</p>
See also	<ul style="list-style-type: none"> • "Policies" on page 155 • "Impact Analysis" on page 65 • "Data Control - Actual and Authorized States" on page 17

User interface elements are described below:

UI Elements (A-Z)	Description
Highest Business Criticality	<p>Displays the CIs having the highest business criticality level of the CIs impacted by the automation.</p> <p>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.</p> <p>The business criticality level of a CI in HP Universal CMDB is mapped as follows:</p> <ul style="list-style-type: none"> • 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 <p>The following icons indicate the business criticality levels:</p> <p> Critical</p>

UI Elements (A-Z)	Description
	<p>  High  Medium  Low </p> <p>Click the drill down 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.</p> <p>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.</p> <p>Click this arrow  to hide the table.</p>
<p>Total Business CIs</p>	<p>Displays the total number of business CIs impacted by the automation.</p> <p>Click the drill down 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.</p> <p>For information on the icons that indicate the impact severity levels, see Worst Impact Severity in this table.</p> <p>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.</p> <p>Click this arrow  to hide the table.</p>
<p>Total System CIs</p>	<p>Displays the total number of system CIs that were impacted by the automation.</p> <p>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.</p> <p>A tooltip indicating the impact severity level of the CI is visible when you hold your pointer over the severity icon.</p> <p>Click this arrow  to hide the table.</p>
<p>Worst Impact Severity</p>	<p>Displays the CIs that have the highest impact severity level of the business CIs that have been impacted.</p> <p>The following icons indicate the following impact severity levels:</p> <p>  Critical </p>

UI Elements (A-Z)	Description
	<p>  High  Medium  Low  Very Low </p> <p>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.</p> <p>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.</p> <p>Click this arrow  to hide the table.</p>

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	"Policies" on page 155

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.


UI Elements (A-Z)	Description
Expected Duration	<p>The estimated time duration of the automation process. The first time the automation is run, the expected duration is 10 minutes.</p> <p>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.</p>
Last Execution	<p>The date and time, or just date, on which the last automation execution ran.</p> <ul style="list-style-type: none"> • 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	<p>The level of risk in the managed automation. Valid values are:</p> <ul style="list-style-type: none"> • 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 66
See also	<ul style="list-style-type: none"> • "Automation Collisions" on page 65 • "Requests for Change" on page 26


User interface elements are described below:

UI Elements	Description
 <Collision exists>	Indicates whether or not the automation is colliding with another automation/RFC.



UI Elements	Description
 <p><Collision does not exist></p>	<p>A collision occurs when a common CI is impacted by more than one automation/RFC running over the same period of time.</p> <p>The collision can be caused due to an automation that is:</p> <ul style="list-style-type: none"> • Colliding with other automations currently running or scheduled to run in Configuration Manager. <p>or</p> <ul style="list-style-type: none"> • Colliding with an RFC that is currently being implemented or scheduled to be implemented in HP Service Manager.
<p>Total Colliding Activities</p>	<ul style="list-style-type: none"> • Colliding Automations <p>Indicates the total number of colliding automations running or scheduled to run in Configuration Manager.</p> <ul style="list-style-type: none"> • Colliding RFCs <p>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.</p> <p>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.</p> <p>For information on how Configuration Manager retrieves RFCs, see "Requests for Change" on page 26.</p>
<p>Total Colliding Activities</p>	<ul style="list-style-type: none"> • Colliding Automations <p>Indicates the total number of colliding automations running or scheduled to run in Configuration Manager.</p> <ul style="list-style-type: none"> • Colliding RFCs <p>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.</p> <p>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.</p> <p>For information on how Configuration Manager retrieves RFCs, see "Requests for Change" on page 26.</p>

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 New RFC Dialog Box

This dialog box enables you to create an RFC for specific CIs, which will be validated in Service Manager.


To access	Select one or more CIs and click  in the Composite CIs pane of the Explore Views module. Click Continue .
Important information	Enter a title and select the relevant information for the RFC that you are creating. By clicking Submit, you are creating an RFC and manually relating it to the selected CIs.
Relevant tasks	"Create an RFC for a Specific CI" on page 69
See also	"Service Manager" on page 189

User interface elements are described below:

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 in the Settings module). For details, see "RFC Creation" on page 188 .
Description	The list of CIs and the required actions that should be performed for each CI.
Impact	Select the widest range of impact that the change will have from the displayed list of values (set in the Settings module). For details, see "RFC Creation" on page 188 .
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 in the Settings module). For details, see "RFC Creation" on page 188 .
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 in the Settings module). For details, see "RFC Creation" on page 188 .

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	Select one or more CIs that breach a policy and click  in the Composite CIs pane of the Explore Views module. Select a policy and click Continue .
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.

UI Elements (A-Z)	Description
Category	Select a category from the displayed list of category values (set in the Settings module). For details, see "RFC Creation" on page 188 .
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 in the Settings module). For details, see "RFC Creation" on page 188 .
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 in the Settings module). For details, see "RFC Creation" on page 188 .
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 in the Settings module). For details, see "RFC Creation" on page 188 .




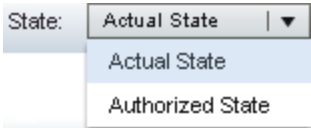




Explore Views Page

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

To access	Select Explorer > Explore Views .
Important information	<p>The Explore Views page includes the following:</p> <ul style="list-style-type: none"> • 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










	<p>run at a future date.</p> <ul style="list-style-type: none"> • Filter pane. In inventory mode, the Filter pane enables you to filter the composite CI list. <p>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.</p>
--	---

User interface elements are described below:

UI Elements (A-Z)	Description
	Click Select View to select a different view to open on the Explore Views page.
	Click to change the display to inventory mode.
	Click to change the display to topology mode.
	<p>Select the state of the view to display:</p> <ul style="list-style-type: none"> • 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.
	<p>Click Export Report to choose a format for the Policy Analysis report data. The available data format options are:</p> <ul style="list-style-type: none"> • Excel. The table data is formatted as an .XLS (Excel) file that can be displayed in a spreadsheet. • PDF. The table data is exported in PDF format. • CSV. The table data is formatted as a comma-separated values (CSV) text file that can be displayed in a spreadsheet. <p>The currently applied filters are taken into account when generating output for reports.</p>
	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.
	Click to create an RFC that remediates the policy breach for the selected changes.
	Click to create an RFC for the highlighted CI.
	Click to open the UCMDB Browser in the context 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 Settings page. For details, see " UI Integrations " on page 191.
	Click Run Automation , which 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.
	Indicates that there are one or more requests for change (RFCs) that are related to this CI.
<List of CIs>	<p>The list displays all CIs currently or previously in the view.</p> <p>Hold the pointer over a CI in the list to display a tooltip containing the name and type of the CI.</p> <p>If no icons appear next to a CI, it indicates that no policies are defined for that CI.</p>

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 Legend to display an explanation of the connections between the nodes in the topology display.

UI Elements (A-Z)	Description
	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 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 Highlight Topology Notes to specify whether to highlight only nodes in the actual state, the authorized state, or both.
	Click Show Topology in Full Screen to display the topology map in the View Topology box.
<Topology Overview Display>	<p>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.</p> <p>Clicking on the policy status indicator in a node displays the policy details for that CI, including the policy name, the source of the policy, and the status of the selected CI for that policy.</p>

Policy Details Pane

User interface elements are described below:








UI Elements (A-Z)	Description
	<p>Click to open the Policy Details dialog box.</p> <p>Note: This button is only active when a baseline rule is selected in the policy list.</p>
Details pane	Displays the details for the policy rule selected in the Policy List pane, including the rule name, description, type, and validation dates.


UI Elements (A-Z)	Description
Policy List pane	Displays all the policy rules defined for the selected CI. For each rule, the name, source of the policy, 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	<p>Displays all automations that ran in the last 24 hours. The automation disappears from the pane 24 hours after it started running.</p> <p>The following data is available for each automation:</p> <ul style="list-style-type: none"> 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. <ul style="list-style-type: none"> 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: <ul style="list-style-type: none">  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

UI Elements (A-Z)	Description
	<p>Automations pane.</p> <p>The following data is available for each automation:</p> <ul style="list-style-type: none"> • 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	<p>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.</p> <p>Available in: Review/Authorize module.</p>
CI Name	<p>Filter the CIs by CI name. Only the selected CIs appear in the view display.</p> <p>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.</p>
CI Type	<p>Filter the CIs by CI type. Only CIs of the selected CI types appear in the view display.</p> <p>Click More... to open a dialog box that enables you to select available CI types from a list.</p>
Has RFCs	<p>Filter according to whether or not the selected CI has an RFC associated with it.</p> <p>Available in: Review/Authorize module.</p>
Managed Status	<p>Filter the CIs by their management status. Only CIs of the selected status appear in the view display.</p> <p>Select Managed or Not Managed.</p>
Policy Name	<p>Filter the CIs by the names of their policies. Only CIs affected by the selected policies appear in the view display.</p> <p>Click More... to open a dialog box that enables you to select available policies from a list.</p>



UI Elements (A-Z)	Description
Policies Status	<p>Filter the CIs by their policy status. Only CIs of the selected status appear in the view display.</p> <p>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.</p> <p>Select In-breach or Satisfied.</p>
Related RFCs	<p>Filter the CIs by specific RFC titles.</p> <p>Click More... to open a dialog box that enables you to select related RFC values from a list.</p> <p>Available in: Review/Authorize module.</p>

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>	<p>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.</p> <p>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.</p>
<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  in the Composite CIs pane.
Relevant tasks	"Create an RFC to Remediate a Policy Breach" on page 68
See also	"Service Manager" on page 189

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.
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.






UI Elements (A-Z)	Description
Authorized By	<p>Displays the name of the user who authorized the snapshots.</p> <p>Use the drop-down list to filter the list to display only snapshots that were authorized by a selected user.</p> <p>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:</p> <ul style="list-style-type: none"> 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. <p>Note: This field appears only for snapshots of the authorized state.</p>
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  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.

UI Elements (A-Z)	Description
	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 85.

Troubleshooting

- **Problem.** Buttons for creating RFCs are disabled.

Possible reasons:

- The Change Management integration has been disabled for the activated configuration.
- The Change Management integration has been defined, saved, and activated, but the user did not log in to Configuration Manager again.

Solution. Do the following:

- Navigate to **Administration > Integrations > Change Management**. To configure the integration, select the check box and provide the details for the Service Manager configuration.
- Save and activate the configuration.
- Log out and then log in again to see the changes take effect.

- **Problem.** RFC creation fails.

- **Reason 1:** Incorrect credentials were defined for the integration user under **Administration > Integrations > Change Management > Service Manager**.

Solution 1: In Service Manager, verify that the integration user exists. If required, update the password (for details, see the Service Manager documentation).

- **Reason 2:** The user does not have the proper credentials to invoke a call to the Service

Manager web-service.

Solution 2: Enable the ability to execute the SOAP API for this integration user (for details, see the Service Manager documentation).

- **Reason 3:** The UNL file for this integration has not been loaded into Service Manager.

Solution 3: To detect if the UNL file has been uploaded, call the following Service Manager URL:

```
<host>:<port example:13080>/sm/7/ucmdcm.wsdl
```

If the call returns an XML file, then a web-service is on, meaning that the UNL file has been uploaded. If not, follow the directions in ["Import a UNL File into Service Manager" on page 112](#)

- **Reason 4:** An RFC has been created with at least one of the following mismatches:

- The service does not exist in Service Manager.
- One or more of the selected CIs does not exist in Service Manager.
- The category value does not match a valid value in Service Manager.
- The risk assessment value does not match a valid value in Service Manager.
- The impact value does not match a valid value in Service Manager.
- The urgency value does not match a valid value in Service Manager.

Solution 4: Change the values for each of the possible mismatches listed above under **Administration > Application Management > RFC > RFC Creation**, so they match with the corresponding values in Service Manager. Save and activate the configuration for the settings to take effect.

- **Problem.** Configuration Manager doesn't display RFC's.

Tip: As a first step in identifying whether the problem is in UCMDB or Service Manager, you can execute a TQL query in UCMDB that fetches all RFCs from Service Manager. If RFCs are expected but do not appear in the query's results, it means that there is an issue with the integration between UCMDB and Service Manager.

To execute this TQL query: log in to UCMDB and navigate to **Modeling > Modeling Studio > Resources** tab (select Queries as the Resource Type) > **Configuration Manager > Configuration Manager – Do not modify > Generate RFC Queries** and execute **amber_rfc_by_id**.

- **Reason 1:** The integration point between UCMDB and Service Manager is either not correctly configured or does not exist.

Solution 1: See the UCMDB documentation for details on how to set up the integration between UCMDB and Service Manager.

- **Reason 2:** An RFC change phase value in the Configuration Manager settings does not match the RFC phase definition in Service Manager.

Solution 2: Change the value for the RFC Change Phase field in the Configuration Manager settings to a valid value (as defined in Service Manager). Navigate to

Administration > Application Management > RFC > Fetch RFCs Criteria > RFC Filters to change the settings. Note that the Change Phases field can contain multiple comma-separated values. Save and activate the configuration for the settings to take effect.

- **Reason 3:** The RFC does not meet the time window condition defined in the Configuration Manager settings for fetching RFCs.

Solution 3: Make sure that the RFC meets the time window condition in the Configuration Manager settings, or change the condition so that the RFC matches the time window. Save and activate the configuration for the settings to take effect.

- **Reason 4:** The date and time format between the integration user used by Configuration Manager for this integration has a different format than the corresponding user in Service Manager.

Solution 4: Make sure that the time format is defined identically for both user instances. In Configuration Manager, the Date Format definition is found under **Administration > Integrations > Change Management > Service Manager > Date Format**.

Chapter 10

Baseline Analysis

This chapter includes:

Baseline Analysis Overview	95
Define a Configuration Model for Comparison	96
Baseline Analysis User Interface	97

Baseline Analysis Overview

The Baseline Analysis 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 Baseline Analysis module, see "[Baseline Analysis Page](#)" on page 98.

Note:


- You must have View CIs permission to work with this module.
- You can only select CIs from views for which you have View, Authorize, or Manage permission

Define a Configuration Model for Comparison





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

1. Navigate to **Analysis > Baseline Analysis**. 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  **Suggest Baseline** in the main Baseline Analysis 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 model from a managed CI**.
 - To create a model based on a policy that you created in the Policies module, click **Select predefined configuration**  in the Configuration Model pane and select **Create model from an 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. For a list of the operators used to define attribute conditions, see "Attribute Operators" on page 166.
 3. Click **Analyze**  in the main toolbar to run the comparison.


Baseline Analysis User Interface

This section includes (in alphabetical order):

Add Composite CIs Dialog Box	97
Select Composite CI Dialog Box	97
Select Baseline Policy Dialog Box	98
Baseline Analysis Page	98
Comparison Details Dialog Box	101

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 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.

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  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 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.

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  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.

Baseline Analysis Page

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







To access	Select Analysis > Baseline Analysis .
Important information	<p>The Baseline Analysis page includes the following panes:</p> <ul style="list-style-type: none"> • Analysis Results • Analysis Scope • Configuration Model <p>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.</p> <p>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.</p>

UI Elements (A-Z)	Description
	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: <ul style="list-style-type: none"> • 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	The names of the attributes of the selected CI type.



UI Elements (A-Z)	Description
column	
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 166.

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.

UI Elements (A-Z)	Description
<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.

Chapter 11

Segmentation Analysis

This chapter includes:

Segmentation Analysis Overview	103
Select CIs that Contain Groups of Similar CIs	103
Segmentation Analysis User Interface	104

Segmentation Analysis Overview

The 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 Baseline Analysis module, or use the CIs that it contains as the basis for a different model.


For details on the Segmentation Analysis module, see "Segmentation Analysis Page" on page 105.

Note:


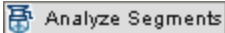

- You must have View CIs permission to work with this module.
- Only views for which you have View permission are displayed.

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 **Analysis > 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** . (missing or bad snippet) This takes you to the Baseline Analysis module, with the selected segment being used as the model.

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


Segmentation Analysis User Interface

This section includes (in alphabetical order):

Add Composite CIs Dialog Box	104
CI Details Dialog Box	105
Segmentation Analysis Page	105
Segmentation Parameters Dialog Box	108

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 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.



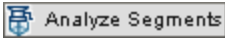
Segmentation Analysis Page

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

To access	Select Analysis > Segmentation Analysis .
-----------	---

<p>Important information</p>	<p>The Segmentation Analysis page includes the following panes:</p> <ul style="list-style-type: none"> • Analysis Scope • Segments List and Results (in chart format) • Configuration Model <p>Select the composite CIs from which to create segments in the Analysis Scope pane. When you are finished, click Analyze Segments.</p> <p>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 Analyze Segments again to re-create the groups.</p>
-------------------------------------	---





User interface elements are described below:

UI Elements (A-Z)	Description
	<p>Click Create New Model to clear all selected values and segments.</p>
	<p>Click Parameters to open the Segmentation Parameters dialog box. For details, see "Explore Views Page" on page 83</p>
	<p>Click Analyze Segments to create segments based on the selected CIs.</p>

Analysis Scope Pane

<p>Important information</p>	<p>In this pane, you select the composite CIs to be used for creating the segments.</p>
-------------------------------------	---

User interface elements are described below:

UI Elements (A-Z)	Description
	<p>Click Add composite CI to select composite CIs to add to the Analysis Scope. For details, see "CI Details Dialog Box" on the previous page.</p>
	<p>Click Remove composite CI from list to delete the selected composite CI from the Analysis Scope.</p>
	<p>Click Remove all composite CIs to delete all managed CIs from the Analysis Scope.</p>
	<p>Click Show CI details to open the CI Details dialog box. For details, see "CI Details Dialog Box" on the previous page.</p>
<p><Composite CI Name></p>	<p>The names of the composite CIs in the Analysis Scope.</p>
<p>Segment ID</p>	<p>Displays the name of the segment to which the composite CI was assigned.</p>

UI Elements (A-Z)	Description
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.
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 166 .

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 Baseline Analysis page, where you can edit the model and save it. (missing or bad snippet)
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 166 .

Chapter 12

Review/Authorize

This chapter includes:

Review/Authorize Overview	109
Integration with Service Manager	110
Reports	111
Authorize Changes to CIs	111
Import a UNL File into Service Manager	112
Launch External Applications	113
Review/Authorize User Interface	113
Troubleshooting	124

Review/Authorize Overview

The Review/Authorize module enables you to review and authorize changes in a view. Review/Authorize 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 119](#).

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 111](#).

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 149](#).

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 Review/Authorize module:

- View permits you to select and review changes.
- Authorize 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 ServiceManagerAdapter9.x 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 112.

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
- CI that had previous relations

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.

For details about creating RFCs, see the following topics:

- ["Create an RFC for a Specific CI" on page 69](#)
- ["Create an RFC to Remediate a Policy Breach" on page 68](#)
- ["Create RFC for Rolling Back Changes Dialog Box" on page 115](#)

Reports

Configuration Manager provides the ability to export policy information for a view, including information about CIs that are in breach of defined policies. Causes of in-breach CIs might be:

- CIs that do not satisfy a baseline condition.
- Missing CIs.
- Additional CIs in a composite CI.

Note: Information about breaching CIs is not included in reports that are exported in .pdf format.

The report compares the policy status of the CIs between two states of a view. Detailed information is displayed when there is a breach in at least one of the states, down to the attribute level. The report lists the causes of the policy breaches, and the status of the breaching CI or attribute in each state.

Authorize Changes to CIs

This task describes how to authorize changes to composite CIs.



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 Review/Authorize 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 115.

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.

Caution: Do not perform this procedure when using a version of Service Manager later than 9.30.

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.

Launch External Applications

Configuration Manager now provides a mechanism to configure a generic UI integration that can launch any application user interface in the context of a UCMDB CI or a UCMDB view. For example, you can launch the HP Enterprise Collaboration user interface in order to open a new discussion related to an issue that may have been found on some CI, or launch UCMDB to view the CI properties of the selected CI). This functionality is available in the Review/Authorize and the Explore Views modules.

Note: In order to be able to integrate with external applications, it is recommended that all applications be configured with LW-SSO and work with the same user management system. This prevents the need to enter a user name and login for each external application.


To launch external applications:

1. Specify the URL of the application that you want to open. For example:

```
http://<UCMDB server machine or IP address>:8080/ucmdb-ui/cms/  
directAppletLogin.do?cmd=ShowProperties&objectId=  
${ucmdbId}&navigation=false&interfaceVersion=9.0.0
```

For this example, `${ucmdbId}` is replaced with the ID of the selected composite CI (as it appears in UCMDB).

For details, see "UI Integrations" on page 191.

Note: You must perform this step for the  icon to be visible.

2. In the Review/Authorize or the Explore Views module, click .

The application that you configured opens in a browser window.


Review/Authorize User Interface

This section includes (in alphabetical order):

Authorize Selected Differences Dialog Box	114
CI Details Dialog Box	114
Create RFC for Rolling Back Changes Dialog Box	115
Policy Details Dialog Box	116
Sort CIs Dialog Box	117
Review/Authorize Page	118
View Topology Dialog Box	123

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 Review/Authorize page.
Important information	<p>By clicking Submit, you are authorizing the proposed changes. This transforms the actual state of the CI into its new authorized state.</p> <p>If the Change Management integration enabled check box in the 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.</p> <p>Note: You cannot authorize a CI whose parent CI is not contained in the view.</p>
See also	"Change Management" on page 184

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




UI Elements (A-Z)	Description
<List of CIs with proposed changes>	<p>The list of changes that were displayed for authorization in the Composite CIs pane.</p> <p>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.</p>


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.

UI Elements (A-Z)	Description
	Indicates a difference between the value in the two states displayed.
Attributes tab	<p>The left pane displays the CI name. For composite CIs, you can expand a CI entry to display the individual component CIs.</p> <p>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.</p>
Incoming Relationships tab	<p>Displays all the relationships of the selected CI in the incoming direction.</p> <p>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.</p>
Outgoing Relationships tab	<p>Displays all the relationships of the selected CI in the outgoing direction.</p> <p>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.</p>

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	Select one or more CIs and click  in the Composite CIs pane of the Review/Authorize module.
Important information	<p>Enter a title and select the relevant information for the RFC that you are creating for the unplanned change.</p> <p>By clicking Submit, you are creating an RFC and manually relating it to the selected CIs.</p>
Relevant tasks	"Authorize Changes to CIs" on page 111
See also	"Service Manager" on page 189


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 in the Settings module). For details, see "RFC Creation" on page 188 .



UI Elements (A-Z)	Description
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 in the Settings module). For details, see "RFC Creation" on page 188.
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 in the Settings module). For details, see "RFC Creation" on page 188.
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 in the Settings module). For details, see "RFC Creation" on page 188.

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







UI Elements (A-Z)	Description
	<p>each CI for which there is a baseline value, an icon indicates whether it is in breach of the policy or not.</p> <p>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.</p>
<Right pane>	<p>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.</p>

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.
Selected Sort Fields	The selected fields by which to sort the CIs. The sort order follows the order of the list.


Review/Authorize 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 Changes > Review/Authorize .
Important information	<p>The Review/Authorize page includes the following panes:</p> <ul style="list-style-type: none"> • 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. 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 88. <p>Select the changes to authorize by clicking the check boxes next to the relevant CIs in the Composite CIs pane.</p>













User interface elements are described below:





UI Elements (A-Z)	Description
	Click Select View to select a different view to open on the Review/Authorize page.
	Click to change the display to inventory mode.
	Click to change the display to topology mode.
	<p>Click Export Report to choose a report to export and the export format for the data.</p> <p>The available reports are:</p> <ul style="list-style-type: none"> • Change Report • Policy Analysis Report <p>The available format options are:</p> <ul style="list-style-type: none"> • Excel. The table data is formatted as an .XLS (Excel) file that can be displayed in a spreadsheet.

UI Elements (A-Z)	Description
	<ul style="list-style-type: none"> • 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. <p>The currently applied filters are taken into account when generating output for reports.</p>
	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 <input type="text" value=""/>	Click <input type="text" value=""/> 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 Settings page. For details, see " UI Integrations " on page 191.
	Click to create an RFC for the highlighted CI.
	Click to create a rollback RFC selected changes.
	Click to open the UCMDB Browser in the context 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 actual state.

UI Elements (A-Z)	Description
	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.
	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>	<p>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.</p> <p>Hold the pointer over a CI in the list to display a tooltip containing the name and type of the CI.</p> <p>If no icons appear after a CI, it indicates that no changes have occurred to that CI.</p> <p>Click the check box next to a selected change to mark it for authorization.</p>

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	<p>The left pane displays the CI name and the change type icon. For composite CIs, the component CIs with changed attributes are displayed.</p> <p>The right pane displays the attribute names and actual and authorized values for the CI selected in the left pane.</p>
Changed Outgoing Relationships tab	<p>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.</p> <p>The right pane displays the source, target, and direction for the relationship selected in the left pane.</p>

UI Elements (A-Z)	Description
<p>Policy Details tab</p>	<p>In the Policy List pane, the following data is displayed for each policy rule:</p> <ul style="list-style-type: none"> • the policy rule name • the external product, if any, that is the source of the policy. • the rule status in the actual state • the rule status in the authorized state • the related CI <p>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.</p> <p>Note: The status bar does not appear for federated policies that contain CIs in the authorized state.</p>
<p>Related RFCs tab</p>	<p>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.</p> <p>The right pane displays the properties for the RFC ID selected in the left pane.</p> <p>Note: When the offline process runs, it discovers only the following RFCs for the CIs in a view:</p> <ul style="list-style-type: none"> • having a state that is specified in the Fetched RFC Criteria settings • with a planned start date is later than today minus X days (as defined in the settings) • with a planned end date earlier than today. <p>Therefore, if an RFC is attached to multiple CIs, not all of the CIs may be shown as connected to the RFC if they do not match these criteria.</p>

Filter Pane


User interface elements are described below:










UI Elements (A-Z)	Description
<p>Changed CIs</p>	<p>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.</p> <p>Available in: Review/Authorize module.</p>

UI Elements (A-Z)	Description
CI Name	<p>Filter the CIs by CI name. Only the selected CIs appear in the view display.</p> <p>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.</p>
CI Type	<p>Filter the CIs by CI type. Only CIs of the selected CI types appear in the view display.</p> <p>Click More... to open a dialog box that enables you to select available CI types from a list.</p>
Has RFCs	<p>Filter according to whether or not the selected CI has an RFC associated with it.</p> <p>Available in: Review/Authorize module.</p>
Managed Status	<p>Filter the CIs by their management status. Only CIs of the selected status appear in the view display.</p> <p>Select Managed or Not Managed.</p>
Policy Name	<p>Filter the CIs by the names of their policies. Only CIs affected by the selected policies appear in the view display.</p> <p>Click More... to open a dialog box that enables you to select available policies from a list.</p>
Policies Status	<p>Filter the CIs by their policy status. Only CIs of the selected status appear in the view display.</p> <p>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.</p> <p>Select In-breach or Satisfied.</p>
Related RFCs	<p>Filter the CIs by specific RFC titles.</p> <p>Click More... to open a dialog box that enables you to select related RFC values from a list.</p> <p>Available in: Review/Authorize module.</p>

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


UI Elements (A-Z)	Description
	Display.
	Click Legend to display an explanation of the connections between the nodes in the topology 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 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 Highlight Topology Notes to specify whether to highlight only nodes in the actual state, the authorized state, or both.
	Click Show Topology in Full Screen to display the topology map in the View Topology box.
<Topology Overview Display>	<p>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.</p> <p>Clicking on the policy status indicator in a node displays the policy details for that CI, including the policy name, the source of the policy, and the status of the selected CI for that policy.</p>

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
	<p>Click the small arrow next to the Highlight Topology Nodes button to open the menu.</p> <p>Select the display mode for the map:</p> <ul style="list-style-type: none"> • Highlight Actual State • Highlight Authorized State • Highlight Both
<p><Topology pane toolbar buttons></p>	<p>The toolbar buttons from the Topology pane are also available in the View Topology dialog box. For details, see "Topology Pane" on page 85.</p>

Troubleshooting

- **Problem.** Buttons for creating RFCs are disabled.

Possible reasons:

- The Change Management integration has been disabled for the activated configuration.
- The Change Management integration has been defined, saved, and activated, but the user did not log in to Configuration Manager again.

Solution. Do the following:

- a. Navigate to **Administration > Integrations > Change Management**. To configure the integration, select the check box and provide the details for the Service Manager configuration.
- b. Save and activate the configuration.
- c. Log out and then log in again to see the changes take effect.

- **Problem.** RFC creation fails.

- **Reason 1:** Incorrect credentials were defined for the integration user under **Administration > Integrations > Change Management > Service Manager**.

Solution 1: In Service Manager, verify that the integration user exists. If required, update the password (for details, see the Service Manager documentation).

- **Reason 2:** The user does not have the proper credentials to invoke a call to the Service Manager web-service.

Solution 2: Enable the ability to execute the SOAP API for this integration user (for details, see the Service Manager documentation).

- **Reason 3:** The UNL file for this integration has not been loaded into Service Manager.

Solution 3: To detect if the UNL file has been uploaded, call the following Service Manager URL:

<host>:<port example:13080>/sm/7/ucmdcm.wsdl

If the call returns an XML file, then a web-service is on, meaning that the UNL file has been uploaded. If not, follow the directions in ["Import a UNL File into Service Manager" on page 112](#)

■ **Reason 4:** An RFC has been created with at least one of the following mismatches:

- The service does not exist in Service Manager.
- One or more of the selected CIs does not exist in Service Manager.
- The category value does not match a valid value in Service Manager.
- The risk assessment value does not match a valid value in Service Manager.
- The impact value does not match a valid value in Service Manager.
- The urgency value does not match a valid value in Service Manager.

Solution 4: Change the values for each of the possible mismatches listed above under **Administration > Application Management > RFC > RFC Creation**, so they match with the corresponding values in Service Manager. Save and activate the configuration for the settings to take effect.

■ **Problem.** Configuration Manager doesn't display RFC's.

Tip: As a first step in identifying whether the problem is in UCMDB or Service Manager, you can execute a TQL query in UCMDB that fetches all RFCs from Service Manager. If RFCs are expected but do not appear in the query's results, it means that there is an issue with the integration between UCMDB and Service Manager.

To execute this TQL query: log in to UCMDB and navigate to **Modeling > Modeling Studio > Resources** tab (select Queries as the Resource Type) > **Configuration Manager > Configuration Manager – Do not modify > Generate RFC Queries** and execute `amber_rfc_by_id`.

- **Reason 1:** The integration point between UCMDB and Service Manager is either not correctly configured or does not exist.

Solution 1: See the UCMDB documentation for details on how to set up the integration between UCMDB and Service Manager.

- **Reason 2:** An RFC change phase value in the Configuration Manager settings does not match the RFC phase definition in Service Manager.

Solution 2: Change the value for the RFC Change Phase field in the Configuration Manager settings to a valid value (as defined in Service Manager). Navigate to **Administration > Application Management > RFC > Fetch RFCs Criteria > RFC Filters** to change the settings. Note that the Change Phases field can contain multiple comma-separated values. Save and activate the configuration for the settings to take effect.

- **Reason 3:** The RFC does not meet the time window condition defined in the Configuration Manager settings for fetching RFCs.

Solution 3: Make sure that the RFC meets the time window condition in the Configuration Manager settings, or change the condition so that the RFC matches the time window. Save and activate the configuration for the settings to take effect.

- **Reason 4:** The date and time format between the integration user used by Configuration Manager for this integration has a different format than the corresponding user in Service Manager.

Solution 4: Make sure that the time format is defined identically for both user instances. In Configuration Manager, the Date Format definition is found under **Administration > Integrations > Change Management > Service Manager > Date Format**.

Changes History

This chapter includes:

Changes History Overview	127
Reports	127
Compare Snapshots	128
Changes History User Interface	128

Changes History 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 Changes History module enables you to display a comparison of two snapshots of a view in the actual state. This 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 143.

Note: You must have one of the following permissions to access the Changes History module:

- View permits you to select views.
- Authorize permits you to select views and save a snapshot.

Reports

Configuration Manager provides the ability to export policy information for a view, including information about CIs that are in breach of defined policies. Causes of in-breach CIs might be:

- CIs that do not satisfy a baseline condition.
- Missing CIs.
- Additional CIs in a composite CI.


Note: Information about breaching CIs is not included in reports that are exported in .pdf format.

The report compares the policy status of the CIs between two points in time. Detailed information is displayed when there is a breach in at least one of the states, down to the attribute level. The report lists the causes of the breaches, and the status of the breaching CI or attribute at each point in time.

Compare Snapshots

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

To compare snapshots:

1. In the Changes History module, 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.


Changes History User Interface

This section includes (in alphabetical order):

CI Details Dialog Box	128
Policy Details Dialog Box	129
Changes History Page	130
Select Snapshot to View Dialog Box	134
Sort CIs Dialog Box	135
Topology Page	136




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



UI Elements (A-Z)	Description
	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>	<p>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.</p> <p>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.</p>
<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.

Changes History Page

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










To access	Select Changes > Changes History .
Important information	<p>The Changes History page includes the following panes:</p> <ul style="list-style-type: none"> • 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. <ul style="list-style-type: none"> 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 88.

User interface elements are described below:

UI Elements (A-Z)	Description
	Click Select View to select a different view to open on the Changes History page.
	Click to change the display to inventory mode.
	Click to change the display to topology mode.
<p data-bbox="282 531 526 594"><Compare between snapshots></p> 	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.
	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: <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • Excel. The table data is formatted as an .XLS (Excel) file that can be displayed in a spreadsheet. • PDF. The table data is exported in PDF format. • CSV. The table data is formatted as a comma-separated values (CSV) text file that can be displayed in a spreadsheet. The currently applied filters are taken into account when generating output for reports.
	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 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>	<p>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.</p> <p>Hold the pointer over a CI in the list to display a tooltip containing the name and type of the CI.</p> <p>If no icons appear after a CI, it indicates that no changes have occurred to that CI.</p>

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	<p>The left pane displays the CI name and change type icon. For composite CIs, the component CIs with changed attributes are displayed.</p> <p>The right pane displays the names and the primary and secondary snapshot attribute values for the CI selected in the left pane.</p>
Changed Outgoing Relationships tab	<p>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.</p> <p>The right pane displays the source, target, and direction for the relationship selected in the left pane.</p>
Policy Details tab	<p>In the Policy List pane, the following data is displayed for each policy rule:</p> <ul style="list-style-type: none"> • the policy rule name • the rule status in the primary snapshot (Status) • the rule status in the secondary snapshot (Previous Status) • the related CI <p>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.</p>
Related RFCs tab	<p>The left pane displays the request for change ID and the related CI.</p> <p>The right pane displays details of the request for change.</p> <p>The left pane displays the RFC IDs that are related to the selected CI, as well as the title and relation type. When an RFC ID is selected in the left pane, its properties are displayed in the right pane.</p>

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 Legend to display an explanation of the connections between the nodes in the topology display.

UI Elements (A-Z)	Description
	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 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 Highlight Topology Notes to specify whether to highlight only nodes in the actual state, the authorized state, or both.
	Click Show Topology in Full Screen to display the topology map in the View Topology box.
<Topology Overview Display>	<p>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.</p> <p>Clicking on the policy status indicator in a node displays the policy details for that CI, including the policy name, the source of the policy, and the status of the selected CI for that policy.</p>

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 128

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	<p>Displays the name of the user who authorized the snapshots.</p> <p>Use the drop-down list to filter the list to display only snapshots that were authorized by a selected user.</p> <p>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:</p> <ul style="list-style-type: none"> 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. <p>Note: This field appears only for snapshots of the authorized state.</p>
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.


UI Elements (A-Z)	Description
	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
	Click the small arrow next to the Highlight Topology Nodes button to open the menu. Select the display mode for the map: <ul style="list-style-type: none"> • 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 85.

Chapter 14

Authorization History

This chapter includes:

Authorization History Overview	137
Reports	137
Compare Snapshots	138
Authorization History User Interface	138

Authorization History 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 Authorization History module enables you to display a comparison of two snapshots of a view in the actual state. This 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 143.

Note: You must have one of the following permissions to access the Authorization History module:

- View permits you to select views.
- Authorize permits you to select views and save a snapshot.

Reports

Configuration Manager provides the ability to export policy information for a view, including information about CIs that are in breach of defined policies. Causes of in-breach CIs might be:

- CIs that do not satisfy a baseline condition.
- Missing CIs.
- Additional CIs in a composite CI.


Note: Information about breaching CIs is not included in reports that are exported in .pdf format.

The report compares the policy status of the CIs between two points in time. Detailed information is displayed when there is a breach in at least one of the states, down to the attribute level. The report lists the causes of the breaches, and the status of the breaching CI or attribute at each point in time.

Compare Snapshots

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

To compare snapshots:

1. In the Authorization History module, 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.


Authorization History User Interface

This section includes (in alphabetical order):





CI Details Dialog Box	138
Policy Details Dialog Box	139
Authorization History Page	140
Select Snapshot to View Dialog Box	143
Sort CIs Dialog Box	144
Topology Page	145

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	<p>The left pane displays the CI name. For composite CIs, you can expand a CI entry to display the individual component CIs.</p> <p>The right pane displays the attribute names and values for this CI. The attribute values of the two compared snapshots are displayed.</p>
Incoming Relationships tab	<p>Displays all the relationships of the selected CI in the incoming direction.</p> <p>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.</p>
Outgoing Relationships tab	<p>Displays all the relationships of the selected CI in the outgoing direction.</p> <p>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.</p>

Policy Details Dialog Box

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

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

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>	<p>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.</p> <p>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.</p>
<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.

Authorization History Page

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










To access	Select Changes > Authorization History .
Important information	<p>The Authorization History page includes the following panes:</p> <ul style="list-style-type: none"> • 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 85. <p>Note: In inventory mode, the Topology pane is called Related CIs.</p> <ul style="list-style-type: none"> • 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 88.

User interface elements are described below:

UI Elements (A-Z)	Description
	Click Select View to select a different view to open on the Changes History page.
	Click to change the display to inventory mode.
	Click to change the display to topology mode.
<p data-bbox="282 531 527 594"><Compare between snapshots></p> 	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.
	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: <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • Excel. The table data is formatted as an .XLS (Excel) file that can be displayed in a spreadsheet. • PDF. The table data is exported in PDF format. • CSV. The table data is formatted as a comma-separated values (CSV) text file that can be displayed in a spreadsheet. The currently applied filters are taken into account when generating output for reports.
	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 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>	<p>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.</p> <p>Hold the pointer over a CI in the list to display a tooltip containing the name and type of the CI.</p> <p>If no icons appear after a CI, it indicates that no changes have occurred to that CI.</p>

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	<p>The left pane displays the CI name and change type icon. For composite CIs, the component CIs with changed attributes are displayed.</p> <p>The right pane displays the names and the primary and secondary snapshot attribute values for the CI selected in the left pane.</p>
Changed Outgoing Relationships tab	<p>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.</p> <p>The right pane displays the source, target, and direction for the relationship selected in the left pane.</p>
Policy Details tab	<p>In the Policy List pane, the following data is displayed for each policy rule:</p> <ul style="list-style-type: none"> • the policy rule name • the rule status in the primary snapshot (Status) • the rule status in the secondary snapshot (Previous Status) • the related CI <p>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.</p>
Related RFCs tab	<p>The left pane displays the request for change ID and the related CI.</p> <p>The right pane displays details of the request for change.</p> <p>The left pane displays the RFC IDs that are related to the selected CI, as well as the title and relation type. When an RFC ID is selected in the left pane, its properties are displayed in the right pane.</p>

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 128

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	<p>Displays the name of the user who authorized the snapshots.</p> <p>Use the drop-down list to filter the list to display only snapshots that were authorized by a selected user.</p> <p>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:</p> <ul style="list-style-type: none"> 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. <p>Note: This field appears only for snapshots of the authorized state.</p>
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.


UI Elements (A-Z)	Description
	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
	<p>Click the small arrow next to the Highlight Topology Nodes button to open the menu.</p> <p>Select the display mode for the map:</p> <ul style="list-style-type: none"> • 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 85.

Chapter 15

Views

This chapter includes:

Views Overview	146
Topology Views and Inventory Views	147
View Refresh Rate	148
Automatic State Transition	149
Add a View to be Managed	150
Set Automatic State Transition Rules for a View	150
Specify the View Refresh Rate	151
Views User Interface	151
Troubleshooting and Limitations	154

Views Overview

To begin working in Configuration Manager, you select views, which are defined in 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 Views 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 148.

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. For details, see "[Specify the View Refresh Rate](#)" on page 151.

Note: You must have Authorize or Manage permission on at least one view to access the Views module.

- Authorize permission on a specific view enables you to see and modify that view.
- Manage permission on a specific view enables you to manage and unmanage that view.

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 153.
- **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 149.

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 Review/Authorize and the other modules.

For details on adding a view to the managed views list, see "[Add a View to be Managed](#)" on page 150.

Out-of-the-Box Views

Note: A license exists for this feature. Ask your system administrator to purchase the necessary license.

Configuration Manager comes with a group of out-of-the-box views that are available for use in UCMDB, ready for you to manage. These views are located in UCMDB in the following location: **Modeling Studio > Resources** tab (select **Views** as the resource type) > **Configuration Manager > Configuration Manager - Do not modify > Automanaged Views** folder.

There are several types of these views:

- All servers – you can manage a view that automatically contains either all Windows servers or all UNIX servers.
- Virtualized or non-virtualized clusters – you can manage a view that contains only non-HACMP, J2EE, MS, Oracle RAC, Service Guard, Sun, or Veritas machines.

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

The Explore Views, Review/Authorize, Changes History, and Authorization History 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	<ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> ▪ 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	<ul style="list-style-type: none"> • 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 ["Specify the View Refresh Rate"](#) on page 151.

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 Views 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 153.
5. Optionally, set automatic state transition conditions for the view. For details, see "[Set Automatic State Transition Rules for a View](#)" below.
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 Views 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 the previous page.
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** (missing or bad snippet) 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 Views 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 111.

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

Specify the View Refresh Rate

1. Navigate to **Views**.
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 **Administration > Settings > Application Management > Offline Analysis and Authorization > Daily View Refresh Settings**.

Tip: As much as possible, schedule the offline analysis to run at a time that discovery processes on UCMDB are not running, to prevent degradation in performance.

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

Views User Interface

This section includes:

Views Page	151
------------------	-----








Views Page

This page displays the list of views currently being managed.

To access	Select Views .
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	<ul style="list-style-type: none"> • "Add a View to be Managed" on page 150 • "Set Automatic State Transition Rules for a View" on page 150

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 147 .

Delete Candidate Policy Pane

UI Elements (A-Z)	Description
Delete CIs marked as candidates for deletion from Actual State (override UCMDDB aging mechanism)	When the check box is selected, CIs marked as candidates for deletion in UCMDDB 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 UCMDDB.

Automatic State Transition Pane

Relevant tasks	"Set Automatic State Transition Rules for a View" on page 150
-----------------------	---

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

UI Elements (A-Z)	Description
<Criteria List>	<p>The following criteria are used to set the automatic state transition rules:</p> <ul style="list-style-type: none"> • 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. (missing or bad snippet) <ul style="list-style-type: none"> 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: <ul style="list-style-type: none"> ▪ 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: <ul style="list-style-type: none"> ▪ 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

UI Elements (A-Z)	Description
	<p>RFCs on CI.</p> <p>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.</p>
Enable automatic state transition	<p>Select this check box to activate the fields in the Automatic State Transition pane. The following options are available:</p> <ul style="list-style-type: none">• 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	<p>After selecting automatic state transition settings, click Test Configuration to check if the view contains changes matching the conditions set for authorization.</p>

Troubleshooting and Limitations

The following limitations are applicable when working with managed views in Configuration Manager:

- Views that contain federated TQL queries cannot be selected for addition to the managed views list.
- If a view contains a node with a date restriction, you will see updated data for this view only if it is configured to be updated once per day (not each time the view is updated). To see updated data for such a view, use the JMX console to manually refresh the view.

Chapter 16

Policies

This chapter includes:

Policies Overview	155
Baselining	157
Policy Groups	157
Define a Baseline or Topology Policy	157
Define a Similarity Policy	158
Configuration Manager Topology Policy - Use Case	158
Configuration Manager Similarity Policy - Use Cases	163
Policies User Interface	166
Troubleshooting and Limitations	173

Policies Overview

A 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 Policies module controls the policy groups and policies you define for the managed views. There are three types of 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.

Detailed information about the CIs in baseline policies can be seen in the Explore Views, Review/Authorize changes, Changes History, and Authorization History modules.

- **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).

You are not able to view detailed information about the CIs in topology policies.

- **Similarity policies**

In a **similarity policy**, you select CIs and attributes that enforce similarity between either all CIs of a certain type in a view, or groups of CIs in a view (where each group is connected to a defined CIT). For instance, you could define a similarity policy stating that all UNIX machines in a lab, which are connected to an Oracle database, must have the same OS version. Another example is to specify that all servers in each cluster are running the same application version.

A similarity policy is not static (it has neither a fixed number of components nor set attribute values, unlike a baseline policy). You choose attributes and/or components without specifying any value. The policy calculation compares the current values or components among all of the compared CIs (or the CIs in each group, if grouping has been selected), and decides the policy status accordingly - either all of the compared CIs satisfy the policy, or they all breach the policy.

Detailed information about the CIs in similarity policies can be seen in the Explore Views (on the latest snapshot only) and Review/Authorize changes modules.

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

- **Validity.** Set the time period for which the policy is valid
- **Filter.** Limit 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.

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

In addition, UCMDB provides, out of the box, a group of out-of-the-box policies to be used in Configuration Manager. For details, see ["Policies" on page 15](#).

For details on defining policies, see ["Policies Page" on page 167](#).

Note:

- You must have Policies Admin permission to work with this module.
- You must also have one of the following permissions:
 - Authorize permits you to assign or remove a policy from a view.
 - View permits you to preview a policy or create a baseline policy from a managed CI (included in Authorize).

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 "[Policies Page](#)" on page 167.

Define a Baseline or Topology Policy



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

1. Click the **Add Policy** button  in the Policies toolbar and select one of the following:
 - Add Baseline Policy
 - Add Topology Policy
2. In the General area of the Details pane, enter the policy name and description.
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. Do one of the following:
 - For baseline policies, define a baseline CI and its attributes in the Baseline area of the Details pane.
 - For topology policies, set the condition type and condition TQL in the Condition area of the Details pane.
7. When you are finished, click the **Save** button  in the Policies toolbar to save your policy.

Define a Similarity Policy

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

1. Click the **Add Policy** button  in the Policies toolbar and select Add Similarity Policy.
2. In the General area of the Details pane, enter the policy name and description.
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. Do one of the following:
 - If you want to allow the grouping of related configurations, select the **Enable grouping by CI type and pattern** check box. Then select the grouping CI type and the related TQL query (pattern) to be used for creating the grouping.
 - If you do not want to enable grouping, make sure the **Enable grouping by CI type and pattern** check box is not selected. In the Comparison Scope pane, select the CI type of the CIs to be tested against the policy.
6. In the Similarity Criteria area, specify the CI types and attributes to be compared.
7. When you are finished, click the **Save** button  in the Policies toolbar to save your policy.

Configuration Manager Topology Policy - Use Case

This section describes a use case for a topology policy in Configuration Manager.

This scenario includes the following steps:

- ["Background" on the next page](#)
- ["Create the Condition TQL Query in UCMDB" on the next page](#)
- ["Define the Topology Policy in Configuration Manager" on page 162](#)

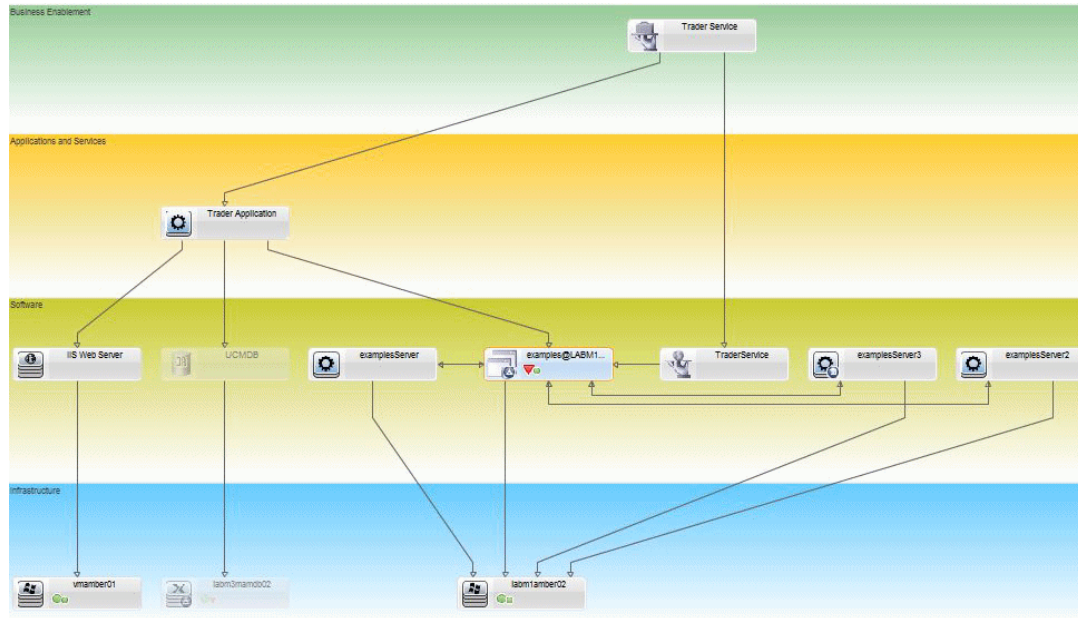
1. Background

A trader service owner needs to continually monitor the high-availability and/or resiliency of his service. The service is based on a J2EE Cluster that contains several Web Logic servers. Each server runs on a Windows host.

The service owner has determined that the cluster supporting this configuration requires a minimum of three physical hosts to provide sufficient coverage and responsiveness for the applications running. As a result, it is important to ensure that when changes occur, the proper level of resources is maintained to guarantee that the service continues to function in accordance with its agreed to requirements.

Toward this end, the service owner wants to define a Configuration Manager topology policy that monitors the number of hosts supporting the cluster. The owner would like to see an indication in the event that the number of hosts in the cluster supporting the service is less than three.

The service topology is modeled in a view in UCMDB and there is a corresponding managed view in Configuration Manager. The following image displays the service topology in Configuration Manager.

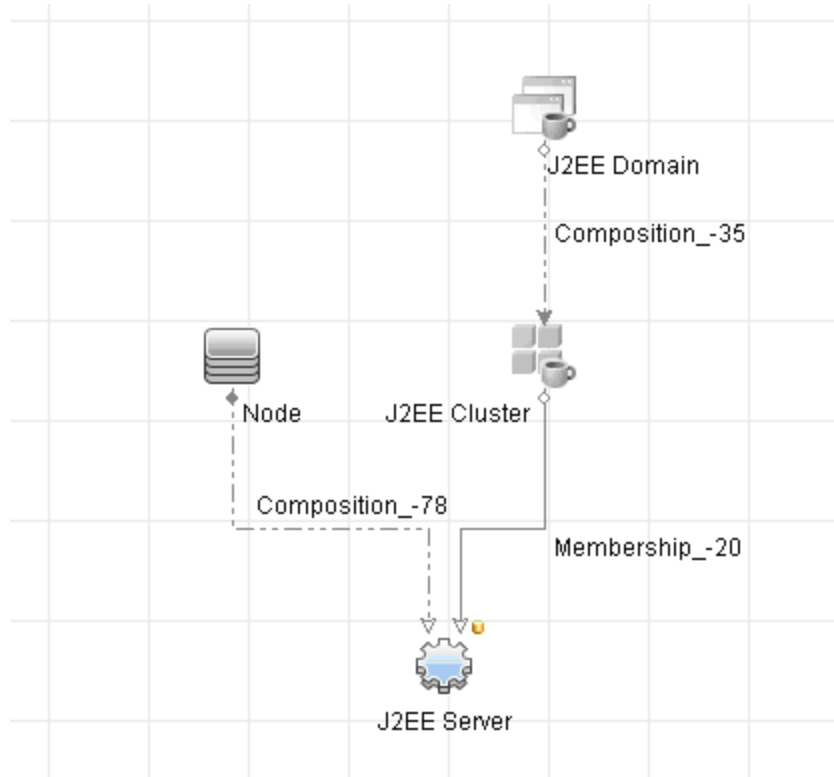


2. Create the Condition TQL Query in UCMDB

Open the UCMDB window (click the **UCMDB Foundation**  icon, and log in).


Navigate to the **Modeling Studio**. Select **Views** as the resource in the Resources tab and locate the **Trader** view. Double-click the view to open it. This view contains the relationships that define the connection between the J2EE domain and the Windows hosts.

The following image displays the relevant portion of the view in UCMDB:

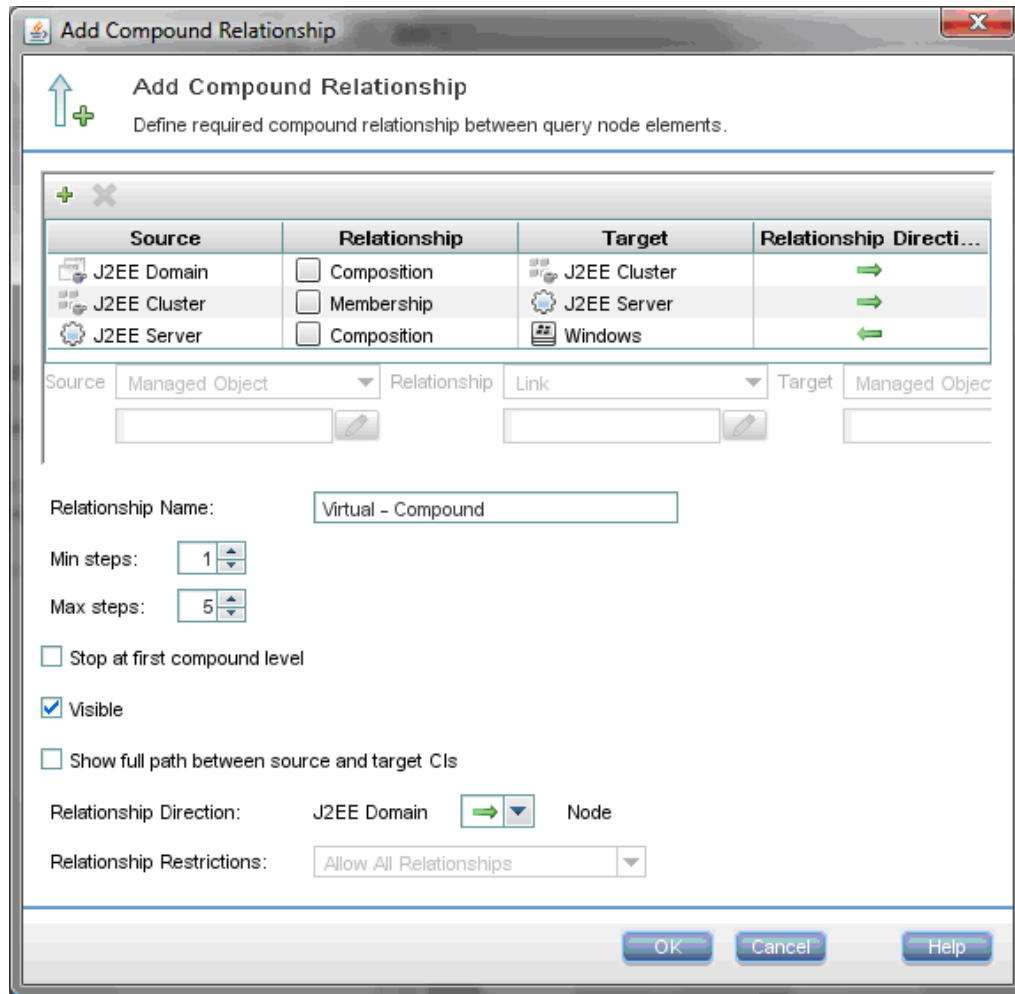


Using the relationship path between the J2EE domain and the Node CI, create a new query consisting of a compound relationship between the J2EE Domain and the host (Node CI).

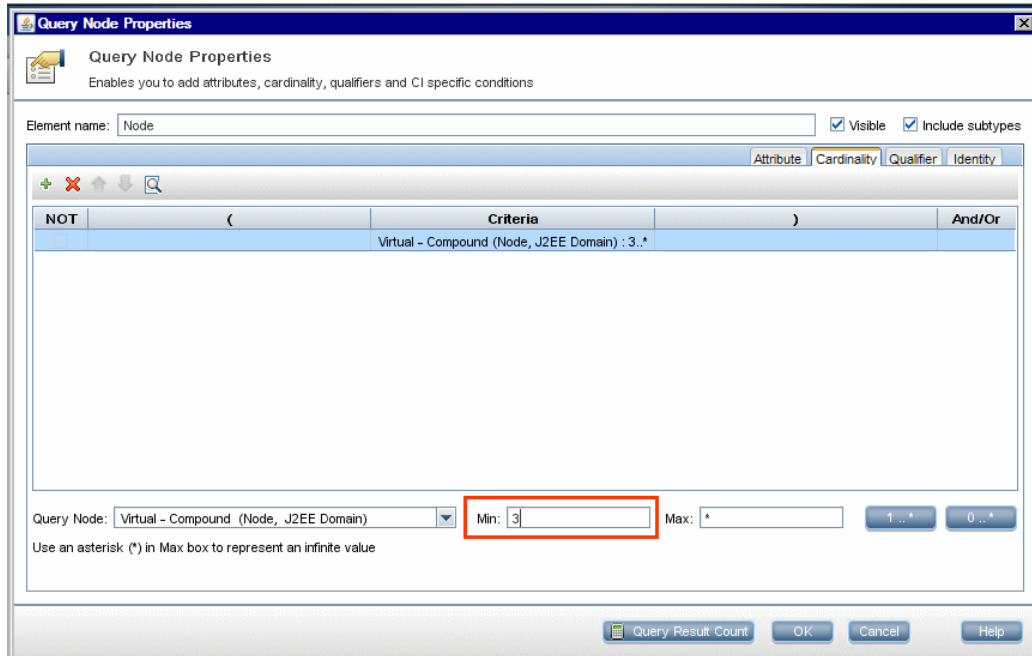
To create a query containing a compound relationship:

- a. Click the **New** button  in the Modeling Studio and select Query.
- b. Drag a J2EE Domain CI and a Node CI onto the modeling pane.
- c. Select both CIs and add a new compound relationship (using right click context menu).
- d. Edit the compound link to add the following path elements:
 - J2EE Domain - Composition - J2EE Cluster
 - J2EE Cluster - Membership - J2EE Server
 - J2EE Server - Composition - Windows

Note that the direction of the compound link is from the J2EE Domain to the node:



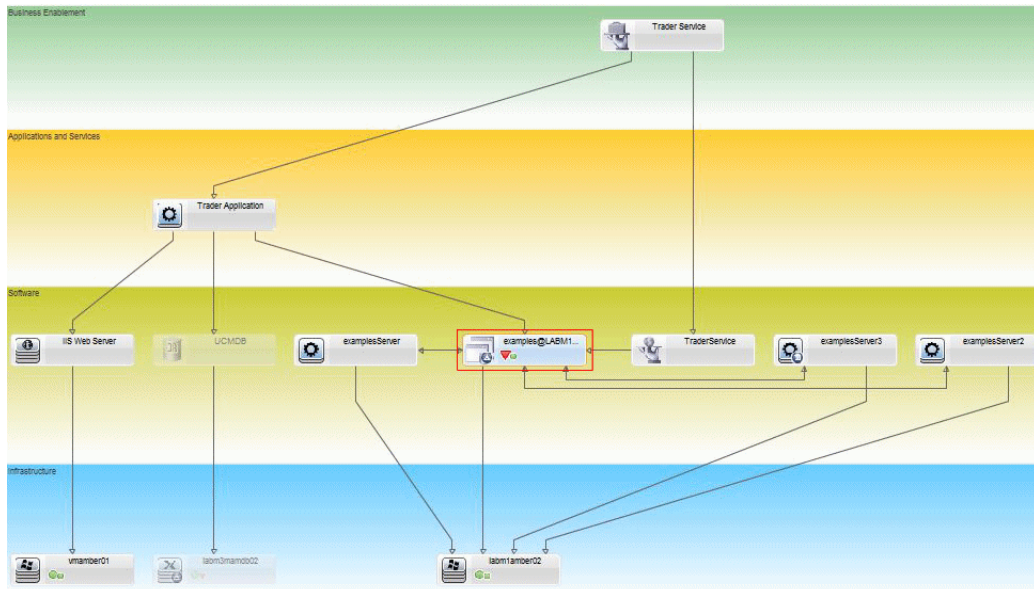
- e. Edit the Node cardinality to be three at minimum. Right-click the Node CI, select **Query Node Properties**, select the **Cardinality** tab and enter **3** in the **Min** box:



- f. When you are finished, save the query.
3. **Define the Topology Policy in Configuration Manager**
 - a. In Configuration Manager, navigate to the Policies moduland create a new topology policy.
 - b. Set the name and description and assign the new policy to the **Trader** managed view.
 - c. Under Condition, select the query you have prepared in UCMDB and select **positive** as the condition type.

- d. Save the new policy and preview it.

Note that the new policy indicates a breach on the J2EE Domain if the number of nodes supporting the J2EE Cluster is less than three, as displayed in the following image:



Configuration Manager Similarity Policy - Use Cases

This section describes two use cases for similarity policies in Configuration Manager.

- "All UNIX machines in a lab that are connected to an Oracle database must have the same OS version" below
- "All application servers in each cluster must have the same attributes " on the next page

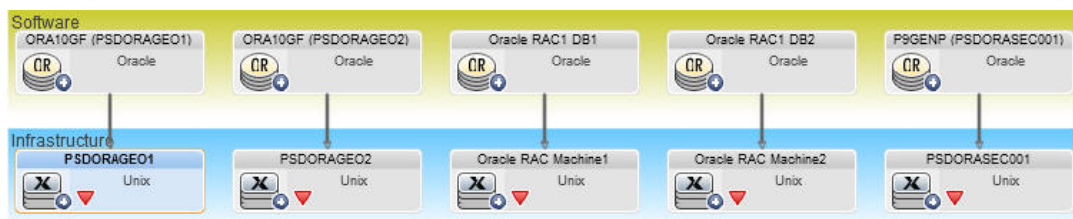
All UNIX machines in a lab that are connected to an Oracle database must have the same OS version

This scenario includes the following steps:

- "Background" below
- "Define a Similarity Policy" on the next page

1. Background

A UNIX lab administrator has the following view managed in Configuration Manager:



He wants to ensure that all the UNIX machines that are connected to an Oracle database (that is, those highlighted in the diagram above) have the same OS version. Since he always likes to make sure his machines are running the latest patch, this version changes often.

2. Define a Similarity Policy

In Configuration Manager, navigate to Policies and create a new similarity policy.

- Deselect the **Enable grouping** check box.
- Set the name and description.
- Select UNIX as the main CIT.
- Filter the comparison scope by **Related to Oracle**.
- Select the OS version attribute as the similarity criterion.

Note: This is unlike a baseline policy, which contains fixed attribute values that are entered when the policy is created or updated.

The new policy dynamically and constantly detects any misalignments in the OS version attribute of each of the UNIX machines that are highlighted in the diagram above. This means that the user does not have to manually update the policy definition every time an upgrade occurs in the environment.

After defining this policy, policy status icons are displayed in the Review/Authorize, Changes History, Authorization History, and Explore Views modules.

All application servers in each cluster must have the same attributes

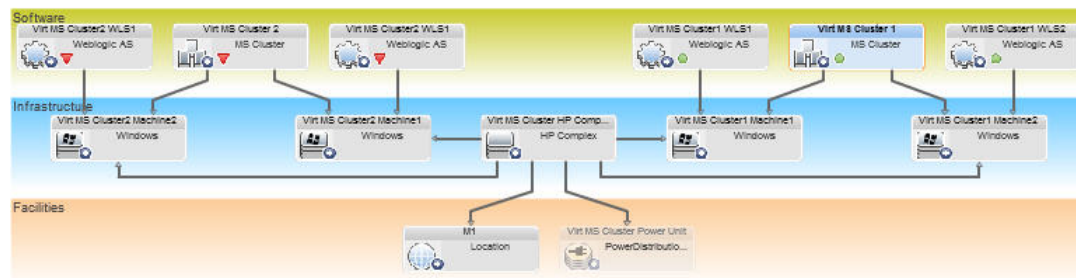
In this example, the attributes that must be the same are Application Installed Path, Application Version Description, Vendor, and Version.

This scenario includes the following steps:

- "Background" on the previous page
- "Create Views" on the next page
- "Define a Similarity Policy" above

1. Background

A user has the following view managed in Configuration Manager:



Since there are many clusters and many application servers in each cluster, he wants to ensure that for each cluster, the application servers have the same defined attributes.

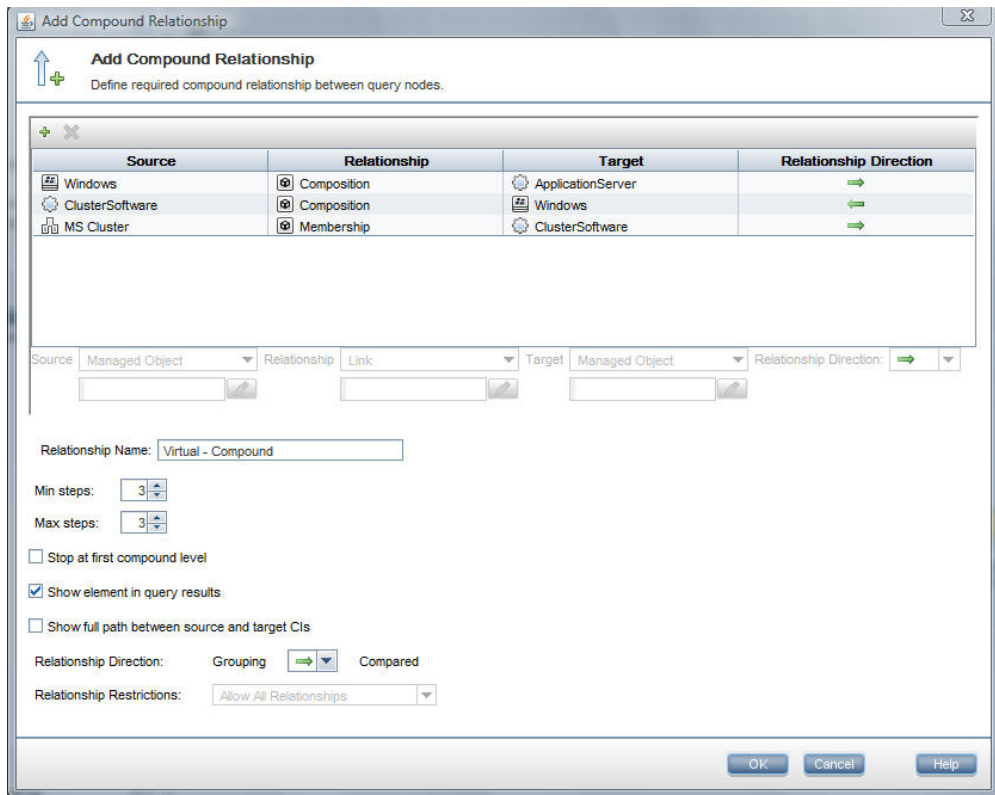
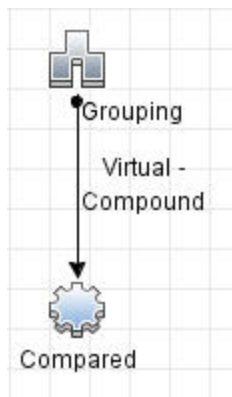
2. Create Views

Use the view shown above or create new views (each containing a cluster) to test against the policy.

3. Define a Similarity Policy

In Configuration Manager, navigate to Policies and create a new similarity policy.

- a. Make sure that the **Enable grouping by CI type and pattern** check box is selected.
- b. In the Grouping section:
 - o Select the grouping CI type (in this example, Cluster).
 - o Select the grouping TQL that defines the desired path between the Cluster CIT and the application server. For example:



- c. Set the name and description.
- d. Select the Version attribute as the similarity criterion.

Note: This is unlike a baseline policy, which contains fixed attribute values that are entered when the policy is created or updated.

The new policy dynamically and constantly detects any misalignments in the compared attributes of each of the highlighted application server groups shown above. This means that the user does not have to manually update a policy definition every time an upgrade occurs in the environment. Note that the compared attributes are compared only within each cluster group, and not between groups.

After defining this policy, policy status icons are displayed in the Review/Authorize, Changes History, Authorization History, and Explore Views modules.

Policies User Interface







This section includes (in alphabetical order):










Attribute Operators	166
Policies Page	167
Policy Preview Dialog Box	172
Select Composite CI Dialog Box	173

Attribute Operators

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

Select the check box in the NOT column next to any operator to exclude the value of that operator from the attribute condition.

Operator	Symbol	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.
Empty		Checks whether the attribute value is empty.
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.



Operator	Symbol	Description
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  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  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 (% or *). Use Like to search for a fragment of a name. You can insert the wildcard character at any point in the name.
Like ignore case		Uses a wildcard (% or *). Use Like ignore case to search for a fragment of a name. The case of the string is ignored.











Policies Page

This page enables you to define and edit configuration policies.

To access	Select 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.
Relevant tasks	<ul style="list-style-type: none"> • "Define a Baseline or Topology Policy" on page 157 • "Define a Similarity Policy" on page 158

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: <ul style="list-style-type: none"> • Add Baseline Policy • Add Topology Policy • Add Similarity Policy

UI Elements (A-Z)	Description
	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.
	<p>Click Preview to open the Policy Preview dialog box, which provides a preview of the satisfaction level of the selected policy over the selected views.</p> <p>In previews of baseline policies, you can select a CI and drill down to analyze its details.</p> <p>Note: Only views for which the user has View permission are sent to the server and are displayed in the preview results. If a user does not have View permission for a particular view and attempts to preview it, an error message is displayed.</p>
	Click Recalculate Policy Analysis to recalculate the policy analysis for the selected policy.
	<p>Click Export Report to choose the export format for the Policies Report data. The available options are:</p> <ul style="list-style-type: none"> • Excel. The table data is formatted as an .XLS (Excel) file that can be displayed in a spreadsheet. • PDF. The table data is exported in PDF format. • CSV. The table data is formatted as a comma-separated values (CSV) text file that can be displayed in a spreadsheet. <p>The currently applied filters are taken into account when generating output for reports.</p>
	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
Comparison Scope (for Similarity policies)	<p>This section is used to specify (and optionally, further filter) the main CI type to be compared for similarity.</p> <p>The comparison scope CI type is automatically selected when you use the Grouping option.</p>
Filter (for Baseline and Topology policies)	<p>This section is used to filter the CIs that are tested against the policy. This section includes:</p> <ul style="list-style-type: none"> • 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 171 • 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 select the required filter TQL query.
General	<p>This section includes:</p> <ul style="list-style-type: none"> • Description. Enter the policy description. • Policy Name. Enter the policy name. • Categories. Categories are optional user-defined keywords that logically categorize the policy, and can be used for filtering. For example, if you create a baseline policy that validates that all lab computers have standard hardware, you might categorize the policy using the keyword 'Standardization'. <p>Click  to open the Policy Categories dialog box, and then click  to add the desired category. You can add multiple categories to a policy.</p>
Grouping	<p>This section is used to specify groups of CIs that need to be similar. CIs will be compared for similarity to each other only if they are located</p>




UI Elements (A-Z)	Description
(for Similarity policies)	<p>within the same group. The Enable grouping by CI type and pattern check box is selected by default. This section includes:</p> <ul style="list-style-type: none"> The main CI type to be used as the basis for a group 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. <p>After selecting a grouping CI type, the system folders are scanned and only those grouping patterns that are relevant to the selected CI type are displayed in the Select grouping pattern dialog box.</p> <ul style="list-style-type: none"> The grouping pattern for the main CI type. Click the  button to open the Select grouping pattern dialog box. <p>Grouping patterns are specific TQL queries (defined in UCMDB). These TQL queries must define only a compound link from the desired Grouping CI type to the desired Compared (main) CI type – and nothing else.</p> <p>For Configuration Manager to correctly identify the Grouping CI type and the Compared (main) CI type, the elements in the TQL query must be named Grouping and Compared, respectively.</p> <p>These grouping TQL queries must be located in UCMDB in the following location: Modeling Studio > Resources tab (select Queries as the resource type) > Configuration Manager > Grouping Patterns folder. If the Grouping Patterns folder does not already exist, create it.</p> <p>Selecting a pattern automatically selects the CI type for the Comparison Scope section.</p> <ul style="list-style-type: none"> Properties selector for the grouping CI type. Click the  button to open the Specify baseline for filter dialog box. For details about selecting properties, see "Baseline CI Section" on the next page An additional CI type that is related to the grouping 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 select the required filter TQL query. <p>For additional details about grouping, see "Configuration Manager Similarity Policy - Use Cases" on page 163.</p>
<p>Similarity Criteria (for Similarity policies)</p>	<p>This section is used to specify the CI type and attributes to be tested against the policy. By default, all components and attributes in the selected CIs are included. If you do not want a specific component to be included, clear the check box next to that component.</p> <p>When you remove a component from the similarity criteria, all of its</p>

UI Elements (A-Z)	Description
	<p>attributes are automatically removed from the scope as well. You can include a component, 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.</p> <p>The comparison scope CI (to which the similarity criteria apply) is automatically selected when you use the Grouping option.</p>
Validity	<p>This section is used to 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.</p>
Views	<p>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.</p>

Baseline CI Section


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

UI Elements (A-Z)	Description
	<p>Select one of the following options:</p> <ul style="list-style-type: none"> • 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.
	<p>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.</p>
	<p>Click Remove Selected Item from Baseline to delete the selected CIs from the baseline definition.</p>
<Check box column>	<p>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.</p>



UI Elements (A-Z)	Description
<Comparable column>	<ul style="list-style-type: none"> 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.
Attribute Name column	The names of the attributes for the selected CI.
Attribute Value column	<p>The values of the attributes for the selected CI.</p> <ul style="list-style-type: none"> 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	<p>Select a CI type from the baseline. The attributes for this CI type are displayed in the table.</p> <p>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.</p>
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 166.


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 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.

UI Elements (A-Z)	Description
	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.
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 policies:

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

Chapter 17

Reports

This chapter includes:

Reports Overview	174
Schedule a Report	174
Reports User Interface	175

Reports Overview

The Reports module enables you to schedule operational reports that are automatically sent to you by email. These reports provides a way for you receive details about the current status of your environment or selected changes to it.



The body of the email that is sent displays the name of the report, its description, and the name of the view for which the report was configured.

The body of the email that is sent displays the name of the report, its description, and the name of the view containing the CIs that are included in the report.

Schedule a Report

This task describes how to schedule operational reports about the status of your system, and have these reports automatically sent to you by email at the frequency that you specify.

To schedule a report:

1. Before you begin, make sure that your system administrator has enabled the system to send email notifications and has provided your email address. For details, see the section about mail settings in the "[Settings Page](#)" on page 181 and the section about specifying details for a user in the *HP Universal CMDB Administration Guide*.
2. Navigate to **Reports**.
3. Do one of the following:
 - Click  to create a new report.
 - Click  to edit an existing report.

The Report Definition page of the Add Report wizard is displayed. Specify the following information:

- The view on which the report will be based. You can only select views for which you have at least View permission.

- The type of report that will be generated. A default description for the selected report type is provided, which you can edit. This description will also appear in the body of the email and in the report.
 - The name of the report, which will be used as the file name of the report, displayed in the list of scheduled reports, and displayed in the subject of the email and the body of the report.
 - The output format of the generated report. The default format is Microsoft Office Excel Workbook (.xls).
4. Click **Next**. The Frequency Selection page is displayed.
- Specify the frequency at which you want the report to be generated.
5. Optionally, click **Next** to add one or more additional filters for the information contained in the selected view, or click **Finish** to end. The report will now appear in the list of scheduled reports.

Note: The available filters are dependant on the report type that you selected.

For details, see "Report Details Wizard" below.


Reports User Interface

This section includes (in alphabetical order):

Report Details Wizard	175
Reports Page	177

Report Details Wizard



This wizard enables you to schedule automatic operational reports.

To access	Click  in the Reports module.
Relevant tasks	"Schedule a Report" on the previous page
Wizard map	The "Report Details Wizard" contains: "Report Definition Page" > "Frequency Selection Page" > "Filter Selection Page"

Report Definition Page

This page allows you to specify general report details.

User interface elements are described below:

UI Elements (A-Z)	Description
Description	A brief description of the report type.
File Type	From the dropdown list, select the format in which you want to receive the report. Available types are: <ul style="list-style-type: none">• Microsoft Office Excel Workbook (*.xls)• Adobe Document (*.pdf)• Comma Separated Values (*.csv)
Name	The name that you assign to the report.
Report Type	Click  to select one of the predefined report types.
View	Click  to select the view on which a report is based.

Frequency Selection Page

This page enables you to specify the frequency at which you want to receive the report.

Certain report types compare data at two points in time. For those report types, the specified frequency also determines which points in time are used when the report is created.

User interface elements are described below:

UI Elements (A-Z)	Description
Frequency	Available frequencies are: <ul style="list-style-type: none">• Daily. Generates the report on a daily basis.• Weekly. Generates the report on a weekly basis.• Monthly. Generates the report on a monthly basis.

Filter Selection Page

This page enables you to optionally specify additional filters for the information contained in the report. The list of available filters depends on the selected report type.

The filters that you specify are listed in the generated report.

User interface elements are described below:






UI Elements (A-Z)	Description
<List of filters>	(Optional) Specify one or more of the available filters.

Reports Page

This page enables you to add new scheduled reports, modify existing reports or delete existing scheduled reports, and to manually run a scheduled report job.

To access	Select Reports .
Relevant tasks	"Schedule a Report" on page 174

User interface elements are described below:

UI Elements (A-Z)	Description
	Click to add a new scheduled report to the list.
	Click to edit an existing scheduled report.
	Click to delete a scheduled report from the list.
	Click to manually generate and send the selected report. Note: The report is generated and sent without changing the next scheduled event time.
	Click to refresh the list of scheduled reports.
Description	A brief description of the report, as specified in the Add Report Wizard. For details, see " Report Definition Page " on the previous page.
Last Execution Time	The last time the report was generated.
Name	The name that you assign to the report, as specified in the Add Report Wizard. For details, see " Report Details Wizard " on page 175.
Next Execution Time	The next time the report is scheduled to be generated. For details, see " Frequency Selection Page " on the previous page
Report Type	The report type that will be used as the basis for the report, as specified in the Add Report Wizard. For details, see " Report Definition Page " on the previous page.
View	The view on which the report is based. For details, see " Report Details Wizard " on page 175. Note: If the view on which a report is based has been deleted from UCMDB, or if you no longer have permission to access the view on which a report is based, a warning icon appears next to the name of the view and an error message is displayed. In these cases, the report cannot be generated and sent.

Chapter 18

Settings

This chapter includes:

Settings Overview	178
Add a New Layer to the Topology Layout	179
Save and Apply Configuration Changes	179
Settings User Interface	180

Settings Overview

The 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 180](#).

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 the next page](#).

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 181](#).

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 192.



Note: Make sure that Server Administrator Privileges have been enabled in order to make changes to the Configuration Manager setup.

Add a New Layer to the Topology Layout

This task describes how to add a new layer to the topology layout.


1. Navigate to **Administration > Settings > Application Management > Topology Presentation > Topology Layout**.
2. In the Layers pane, click  to add a new configuration to the configuration set.
 - In the Display Name field, enter a name for the new layer.
 - From the Name list, select **virtualization_infrastructure**.
 - In the Level Number field, enter **5**.
 - In the Color of the Layer column, select a color for the new layer. Verify that the color of the new layer is the same as the color of the virtualization infrastructure classification.



Note: It is recommended that both the color of the layer and the color of the classification values be the same.

3. In the Level Number field for the Facilities layer, enter **6**.
4. Click  to save the new configuration set.
5. In the Save as Draft dialog box, enter a name for the new configuration set and click **Save**.
6. Click  to activate the configuration set that you just saved.

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 **Administration > 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.


Settings User Interface

This section includes (in alphabetical order):




Open Configuration Set Dialog Box	180
Save as Draft Dialog Box	181
Settings Page	181

Open Configuration Set Dialog Box

This dialog box displays a list of all the existing configuration set versions.

To access	Select Administration > 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 the previous page


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.
	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.

UI Elements (A-Z)	Description
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 179](#).

To access	Select Administration > 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 179

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.




Settings Page






This page enables you to modify the configuration settings for Configuration Manager.

To access	Select Administration > 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.

Left Pane

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

UI Elements (A-Z)	Description
	<p>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.</p> <p>This button is enabled when you make a change to the currently activated configuration set. For details, see "Save as Draft Dialog Box" on the previous page.</p>
	<p>Open configuration set. Displays a list of all the existing configuration set versions. For details, see "Open Configuration Set Dialog Box" on page 180.</p>
	<p>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.</p> <p>Important: Configuration Manager enables you to import a partially exported configuration set from the same version of Configuration Manager, to an existing configuration set.</p> <ul style="list-style-type: none"> 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. <p>For example:</p> <ol style="list-style-type: none"> Select Administration > Settings > Application Management > Topology Presentation > Topology Layout. In the Layers pane, remove the field Software and its associated color. Export that configuration set. 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. <p>Note:</p> <ul style="list-style-type: none"> 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

UI Elements (A-Z)	Description
	<p>Import Configuration Set dialog box to create a draft.</p> <p>Limitations:</p> <ul style="list-style-type: none"> • 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 212. • 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. <p>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.</p>
	<p>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.</p> <p>Select the configuration settings you want to export from the tree in the Export Configuration Set tree dialog box.</p>
	<p>Activate current configuration set. Applies the configuration properties in the draft/configuration set to Configuration Manager and becomes the active configuration set.</p> <p>Note: Only one configuration set is considered active at any given point of time.</p>
	<p>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.</p>
	<p>Remove configuration from configuration set. This button is only enabled when you select a node on the configuration tree that allows you to delete a child configuration.</p>
	<p>Denotes a configuration category.</p> <p>Note: The arrow next to each category enables you to expand or collapse the lower-level categories.</p>
<p><Configuration tree></p>	<p>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.</p>

The following categories contain configuration settings:

Automation Impact

To access	Select Administration > Settings > Application Management > Automation Impact .
------------------	---

User interface elements are described below:

Setting	Description
Impact analysis state	<p>Enables you to determine whether impact analysis calculates the effects of the automation on CIs from the actual or authorized state of a view.</p> <p>The options are:</p> <ul style="list-style-type: none">• Actual (default)• Authorized <p>For details, see "Automation Analysis > Impact - <State> Pane" on page 76.</p>

Change Management

To access	Select Administration > Settings > Integrations > Change Management .
------------------	---

User interface elements are described below:

Setting	Description
Change Management integration enabled	<p>Select the check box to:</p> <ul style="list-style-type: none">• enable direct integration with the change management system to create an RFC.• log authorization actions for the relevant RFC in the change management system. <p>These can either be rollback RFCs in the Review/Authorize module or policy remediation RFCs in the Explore Views module.</p>

Daily View Refresh Settings

To access	Select Administration > 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.

Display Settings

To access	Select Administration > Settings > Display Settings .
------------------	--





User interface elements are described below:

Setting	Description
Enable CIs in multiple views indication	Select this check box if you want warning icons to be displayed in the CI lists saying that the CI is managed in multiple views. By default, this option is disabled.

Fetches RFCs Criteria

To access	Select Administration > 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: <ul style="list-style-type: none">•  Click to add a new CI type.•  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: <ul style="list-style-type: none">•  Click to add a new property.•  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 Administration > 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 205.
Hour at which to send mails (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	<p>The full URL of the Configuration Manager server. This URL fulfills two purposes:</p> <ul style="list-style-type: none"> • Provides the ability to insert links to Configuration Manager into email notifications and scheduled reports (when this URL is specified and detailed information is requested.) • Links to Configuration Manager from the launch page of UCMDB. (This URL can be configured in UCMDB as well.) <p>Note: If Configuration Manager is installed behind a reverse proxy, provide reverse proxy URL.</p>
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 Administration > 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 Administration > 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 Administration > 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.

Setting	Description
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 Administration > 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 (enterprise, site/department, multiple users, or individual user).
Urgency	The urgency of the RFC (critical, high, average, or low).
Risk Assessment	The assessment of the risk of the RFC (no risk, low risk, some risk, moderate risk, high risk, or very high risk). Relevant to: planned RFCs
Reason for change	The reason why the RFC is required.

RFC Display

To access	Select Administration > Settings > Application Management > RFC > RFC Display .
------------------	--

User interface elements are described below:

Setting	Description
RFC Properties	Configure the RFC properties for display:

Setting	Description
	<ul style="list-style-type: none">  Click to add a new property.  Click to delete the selected property. <p>You can edit the property names manually.</p>

Service Manager

To access	Select Administration > Settings > Integrations > Change Management > Service Manager .
Important information	You must load the cm4sm.unl file into Service Manager to enable the service that allows integration between Service Manager and Configuration Manager. For details, see " Import a UNL File into Service Manager " on page 112.
See also	"Change Management" on page 184



User interface elements are described below:





Setting	Description
Connection strategy	Select HTTP or HTTPS.
Host Name	The host name of the Service Manager server.
Port Number	The port number of the Service Manager server (default: 13080).
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 Administration > Settings > Application Management > Topology Presentation > Topology Layout .
------------------	--

User interface elements are described below:

Setting	Description
Layers	<p>Configure the layers of the topology map display:</p> <ul style="list-style-type: none">  Click to add a new layer.  Click to delete the selected layer.

Setting	Description
	<p>You can edit the name, display name, level number, and color of the layers.</p> <p>For details, see "Add a New Layer to the Topology Layout" on page 179</p>
Classifications	<p>Configure the classifications of the topology map display:</p> <ul style="list-style-type: none">  Click to add a new classification.  Click to delete the selected classification. <p>You can edit the name, display name, and color of the classifications.</p>
Layout Exceptions	<p>Configure exceptions to the classifications defined above:</p> <ul style="list-style-type: none">  Click to add a new exception.  Click to delete the selected exception. <p>For the selected CI type, if the specified attribute has the specified value, the specified classification applies.</p>

Topology Limitations

To access	Select Administration > Settings > Application Management > Topology Limitations .
Important information	After changing the topology limitation settings, you must restart the Configuration Manager server.

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 Administration > Settings > Integrations > UCMDB Foundation > UCMDB Foundation .
Important information	This section contains the information UCMDB Foundation connection that was specified during installation. You can only edit the UCMDB access URL field. Note that if you define a reverse proxy or root context for UCMDB, you must update the UCMDB access URL field accordingly.



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 Administration > Settings > Integrations > UI Integrations .
------------------	---

User interface elements are described below:

Setting	Description
Configured UIs	<p>Configure the URLs that can be opened:</p> <ul style="list-style-type: none"> •  Click to add a new URL to the list. <p>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:</p> <ul style="list-style-type: none"> ▪ \${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) ▪ \${ucmdbcmViewId}—The ID of the view (Configuration Manager view ID) <ul style="list-style-type: none"> •  Click to delete the selected URL. <p>A valid URL must begin with one of the following:</p> <ul style="list-style-type: none"> • http:// • https:// • mailto:

Value Suggestions






To access	Select Administration > 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.

Problems Pane

User interface elements are described below:

UI Elements (A-Z)	Description
	Indicates the severity level of the problem. The following icons appear: <ul style="list-style-type: none">  . 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.  . 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.

Chapter 19

Automation Setup

This module is only valid for use by customers who purchased the relevant license for HP Universal CMDB Configuration Manager versions 9.2 or 9.3. New customers cannot purchase this license.

HP Software recommends using the UCMDDB Browser Automation widget (also available in the embedded UCMDDB Browser in Configuration Manager) to configure automated flows that are based on Configuration management conditions. For details, see the section about the Automation widget in the UCMDDB Browser online help.

This chapter includes:

Automation Setup Overview	193
Set Up an Automation	194
Automation Setup User Interface	195

Automation Setup 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.

This task includes the following steps:

- "Configure HP Operations Orchestration connection settings" below
- "Import a flow from HP Operations Orchestration" below
- "Specify automation properties" on the next page


1. Configure HP Operations Orchestration connection settings

- a. Navigate to **Administration > Settings > Integrations > Operations Orchestration (OO) > OO Server Location**. (missing or bad snippet)
- 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.
OO Server Unique ID	The HP Operations Orchestration instance name that uniquely identifies the HP Operations Orchestration instance being used by Configuration Manager.
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 Setup**.
- b. Click  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 Setup 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.
 - o The name of the automation is automatically taken from the OO flow, but can be changed.
 - o You must specify the CI type to be automated.
- c. Click **Save** .

Automation Setup User Interface

This section includes:





Automation Setup Page195


Automation Setup 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 Setup .
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 66


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.

UI Elements (A-Z)	Description
	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. <ul style="list-style-type: none"> In a controlled automation, you review the policies and analysis before running the automation.

UI Elements (A-Z)	Description
	<ul style="list-style-type: none"> In a non-controlled automation, the automation runs without any additional information. <p>For details on running an automation, see "Run a Controlled or Non-Controlled Automation" on page 66.</p>
Estimated level of risk	<p>A subjective evaluation of the level of risk in the automation. Valid values are:</p> <ul style="list-style-type: none"> Unknown None Low Medium High <p>Relevant when defining policies and during automation analysis.</p>

<Automation> Pane - Execution Parameters Area

User interface elements are described below:

UI Elements (A-Z)	Description
<Flow execution parameters>	<p>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.</p> <p>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 the Explore Views module. For information on how to run an automation, see "Run a Controlled or Non-Controlled Automation" on page 66.</p>

Chapter 20

Automation Policies

This module is only valid for use by customers who purchased the relevant license for HP Universal CMDB Configuration Manager versions 9.2 or 9.3. New customers cannot purchase this license.

HP Software recommends using the UCMDB Browser Automation widget (also available in the embedded UCMDB Browser in Configuration Manager) to configure automated flows that are based on Configuration management conditions. For details, see the section about the Automation widget in the UCMDB Browser online help.

This chapter includes:

Automation Policies Management Overview	198
Define an Automation Policy	199
Configuration Manager Automation Policy - Use Case	199
Automation Policies User Interface	200

Automation Policies 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 72.

For details on defining automation policies, see "[Automation Policies Page](#)" on page 201.

Note: Users with Automation Policies 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 > 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:

- ["Background" below](#)
- ["Prerequisite - Import the Managed View from HP Universal CMDB" below](#)
- ["Define the Automation Policy in Configuration Manager" on the next page](#)
- ["View Policy Evaluation Results" on the next page](#)

1. Background

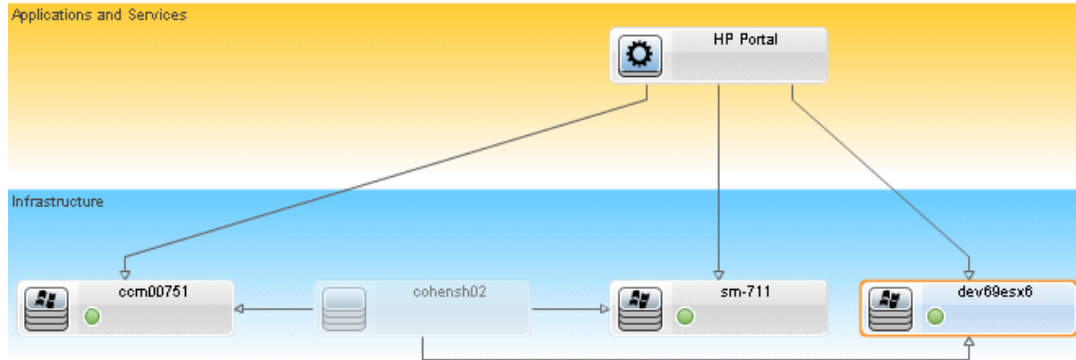
The owner of the **HP Portal** application needs to continually monitor the high-availability of his application. As a result, it is important to guarantee that when changes occur, the application will continue to function in accordance with its agreed to requirements.

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 150.

3. Define the Automation Policy in Configuration Manager

- a. Navigate to **Administration > 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 **BusinessApplication** as the CI type to be tested against the policy.
- d. In the **Restriction** area, do the following:
 - Under **Automation restriction conditions**, select **Causes Downtime**.
 - Under **CI restriction conditions**, select **Direct Collision Exists**.
- 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 66.

Automation Policies User Interface

This section includes:

Automation Policies Page	201
--------------------------------	-----





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 > Automation Policies .
Important information	You must have Automation Policies permission to work with this module.
Relevant tasks	<ul style="list-style-type: none"> • "Run a Controlled or Non-Controlled Automation" on page 66 • "Define an Automation Policy" on page 199 • "Configuration Manager Automation Policy - Use Case" on page 199
See also	"Automation Execution Dialog Box" on page 72.

User interface elements are described below:

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

UI Element (A-Z)	Description
	<ul style="list-style-type: none"> • 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. <p>Note: If neither of the check boxes are selected, the policy validation is never calculated.</p>
Policy Name	Enter a unique policy name.

Scope Pane

User interface elements are described below:

UI Element (A-Z)	Description
Assign CI Type	<p>The CI type of the CIs to be tested against the policy.</p> <p>Click the  button to open the select CI Type dialog box, which enables you to select the required CI type.</p> <p>At least one CI of the CI type selected must appear in the impact topology map for policy validation to be calculated.</p> <p>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.</p> <p>If there is no CI of the type Windows in your topology map, the policy is not evaluated.</p> <p>Note: If no CI type is specified, then the policy applies to all CIs.</p>
Assign policy to views	<p>Enables you to select the views to which the policy applies.</p> <ul style="list-style-type: none"> • All Views. Apply the policy to all managed views. Note: You need Authorize permission to apply a policy to all views, including the views you are not managing. If you do not have Authorize 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. <p>Note: If you do not select either All Views or select a view from the Selected Views option, the policy validity is not calculated.</p>

Restrictions Pane

User interface elements are described below:

UI Element (A-Z)	Description
<p>Automation Restriction Conditions</p>	<p>Describes the automation restriction conditions for this policy.</p> <p>For example, you can define a policy which stipulates that running your automation for the first time causes a policy breach.</p> <p>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.</p> <p>For a list of the operators used to define attribute conditions, see "Attribute Operators" on page 166.</p> <p>For a description of the conditions you can define, see "Automation Execution Dialog Box" on page 72.</p>
<p>CI Restriction Conditions</p>	<p>Describes the CI restriction conditions for this policy.</p> <p>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.</p> <p>There must be at least one CI in your impact map that complies with all the conditions defined for the policy to be breached.</p> <ul style="list-style-type: none"> • 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. <p>For a list of the operators used to define attribute conditions, see "Attribute Operators" on page 166.</p> <p>The CI Restriction conditions are:</p> <ul style="list-style-type: none"> • 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. <p>For more information about collisions, see "Automation Execution Dialog Box" on page 72.</p> <p>For more information on impact importance and impact severity, see "Automation Analysis > Impact - <State> Pane" on page 76.</p>

Chapter 21

User Preferences

This chapter includes:

User Preferences Overview	204
Configure Email Notifications	204
User Preferences User Interface	205

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.

Note: Clicking on a link in an email notification on a mobile device opens the UCMDB Browser.

This task describes how to set up emails that inform you when items requiring your intervention or attention occur, such as CIs or views that are waiting to be authorized, or CIs that are breaching policies. This allows the user to get an overview of events that are possibly waiting for his action

This task includes the following steps:


1. "Prerequisites " below
2. "Specify notification content and frequency" below

1. Prerequisites

Make sure that the system administrator has specified the following:

- Your email address. For details, see the section about specifying details for a user in the *HP Universal CMDB Administration Guide*.
- Time and SMTP account information for emails.

2. Specify notification content and frequency

- a. Click the **User Preferences**  icon. Click **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 Review/Authorize 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 205

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	Click  at the top of the Configuration Manager screen.
Important information	<p>The following options are available:</p> <ul style="list-style-type: none"> • 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. <p>Note:</p> <ul style="list-style-type: none"> • 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 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: <ul style="list-style-type: none"> • 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	<p>Select the frequency at which you want to receive notifications. Select one of the following options:</p> <ul style="list-style-type: none"> • 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	<p>Select the Enable notifications check box to enable email notifications.</p>
Views	<p>Specifies the views for which you want to received notifications. Select one of the following options:</p> <ul style="list-style-type: none"> • All views. Receive notifications for all views for which you have View permission. • Only views for which I have Authorize permission. Receive notifications for all views for which you have Authorize permission (default). • Favorite views. Receive notifications only for your favorite views. • Selected views. Receive notifications for a customized list of views
Notifications scope	<p>Select one or both of the Configuration Manager actions for which you want to received notifications:</p> <ul style="list-style-type: none"> • authorizations that are pending approval • policies that are in breach <p>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.</p>

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 <i>HP Universal CMDB Deployment Guide</i> .	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:

Export Configuration Set	212
Import Configuration Set	214
Password Encryption	216
Populate	217
Generate Keys	218

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 <data base 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: H2Dialect, 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>	Dump file name
-file <filename>	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 <code>--connection-url</code> , <code>--driver</code> , <code>--username</code> and <code>--password</code> to specify the database properties.
--password	Database password Note: Use this only if <code>-p</code> is not used. Use it with <code>--connection-url</code> , <code>--dialect</code> , <code>--driver</code> and <code>--username</code> .
--username	Database username Note: Use this only if <code>-p</code> is not used. Use it with <code>--connection-url</code> , <code>--dialect</code> , <code>--driver</code> and <code>-password</code>
--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 <d  
atabase 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: H2Dialect, 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 .

Option	Description
-f <filename>	Dump file name
-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 <code>--connection-url</code> , <code>--driver</code> , <code>--username</code> and <code>--password</code> to specify the database properties.
-password	Database password Note: Use this only if <code>-p</code> is not used. Use it with <code>--connection-url</code> , <code>--dialect</code> , <code>--driver</code> and <code>--username</code> .
-username	Database username Note: Use this only if <code>-p</code> is not used. Use it with <code>--connection-url</code> , <code>--dialect</code> , <code>--driver</code> and <code>-password</code>
-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 section includes:

Importing and Exporting System Data Overview	219
Export the System Data	220
Import the System Data	221
Set Log Verbosity Levels	221

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 Views module. The TQLs which the views reference are not exported.
- The configuration policy setting defined in the 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 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 Policies module.

To export the referenced TQLs, use the Package Manager in HP Universal CMDB. For details, see the *HP Universal CMDB Administration Guide*.

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 the next page](#).

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 = **sysadmin**
- Password = **sysadmin**
3. Under **Configuration Manager**, 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 = **sysadmin**
 - Password = **sysadmin**
3. Under **Configuration Manager**, 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 the [previous page](#).

To modify the message severity level displayed:

Edit the following line in the **<Configuration Manager installation directory>\conflcmlog4j.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.